3. SCOPE OF SERVICES

To enable the State to determine the capabilities of a Contractor to provide a Provider Services Module for the Department of Public Health and Human Services (DPHHS), the Offeror shall respond to the following regarding its ability to meet the State's requirements.

All subsections of Section 3 require a response. The Offeror must indicate certification of understanding for Sections 3.1-3.8. For Sections 3.9 -3.10, the offeror must restate the subsection number and the text immediately prior to your written response.

NOTE: Each item must be thoroughly addressed. Offerors taking exception to any requirements listed in this section may be found nonresponsive or be subject to point deductions.

Team CNSI has fully assessed the MT PSM RFP and our response confirms and certifies our understanding of the detailed scope. Team CNSI is well-positioned to deliver the services for MT PSM based on the following factors:

- Feature-rich evoBrix Provider Management and CRM/IVR modules aligned with multi-state RFP requirements
- A solution built on previously certified application components
- Multi-state SaaS implementation and operations track record
- Mature business operations teams
- Streamlined implementation methodology using our Solution, Configuration, and Implementation (SCI) approach
- Mature SaaS ITIL-based operations methodology
- Secure FedRAMP cloud hosting capabilities

Team CNSI has fundamentally transformed its technology, infrastructure, and service delivery models over the past several years to align with a modular architecture delivered through SaaS services. Our assessment of the state's vision and the MPATH road map is that it is highly aligned to Team CNSI's strategy.

Team CNSI has assessed the detailed requirements of the MT PSM module including Base, Option A, and Option B. At a high level, our approaches to each component of the MT PSM module are explained in Figure 3-1.

Component	Approach	Foundational Components, Hosting, and Methodologies
Base	■ Leverage Team CNSI's evoBrix Provider Management Information System (PMIS) module and sub-modules including: ● Provider enrollment and management ● Provider Credentialing Service (PCS) integrated with LexisNexis ● SiteVisitPro (SVP) ● Reporting - Cognos COTS solution ● Address Validation/Standardization - Pitney Bowes Spectrum Universal Addressing Model ● Correspondence - EngageOne COTS solution ● Enterprise Content Management - FileNet COTS solution ● Fee Collection - FirstData cloud solution	■ Leverage evoBrix foundational components: ● SOA/ESB integration built on Oracle SOA suite ● Interface Service Repository (ISR) for interface processing ● RuleIT rules engine ■ Leverage existing Training materials delivered through a web-based LMS ■ Hosted in CNSI's private cloud residing in Oracle's FedRAMP Government Cloud with High Availability and Disaster Recovery ■ SCI implementation methodology assessed

Component	Approach	Foundational Components, Hosting, and Methodologies
Option A	■ Leverage Team CNSI's evoBrix Provider, Core Claims, and Eligibility module components: ● Eligibility Inquiry ● Claims Inquiry ● HIPPA EDI Gateway ● Claims Entry (DDE) ● Payment Inquiry ● Provider Appeals ■ Standards based data exchange protocols via web services utilizing standard EDI X12 transaction sets enabled by Edifecs EDI engine	
Option B	■ Leverage Team CNSI's evoBrix CRM and IVR modules: ● CRM - Siebel COTS solution ● IVR - Avaya COTS solution ■ Leverage our Service Delivery Excellence capabilities for provider support services ■ Leverage existing Provider Call Center infrastructure, staff, facilities, and processes	

Figure 3-1. MT PSM Module Components Approach. Team CNSI's high level approach for delivering the solution and services for each component within the MT PSM module.

Team CNSI will demonstrate in our response that our components, approach, and methodologies will deliver a world class solution and services to DPHHS and other participating states.

3.1 Purpose and Intent

The Montana Department of Public Health and Human Services (DPHHS) is releasing this RFP to procure a Provider Services Module Contractor to support Montana's Medicaid modernization effort, referred to as Montana's Program for Automating and Transforming Healthcare (MPATH). The Provider Services module is part of the overall MPATH program to replace aging legacy components of the Montana Healthcare Programs enterprise.

The intent for this RFP is for DPHHS to obtain a discrete module that aligns with the Final Rule for Mechanized Claims Processing and Information Retrieval Systems as described in 42 CFR 433.111. This module will support specific business objectives within the Montana Healthcare Programs enterprise that are detailed in Sections 3.9 High Level Scope of Work and 3.10 Detailed Scope of Work in this RFP, and will be required to have interoperability with other MPATH modules. Consistent with recent definitions in the Final Rule for Mechanized Claims Processing and Information Retrieval Systems, DPHHS defines a module as a group of business processes that can be implemented through software, data and interoperable interfaces that are enabled through design principles in which functions of a complex system are partitioned into discrete, scalable, reusable components.

Each procured module must meet all of the automation and interfacing requirements included in this RFP. In addition, DPHHS expects Offerors to present solutions that can be easily configured to achieve the outcomes described in this RFP and that will be flexible and adaptable enough to support Montana Healthcare Programs well into the future.

Regulations at 42 CFR § 433.112(c)(2) provide that COTS-related development costs at the enhanced match rate may only include the initial licensing fee and the minimum necessary to install, configure, and customize the COTS software and ensure that other state systems coordinate with the COTS software solution. When responding to a request for the 90 percent FFP rate for a COTS product, CMS will

consider whether the configuration and customization of the product would be kept to minimal levels to achieve full functionality in the most cost- effective manner.

A condition for enhanced funding of COTS software is that customization of the product is minimal. Examples of minimal customization include modification of database interactions to include additional required data elements, processing of state specific but necessary business rules, and modification of interfaces to allow interoperability with existing components or modules. If a COTS product is heavily customized, then the solution may become so unique to that state that other states are unable to reuse it, or that newer releases of that software cannot be easily integrated into the state's system, resulting in a solution that no longer meets the Standards and Conditions criteria outlined in the most current version of MECT.

Team CNSI understands DPHHS' overall purpose and intent for the MT PSM proposal in the context of its comprehensive MPATH program to transforming its healthcare systems. Team CNSI has a strong record of delivering modern and highly automated solutions – most notably with the states of Michigan, Washington, Illinois, and Utah. Our solutions are 100 percent web-based and modular, and meet CMS regulations and guidelines, including MITA, MECT, and the TRA. As a result, modules and sub-modules can be separated and/or combined to fit the needs of states based on the business services required.

Team CNSI's evoBrix platform has been engineered with configuration in mind rather than traditional customization. Our experience in multiple states has shown that more than 80 percent of functionality is re-usable and that our focus should be on configuration and the minimal customizations required for state-specific mandates. Additionally, the applications are web-based, highly automated, data driven, and integrated through our service-oriented architecture (SOA) enterprise service bus (ESB). Our SaaS delivery model focuses on streamlined implementation and operations through our SCI implementation methodology and our cloud operations model.

✓ Offeror has read, understands, and will comply with each requirement in this section.

3.2 Anticipated Risks and Proposed Mitigation Strategies

3.2.1 State Vision

DPHHS management team envision the new Montana Healthcare Programs enterprise to be a means to improve access to healthcare and treatment outcomes for Montanans.

Team CNSI understands and supports DPHHS' vision for the healthcare enterprise. We believe that we have multiple module offerings that will aid DPHHS in achieving this vision. Our evoBrix platform was designed with the CMS Triple Aim principles of Better HealthCare, Better Health, and Lower Cost in mind. Every module within the evoBrix platform supports these principles and in turn supports the DPHHS vision to improve access to healthcare and treatment outcomes for its citizens.

3.2.2 Modularity Business Objectives

The MPATH Program objectives include:

- *An enterprise system that is flexible to quickly adapt to the dynamic, evolving needs of existing programs and support new regulations, policies and innovations*
- *An enterprise system founded on business driven technical solutions*
- *An enterprise system where business processes are automated wherever possible*
- *An enterprise system that provides centralized access to data*

- *An enterprise system that includes data analytics tools to support the use of clinical data to measure treatment outcomes and the changing health status of members.*

- *An enterprise system that includes standardized and automated electronic communication and data exchange capabilities*

- *An enterprise system that includes a Master Client Index (MCI)*

- *An enterprise system that integrates data from disparate systems to enable enterprise wide-program management*

Team CNSI understands the MPATH modularity objectives and our solution is aligned to the DPHHS Enterprise Business Objectives. Figure 3-2 depicts Team CNSI's solution alignment to DPHHS Business Objectives.

Objective	Team CNSI Solution Alignment
Flexibility and Adaptability to Change	■ evoBrix is built with configurability in mind. ■ Modules are highly data driven. ■ Business rules implemented in a configurable rules engine. ■ Users able to control many aspects of their business operations.
Business driven technical solutions	■ Functionality was built from experience gathered in multiple states. ■ Business functionality covers a broad spectrum of business needs across the Medicaid enterprise. ■ Rich feature set represents a broad cross-section of requirements from the Federal and State level.
Business process automation	■ evoBrix modules are highly automated and aligned to business processes that are common to all Medicaid programs. ■ Functionality driven by business processes through analysis rather than driven by technology needs ■ Front-end screens provide rich features for users to access and process information. ■ Back-end processes are orchestrated through our middle layer without user intervention. ■ Extensive automation of processes that link multiple business processes that combine in end to end workflows. These linkages are flexible and can be plugged in and out as needed. For example: • Provider enrollment approval is linked to claims entry/receipt/loading and eligibility inquiry with no manual intervention. This enables providers to enroll and submit claims the same day. • Claims entry/receipt/loading is linked to adjudication then to payment and to RA generation in a completely automated flow without manual intervention or job scheduling. • Eligibility feeds are linked to eligibility inquiry, claims processing, and managed care processing in a completely automated flow without manual intervention, or job scheduling.
Centralized data access	■ evoBrix Integrator enables data exchange across modules via the ESB.
Data analytics tools	■ evoBrix Reporting module provides robust features for generating ad hoc reports. ■ evoBrix Operational Data Store (ODS) provides extensive analytics capabilities.
Standardized data communication and exchange capabilities	■ evoBrix Integrator is based on SOA standards and provides multiple data exchange mechanisms.
Master Client Index (MCI)	■ Experience with Master Client Index (MCI)/Master Patient Index (MPI) integration in multiple states. ■ Flexible data exchange with MCI module via ESB.
Integrated program management across disparate systems	■ Extensive experience with multi-vendor governance structures and processes. ■ Extensive experience with designing and participating in multi-state governance models.

Figure 3-2. Team CNSI Alignment to DPHHS Enterprise Objectives and Guiding Principles. Team CNSI's solution is well aligned to DPHHS Objectives.

3.2.3 Guiding Principles

The MPATH Program team, leadership and program stakeholders have established guiding principles to be considered in all decisions throughout the overall program and module specific project phases to ensure that risks are mitigated appropriately, the procurements are successful, and member and provider communities and other stakeholders encounter minimal negative impacts. Table 3.2.3 illustrates the, guiding principles established to guide the program administration

Table 3.2.3 MPATH Guiding Principles

Guiding Principles	
Flexible Enterprise Technology Platform	*Implement flexible, rule-based, configurable components and services to enhance decision-making, increase management efficiency and promotes agile adaptability for new and evolving regulations, programs, and initiatives.*
Centralized Data Repository	*Implement a centralized data warehouse and associated data analytics tools to enable real-time or near-time access to data, including clinical data and enhanced reporting that meets changing business and management needs.*
Business-driven Enterprise transformation	*Business functions must drive technical solutions and the modular MMIS capability must be flexible to meet future needs, including new regulations, legislation, and innovations.*
Process Automation	*Automate manual processes and eliminate human intervention wherever possible and utilize workflow tools to standardize business processes that guide internal and external users through process steps, activities, and tasks.*
Data Integration and Interoperability	*Promote reusable components by using open architecture and adopting industry and national standards for interoperability, integration, and data exchange.*
Data Consistency Across the Enterprise	*Utilize a comprehensive data governance process to ensure consistent data management processes and policies across the Montana Healthcare Programs enterprise. Provide data that is timely, accurate, usable, and easily accessible to support analysis and decision making for healthcare management and program administration.*
Progressive Technology	*Implement services that will allow the State to take advantage of progressive technology (e.g., access via mobile devices, mobile apps, instant messenger) to improve how it interacts and communicates with recipients, providers, and contractors.*
Member and Provider Centric Focus	*Implement solutions that provide easy to access and comprehensive portal for providers, members, and other stakeholders to promote self-service functionality (e.g., claims status and member eligibility inquiries). The solution leverages role-based security to make sure stakeholders have access to only the information required for their needs.*
Cost Efficiency and Effectiveness	*Implement a solution that supports future State strategies of paying providers based on the quality of services rather than quantity of services, focuses on the member outcomes, and efficiently processes fee-for-service claims.*

Team CNSI understands the MPATH modularity Guiding Principles and our solution is aligned to them as listed above. Figure 3-3 depicts Team CNSI's alignment to DPHHS Guiding Principles:

Guiding Principle	Team CNSI Solution Alignment
Flexible Enterprise Technology Platform	■ The evoBrix platform is a flexible platform of modules and sub-modules that can be configured and combined to meet evolving business needs and adapt to a changing enterprise.
Centralized Data Repository	■ evoBrix supports flexible data exchange through the ESB for feeding ODS and data warehouse repositories.
Business-driven Enterprise transformation	■ evoBrix modules enable enterprise transformation by providing a broad set of services across the Medicaid enterprise. ■ evoBrix module features developed from experience across multiple states and aligned to CMS standards, such as MITA, MECT, and TRA.
Process Automation	■ evoBrix is highly automated and provides rich features with little to no manual intervention required to conduct business operations. ■ Provider Enrollment is a highly automated self-service interface driven by a Business Process Wizard which guides providers through the enrollment process.
Data Integration and Interoperability	■ evoBrix Integrator provides SOA-based ESB integration features to provide real-time data exchange across modules.
Data Consistency Across the Enterprise	■ evoBrix Integrator enables data consistency throughout the Enterprise via real-time data exchange across modules rather than maintaining redundant data stores in each module.
Progressive Technology	■ evoBrix is: ● 100% web based ● Modular ● Data driven ● UX-2014 compliant UI supporting multiple browsers ● SaaS delivered ● FedRAMP hosted
Member and Provider Centric Focus	■ evoBrix Provider modules contain rich features for Provider Self Service. ■ evoBrix Consumer Engagement modules offer industry innovations to inform and engage Medicaid Members. Members can use mobile devices to search for Medicaid providers, view their medical information, update TPL records, request ID cards, and perform many other functions.
Cost Efficiency and Effectiveness	■ evoBrix provides a comprehensive set of features for the Medicaid enterprise. ■ evoBrix achieves efficiencies through: ● Extensive self-service features reduce state operations costs ● Streamlined implementation methodology reduces implementation costs ● Multi-state Operations methodology reduces operations costs ● Cloud infrastructure shared across states reduces implementation and operations costs

Figure 3-3. Team CNSI Alignment to DPHHS Enterprise Guiding Principles. Team CNSI's solution is well aligned to DPHHS Guiding Principles.

As depicted above, Team CNSI's solution is aligned to DPHHS' Enterprise Objectives and Guiding Principles. This alignment is reflected in our responses to each of the high level and detailed scope and requirements.

✓ Offeror has read, understands, and will comply with each requirement in this section.

3.3 Modularity Approach and Blueprint

3.3.1 Modularity Approach

DPHHS has adopted a modularity component/services blend approach to procuring new systems and services to support the Medicaid modernization effort. This approach will result in multiple, strategically timed procurements and implementations. A modular component/services blend approach allows the state to focus on best of breed functionality versus best of suite to meet the "to be" business objectives defined in the Montana MITA 3.0 State Self-Assessment. Montana believes that this approach expands the universe of available vendors as opposed to the traditional monolithic Medicaid Management Information Systems (MMIS) replacement approach. The modularity component/services blend approach is also aligned with the principles behind the Standards and Conditions for Medicaid outlined in the most current version of MECT and further clarified in SMD #16-010. The very nature of this approach promotes modularity, interoperability, aligns with MITA 3.0 Business Results conditions as well as optimizing the state's ability to meet the Industry Standards Condition.

Team CNSI's evoBrix platform is completely modular and is composed of building blocks of modules and sub-modules that can be combined to enable delivery of business services. Our solution meets the Standards and Conditions for Medicaid and is aligned to the MITA architecture. We have been at the forefront of modularity and interoperability in the industry and have operationalized it in the form of our SaaS implementations for the states of Michigan and Illinois. Our SaaS evoBrix platform architecture was reviewed by CMS as part of the Michigan cloud approval process to ensure that it would meet the emerging standards for modularity and interoperability.

3.3.2 Modularity Blueprint

The State developed the MPATH Modularity blueprint through a number of modularity planning and decision meetings with stakeholders, guidance received from CMS, discussions with industry vendors, and through collaboration with other States' Medicaid Programs. In addition to this RFP, there are a number of other procurements planned as illustrated in Figure 3.3.2.1 to replace the Montana Healthcare Programs enterprise. Figure 3.3.2.2 represents the timeline of the overall Medicaid modernization effort.

Figure 3.3.2.1 MPATH Modularity Groups

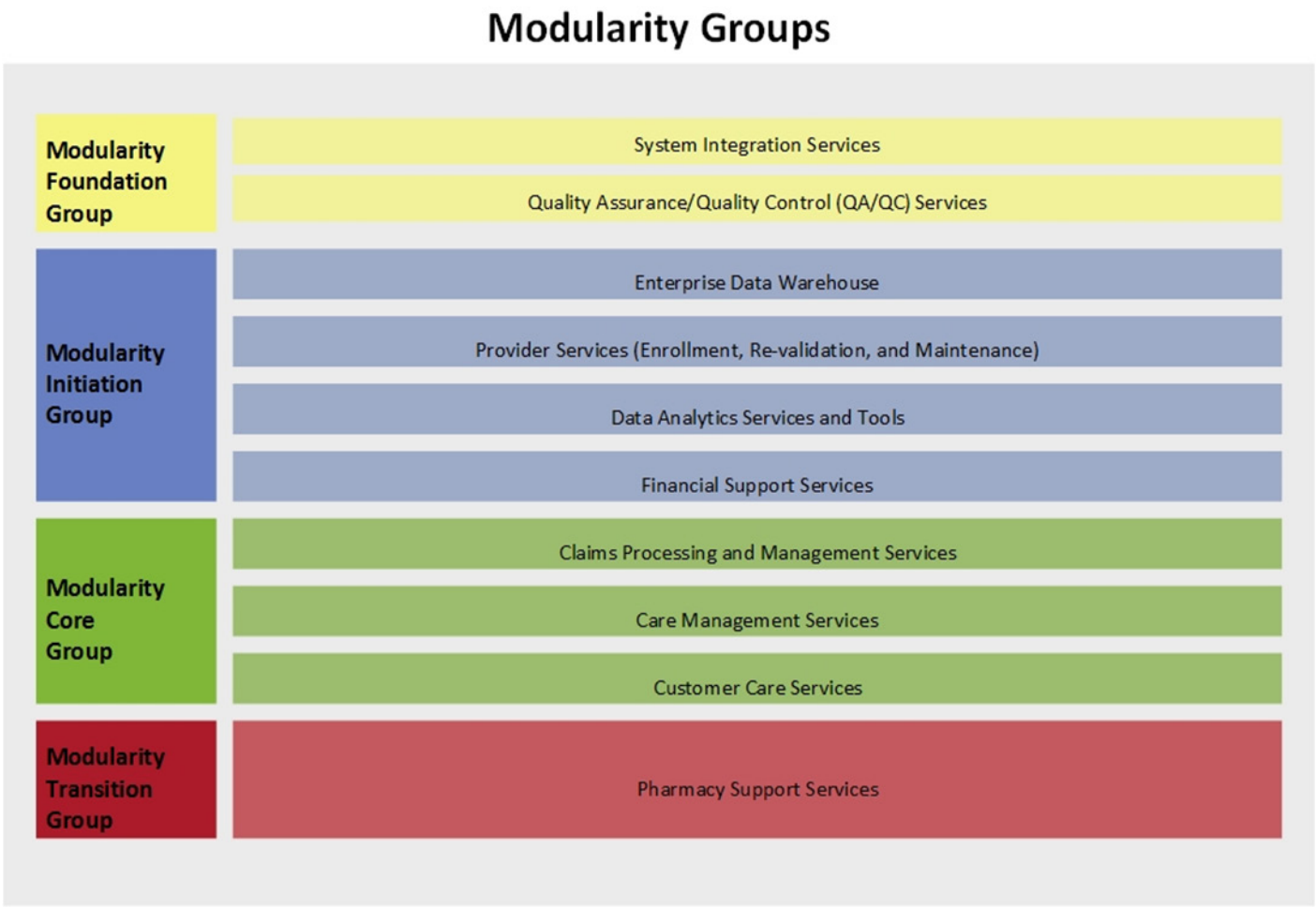
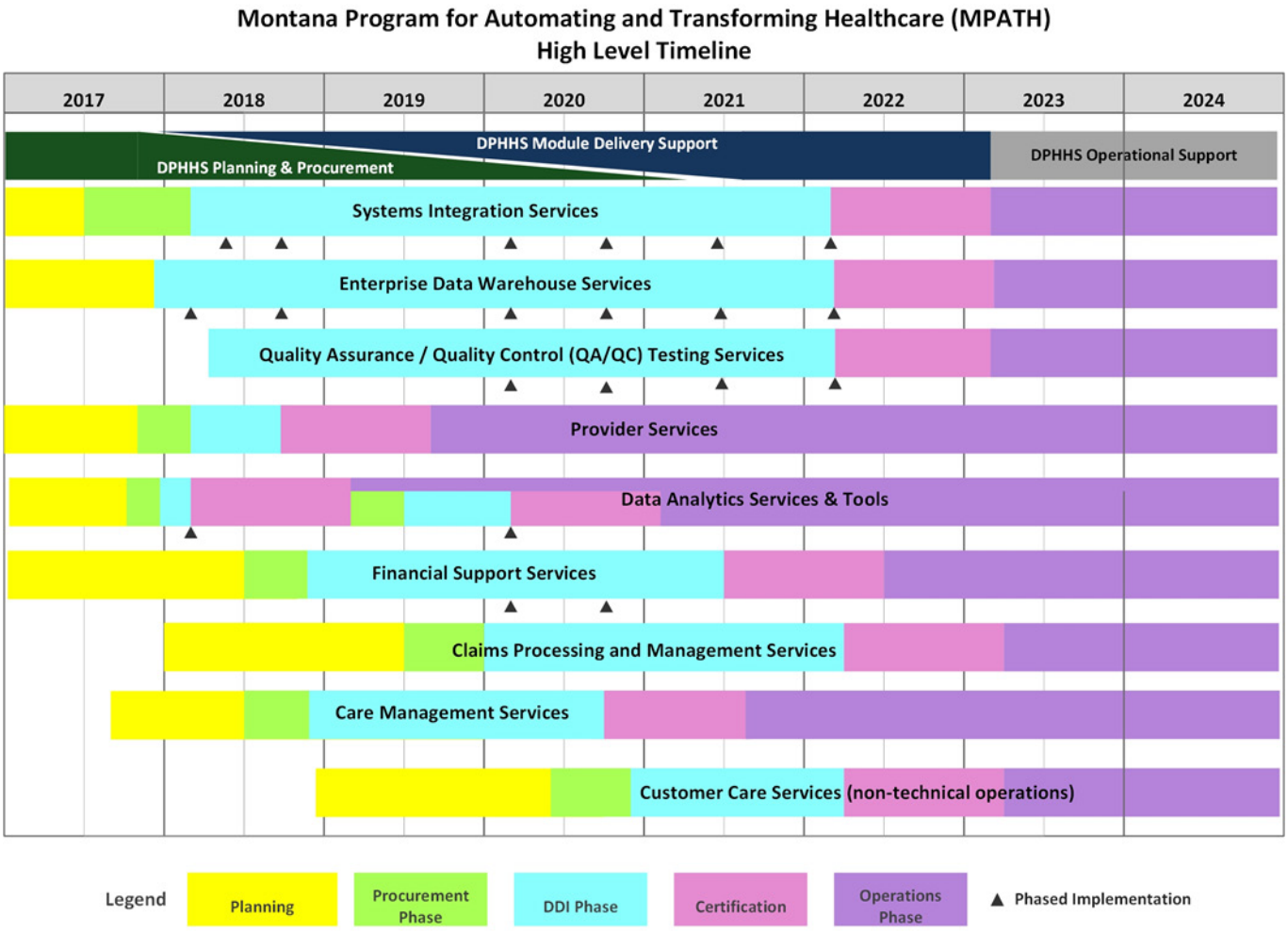


Figure 3.3.2.2 Montana Program for Automating and Transforming Healthcare (MPATH) Modularity High Level Timeline



Team CNSI's module offerings are well aligned to the MPATH vision and road map represented in the Modularity Blueprint. Team CNSI's strength is the delivery of core Medicaid solutions and services. Our evoBrix platform modules are particularly aligned to the below MPATH Groups:

- Modularity Initiation Group
- Modularity Core Group

Figure 3-4 depicts the evoBrix platform modules and sub-modules. It is important to note that all modules depicted are operational in one or more states.



MTPSM-3-319

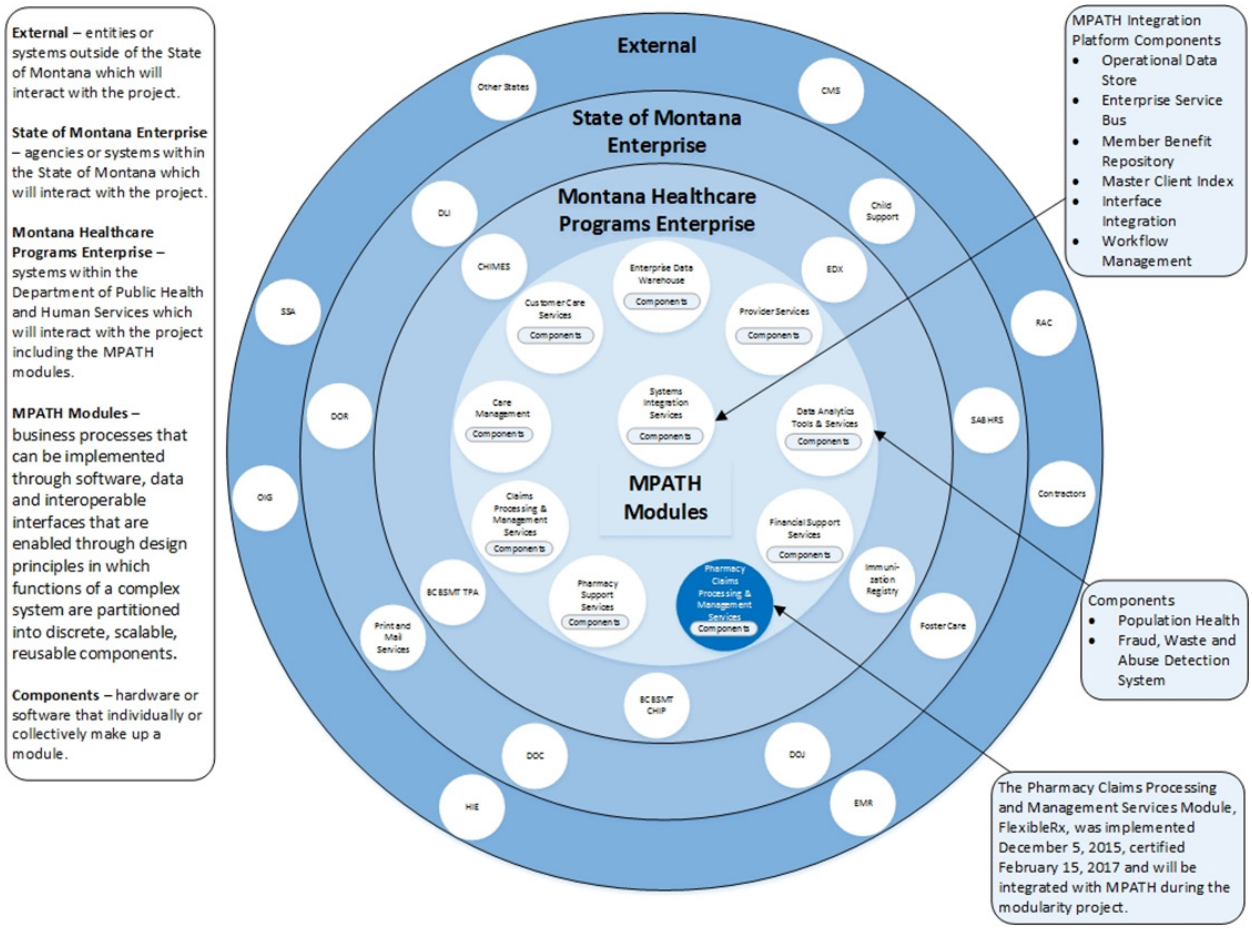
Figure 3-4. Team CNSI's evoBrix Platform. Team CNSI's solution is well aligned to the DPHHS Modularity vision and road map.

Team CNSI's evoBrix platform is well positioned to be an attractive solution for multiple Modularity Groups and Modules within the MPATH blueprint.

3.3.3 MPATH Modules

The MPATH modules and components will be integrated with the overall Montana Healthcare Programs enterprise, the State of Montana enterprise, and other External stakeholders and entities to create standardized, automated electronic data exchanges to enable enterprise wide program management and maximize interoperability through integration. The MPATH Integration Layer graphic in Figure 3.3.3, illustrates the integration/transactional relationships between the MPATH components and modules and the various entities that are related by shared business processes.

Figure 3.3.3 MPATH Integration Layers



Systems Integration Services (SI)

The state will obtain Systems Integration Services. Systems Integration Services will encompass three areas of the modularity technology platform; interoperability and enterprise integration, technical coordination, and the creation and maintenance of the operational data store. The Systems Integration Services Contractor will provide an enterprise technology platform and a diverse and flexible set of integration and interoperability services which are needed to support a variety of infrastructures, applications and technical solutions. The Systems Integration Services Contractor will also provide real-time web based entry and maintenance of member and benefit plan information for select Montana Healthcare Programs and support the receipt and creation of X12 transactions. Finally, the Systems Integration Services Contractor will provide Master Client/Provider Index functionality to uniquely identify and manage members, providers and other entities within the Montana Healthcare Programs enterprise.

Provider Services (PS)

The state will obtain a Provider Services module. The Provider Services vendor will need to provide a modern, web based self-service solution that allows healthcare providers (which includes but is not limited to, physicians, hospitals, nursing homes, pharmacies, home health agencies, personal care workers and durable medical equipment providers) to enroll with Montana Healthcare Programs to provide healthcare services to thousands of Montanans covered by Montana Healthcare Programs. The solution will also allow providers to view and maintain their information on file (e.g., address, licensure and group affiliations) and revalidate their enrollment details online.

Enterprise Data Warehouse (EDW)

The Department will receive Enterprise Data Warehouse Services from the State of Montana Department of Administration (DOA), State Information Technology Services Division (SITSD) to establish an Enterprise Data Warehouse (EDW) for the Montana Healthcare Programs enterprise. The Enterprise Data Warehouse (EDW) will serve as a central repository for all Montana Healthcare Programs Enterprise data and it will provide decision makers timely, accurate and consistent access to information. The EDW will provide integrated program data which will provide the State's Medicaid Program with enhanced abilities to gain insights into outcomes and anticipate future needs.

Data Analytics Services and Tools (DA)

The state will obtain Data Analytics Services and Tools to be integrated with the centralized Enterprise Data Warehouse repository of enterprise data for data aggregation, reporting, and analytics. It will enable the creation of comprehensive statistical profiles of healthcare delivery and utilization by both providers and members. These tools and services will provide comprehensive analytical reporting, budgeting, forecasting, and daily program monitoring.

Financial Support Services (FSS)

The state will obtain a Financial Support Services module. This will translate information received from the various Montana Healthcare Programs systems (including multiple payer systems) and assign DPHHS-defined account coding for integrated financial reporting. It will serve as an intermediary between the Department's payment systems and the State of Montana's Statewide Accounting, Budgeting and Human Resource System (SABHRS) and Accounts Receivable Management System (ARMS). It will support financial transaction processing and reconciliation for both claims and non-claims expenditures. It will support our Third-Party Liability (TPL), Medicare, and Surveillance and Utilization Review System (SURS) activities including recovery and reconciliation.

Claims Processing and Management Services (Claims)

The state will obtain a Claims Processing and Management Services module. This module will support the receipt, adjudication and editing, pricing (using Montana Healthcare Programs approved reimbursement methodologies), and payment for health care claim types including (but not limited to): physician, hospital, outpatient, nursing home, dental, vision, transportation, disability services, mental health, and waiver services. During claims adjudication, this module will also process service authorizations, third party insurance liability, and calculate member liabilities including cost share and cost share coordination between multiple payers. This module will be configurable and flexible in order to support claims processing for multiple programs. Claims will be adjudicated "real-time" and process payments and remittance advice daily (or at an interval determined by the state).

Care Management Services (CM)

The state will obtain a Care Management Services module. This module will support activities to improve member healthcare outcomes and reduce healthcare costs for Montana Healthcare Programs by helping members and caregivers more effectively manage health conditions. The care management module will utilize defined criteria to identify members for specific programs, coordinate care for members enrolled in individual or multiple care management programs and collect and report on treatment outcomes. The solution will need to support member outreach, configurable development of assessments, capturing and monitoring assessments and screenings, treatment plans, authorize services, and incident management and reporting. It will provide comprehensive case management and workflow to track a member's care from inception to conclusion with the tracking of key events being triggered based on the member's condition or type of services required.

Customer Care Services (CCS)

The state will obtain a Customer Care Services module. This module encompasses all aspects of the customer care experience for Montana Healthcare Programs providers and members prior to or following

their enrollment in the Departments healthcare programs. The Contractor is expected to provide a comprehensive suite of services, tools, and systems necessary to promote a positive customer care experience. Provider and member self-service supplemented by call center support is key to a successful and positive customer experience. Provider and member data will be available through a variety of secure customer self-service options such as website, mobile aps, and social media. Real-time account information will be accessible securely using various devices such as computers, tablets, and smartphones. Provider and member self-service options will be available across all platforms and provide a positive, comprehensive and seamless experience for all users.

Pharmacy Claims Processing and Management Services (PBMS)

FlexibleRx, the Pharmacy Claims Processing and Management Services module is an on-line, real time pharmacy claims adjudication system. FlexibleRx was implemented December 2015 as the first legacy replacement module within the Montana Healthcare Programs enterprise. FlexibleRx was certified by the Centers for Medicare and Medicaid Services (CMS) on February 15, 2017. FlexibleRx receives member eligibility and provider information from the legacy MMIS. Claims adjudicated in FlexibleRx are sent to the MMIS for payment generation to providers.

Quality Assurance/Quality Control Testing Services (QA/QC)

In order to ensure the quality and success of the MPATH Program, the state will obtain a Quality Assurance/Quality Control (QA/QC) Testing services vendor. These services will meet Montana's need for comprehensive functional and non-functional testing, integration testing, parallel testing, and user acceptance testing support throughout each phase of the system development lifecycle for each module. The QA/QC Testing Services vendor will utilize testing tools and testing databases provided by the module contractors for concurrent testing and other activities throughout the project.

Pharmacy Support Services (PSS)

The Pharmacy Support Services module (PSS) encompasses two objectives. DPHHS will procure new components to replace the legacy Drug Rebate Analysis and Management System (DRAMS) and Retrospective Drug Utilization Review (RetroDUR) systems. Additionally, in order to reduce the dependency of FlexibleRx, the pharmacy claims processing and management system on the existing legacy MMIS, the current pharmacy claims processing and management services contractor, Conduent will complete enhancements to integrate multiple services including member eligibility, provider, financial transaction processing, and centralized data storage and reporting into the MPATH Integration Platform.

Team CNSI understands the Integration Layer approach as outlined above. Our modular solutions are built to be interoperable with other evoBrix modules or third-party solutions. Our evoBrix Integrator framework provides multiple methods for integration between modules and systems. We also have many pre-built interfaces and extracts for enabling exchange of data between our PMIS module and other modules or systems – most notably Claims and Data Warehouse whether they be legacy or modernized applications.

We acknowledge the critical nature of the SI role in modular procurements. Team CNSI member Noridian has performed this role in other states and we are accustomed to multi-vendor implementations where one or more vendors assume responsibility for managing governance and the data integration hub. This model was successfully employed in Michigan for Medicaid Modernization of Eligibility systems. Over a dozen systems and vendors were involved including our MMIS system. We worked within the governance ecosystem and integrated with the data hub to maintain seamless integration between the MMIS and the other Eligibility systems within the state.

We understand the need for independent QA/QC services and have successfully worked with this model in the past in multiple states. Many states outsource some or all of the activities to a vendor for parallel,

performance, integration, UAT, and business to business testing. We work closely with the QA/QC vendor to ensure consistency and integrity between our testing and that of the QA/QC vendor.

3.3.4 Exclusions

The Montana Department of Public Health and Human Services (DPHHS) will release a number of RFPs for software, components and services to replace legacy Montana Healthcare Programs services and components. Contractors awarded the Systems Integration Services, Quality Assurance/Quality Control Testing Services and Independent Verification and Validation Services contracts are precluded from bidding on any other module within the MPATH Program scope.

DPHHS developed prime contractor and subcontractor exclusions based on the August 16, 2016 State Medicaid Director letter (SMD # 16-010 CMS, RE-2392-F Mechanized Claims Processing and Information Retrieval Systems – Modularity). SMD letter #16-010 directs states to use an acquisition strategy that limits the potential for conflicts of interest Systems Integration Services Contractors may encounter based on their specific scope of services by precluding them from bidding on other functional modules. Additionally, DPHHS identified exclusions for the Quality Assurance/Quality Control Testing Services contractor to ensure independence from any and all module prime or subcontractors.

DPHHS used the following key principles to make exclusionary decisions:

- *Eliminate potential conflicts of interest based on contractor roles.*
- *Minimize the dependence of DPHHS on individual contractors.*
- *Focus on a best of breed replacement strategy rather than a best of suite approach.*

Table 3.3.4 details the mapping of module procurement contractor exclusions for the MPATH Program. The exclusions identified in Table 3.3.4 apply equally to both prime contractors and subcontractors (e.g., if a company is part of the team that is awarded the Systems Integration Services Contract, they are precluded from being able to participate as a prime contractor or as a subcontractor on the Provider Services module or any other MPATH module).

In the event that the Systems Integration Services are re-procured after the award of other MPATH module(s), any successful module(s) prime contractor and their subcontractors will be precluded from a contract award as a prime contractor or subcontractor for the Systems Integration Services re-procurement.

Table 3.3.4 MPATH Contractor Procurement Exclusions

Module Name	SI	QA/QC	PS	DA	FSS	Claims	CM	CCS	PSS	EDW
Systems Integrator (SI)	Open	Excluded	Excluded	Excluded	Excluded	Excluded	Excluded	Excluded	Excluded	N/A
Quality Assurance/Quality Control (QA/QC) Services	Excluded	Open	Excluded	Excluded	Excluded	Excluded	Excluded	Excluded	Excluded	N/A
Provider Services (PS)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Data Analytics, Tools and Services (DA)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Financial Support Services (FSS)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Claims Processing and Management (Claims)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Care Management Services (CM)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Customer Care Services (CCS)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Pharmacy Support Services (PSS)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Enterprise Data Warehouse (EDW)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Legend										
Excluded: Awarded vendor(s) are excluded from bidding on subsequent modules within the overall program.										
Open: Awarded vendor(s) are not excluded from bidding on subsequent modules within the overall program.										
N/A: Not applicable. Service will be provided by the State of Montana Information Technology Services Division.										

Team CNSI understands the rationale for Exclusions as defined by DPHHS to ensure integrity across program modules and avoid any potential conflicts of interest. Team CNSI does not anticipate any issues with the Exclusions as defined in the matrix nor do we believe any Exclusions will apply to us for any MPATH RFPs that we would respond to.

✓ Offeror has read, understands, and will comply with each requirement in this section.

3.4 Technology Standards

The overall goal of the MPATH Program is to implement components and services that improve access to healthcare and treatment outcomes for Montanans. Montana's modularity blueprint is founded on a strategy that utilizes a flexible enterprise technology platform which leverages solutions and services that provide the State of Montana the ability to more effectively meet current business objectives and provide a platform to support the evolving complexities of individuals served by Montana Healthcare Programs. The state intends to utilize commercial off-the shelf (COTS) products and software as a service (SaaS) where possible, to enable an enterprise-wide program management system that utilizes claims and clinical data to measure treatment outcomes, improve the health status of Montanans and reduce healthcare costs. DPHHS will collaborate with multiple vendors to implement streamlined business rules and flexible solutions to meet State and Federal laws, rules and regulations.

DPHHS high level requirements for the MPATH Program are reflected in Table 3.4.

Table 3.4 High Level Requirements for the MPATH Program

Requirements	Requirement Definition
Alignment with the Seven Standards and Conditions	Comply with the Standards and Conditions, set forth by CMS, in order to receive enhanced FFP.
Flexible Enterprise	Utilize enterprise architecture governance process that incorporates MITA

Technology Platform	*standards to accommodate future programs and initiatives.*
Automated workflow management	*Provide centralized, configurable workflow solution that allows for workflow creation, execution and automation.*
Enhance program reporting and data analytics	*Implementation of Data Analytic tools and services to enable accurate, real-time data and reporting that will meet changing business and management needs. The solution should be enterprise centric, which would enable other health care and program data typically not found in an MMIS to support enterprise decision-making.*
Centralized access to data	*Provide real-time and centralized access to members, providers, benefit plan(s), claims, and case management data for the Department's programs including Medicaid, Healthy Montana Kids Plus (HMK Plus), Healthy Montana Kids (HMK) (the state's Children's Health Insurance Program CHIP)), Montana Health and Economic Livelihood Partnership Plan (HELP), Mental Health Services Plan (MHSP), Passport to Health, Patient Centered Medical Home (PCMH) and waiver services. Ability to enhance decision-making and increase management efficiencies.*
Data integration and interoperability	*Provide interfaces and components that are reusable and follow industry and national standards for data exchange. Procured solutions will include exposed APIs for easy integration with other enterprise solutions.*
Standard Communication Protocols	*Standardized protocols for electronic communication will allow DPHHS to move to electronic options for communications using modern services such as Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) including a Web Portal. In addition, standardization will support the ability to provide messaging in Multilanguage and multi-literate formats.*
Progressive technology	*Provide progressive technology, e.g., mobile apps, text messaging, etc., that increase communication venues and encourages member and provider interaction with Montana Healthcare Programs.*
Automate Manual Processes	*Automate a majority of manual processes to replace human interactions with automated configurable business rules.*
Administrative Simplification	*Adhere to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II).*
Mechanized Claims Processing and Information Retrieval Systems Final Rule	*Meet requirements specified in the Mechanized Claims Processing and Information Retrieval Systems (90/10) Final Rule (42 CFR 433), specifically related to configuration and customization of COTS software.*
Standards and Implementation Specifications for Health Information Technology Final Rule	*Modularity approach is aligned with industry standards adopted by the Office of the National Coordinator for Health IT described in Final Rule (45 CFR part 170, subpart B).*
HIPAA and HITECH	*All solutions and services shall be fully compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-1919) and Administrative Simplification (Subset of Title II) requirements in effect as of the date of release for the RFP and with any changes that subsequently occur, unless otherwise noted.* *The Contractor shall sign a Business Associate Agreement, included in the contract, which is subject to HIPAA and HITECH regulations CFR 45 parts 160 and 164.*

Team CNSI's solution is aligned to the requirements above. Figure 3-5 depicts how the evoBrix solution is aligned to each requirement.

Requirements	Requirement Definition	evoBrix Solution Alignment
Alignment with the Seven Standards and Conditions	Comply with the Standards and Conditions, set forth by CMS, in order to receive enhanced FFP.	Platform architecture and design meets all Seven Standards and Conditions.
Flexible Enterprise Technology Platform	Utilize enterprise architecture governance process that incorporates MITA standards to accommodate future programs and initiatives.	Platform built on MITA architecture standards and industry standard best practices.
Automated workflow management	Provide centralized, configurable workflow solution that allows for workflow creation, execution and automation.	Configurable workflow for business process automation.
Enhance program reporting and data analytics	Implementation of Data Analytic tools and services to enable accurate, real-time data and reporting that will meet changing business and management needs. The solution should be enterprise centric, which would enable other health care and program data typically not found in an MMIS to support enterprise decision-making.	Extensive Business Intelligence and Analytics modules and components for real-time reporting across modules. Enables complex analysis combining multiple sources of structured and unstructured data. Also includes predictive and cognitive capabilities for advanced analytics.
Centralized access to data	Provide real-time and centralized access to members, providers, benefit plan(s), claims, and case management data for the Department's programs including Medicaid, Healthy Montana Kids Plus (HMK Plus), Healthy Montana Kids (HMK) (the state's Children's Health Insurance Program CHIP)), Montana Health and Economic Livelihood Partnership Plan (HELP), Mental Health Services Plan (MHSP), Passport to Health, Patient Centered Medical Home (PCMH) and waiver services. Ability to enhance decision-making and increase management efficiencies.	Platform includes many real-time features for self-service and automated business processes across all modules. Our well-structured data model enables effective reporting, analytics, and data exchange of module data.
Data integration and interoperability	Provide interfaces and components that are reusable and follow industry and national standards for data exchange. Procured solutions will include exposed APIs for easy integration with other enterprise solutions.	evoBrix integrator implemented on SOA and ESB technology for flexible integration and data exchange.
Standard Communication Protocols	Standardized protocols for electronic communication will allow DPHHS to move to electronic options for communications using modern services such as Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) including a Web Portal. In addition, standardization will support the ability to provide messaging in Multilanguage and multi-literate formats.	evoBrix Integrators supports multiple protocols including SOAP and REST.
Progressive technology	Provide progressive technology, e.g., mobile apps, text messaging, etc., that increase communication venues and encourages member and provider interaction with Montana Healthcare Programs.	Platform includes innovative and progressive technology such as mobile, cloud, and SOA integration. Groundbreaking Consumer Engagement modules encourage member participation and our Provider Management Information System (PMIS) module includes powerful Provider self-service features.

Requirements	Requirement Definition	evoBrix Solution Alignment
Automate Manual Processes	Automate a majority of manual processes to replace human interactions with automated configurable business rules.	System is highly automated across multiple modules and business processes. Automated system processes can be controlled and tuned through operations management tools.
Administrative Simplification	Adhere to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II).	Solution adheres to Administrative Simplification provisions including but limited to compliance with HIPAA 5010 EDI transactions sets, ICD-10 code sets, and unique identifiers such as NPI, EIN, and HPID.
Mechanized Claims Processing and Information Retrieval Systems Final Rule	Meet requirements specified in the Mechanized Claims Processing and Information Retrieval Systems (90/10) Final Rule (42 CFR 433), specifically related to configuration and customization of COTS software.	Platform is built and delivered as a SaaS solution and is augmented by multiple industry leading COTS solutions.
Standards and Implementation Specifications for Health Information Technology Final Rule	Modularity approach is aligned with industry standards adopted by the Office of the National Coordinator for Health IT described in Final Rule (45 CFR part 170, subpart B).	evoBrix modular solutions are compliant with the published HIT standards.
HIPAA and HITECH	All solutions and services shall be fully compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-1919) and Administrative Simplification (Subset of Title II) requirements in effect as of the date of release for the RFP and with any changes that subsequently occur, unless otherwise noted. The Contractor shall sign a Business Associate Agreement, included in the contract, which is subject to HIPAA and HITECH regulations CFR 45 parts 160 and 164.	evoBrix solutions are fully HIPAA and HITECH compliant. Team CNSI has executed BAAs with all of its state customers.

Figure 3-5. Team CNSI Alignment to DPHHS Technology Standards. Team CNSI's solution is well aligned to DPHHS Technology Standards.

Team CNSI's evoBrix platform meets all the Technology Standards as highlighted above. This is also reflected in our detailed responses to the requirements in the RFP.

✓ Offeror has read, understands, and will comply with each requirement in this section.

3.5 Montana Healthcare Programs Review

Montana Healthcare Programs is a group of programs funded by a combination of federal and state funds that provide health and long-term care coverage to Montanans who meet specified income guidelines, and/or are elderly and/or have certain healthcare conditions, disabilities or illnesses. The term "Montana Healthcare Programs" collectively refers to all healthcare benefit programs administered by the State of Montana in partnership with the federal Centers for Medicare and Medicaid Services (CMS). Montana Healthcare Programs operates under Title XIX of the Social Security Act, Title XXI State Healthy Montana Kids (HMK), State funded Mental Health Services Plan (MHSP), and the Montana Health and Economic Livelihood Partnership (HELP) Act. Montana Healthcare Programs is the state's largest public/private healthcare coverage program and now touches the lives of approximately 20% Montanans. Table 3.5 represents the groups of individuals who may receive healthcare coverage through Montana Healthcare Programs.

Table 3.5 Montana Healthcare Programs Member Groups

Healthy Montana Kids (HMK) coverage may be provided to children who are in the following groups:	
HMK Plus	*Medicaid coverage provided to children up to the age of 19 in families with countable income equal to or less than 143% of the Federal Poverty Level (FPL)*
HMK	*Previously referred to as the Children's Health Insurance Program (CHIP), HMK is administered by Blue Cross Blue Shield (BCBS) of Montana and provides healthcare coverage to children up to the age of 19 in families with countable income equal to or great than 144% of the FPL, up to 250 % of the FPL.*
Standard Medicaid benefits may be provided to individuals who are in the following groups:	
Pregnant Women	*Standard Medicaid benefits may be provided to eligible pregnant women with countable income equal to or less that 157% FPL.*
Families with Dependent Children	*Standard Medicaid benefits may be provided to parents or related caretakers (grandparents, aunts/uncles, etc.) whose countable income is below the Family Medicaid income level (approximately 24% FPL).*
Subsidized Adoption, Subsidized Guardianship and Foster Care	*Children eligible for an adoption or guardianship subsidy through the department are automatically eligible for Medicaid coverage through the month of the child's 21st birthday. Children, placed into licensed foster care homes by the Child and Family Services Division are also Medicaid eligible.*
Former Foster Care Children	*Standard Medicaid benefits may be provided to young adults between the ages of 18-26 that were receiving Medicaid at the age of 18, may be eligible for the Former Foster Care Medicaid program.*
Aged, Blind or Disabled Individuals Who Receive Supplemental Security Income (SSI)	*Standard Medicaid benefits are available for any individual determined eligible for SSI.*
Aged	*Individuals, age 65 or older, may be eligible for Medicaid if their countable income is within allowable guidelines and their resources do not exceed $2000 for an individual or $3000 for a couple.*
Blind/Disabled	*Individuals may be eligible for Medicaid if determined blind or disabled using Social Security criteria, and if their income is within allowable limits and their resources do not exceed $2000 for an individual or $3000 for a couple.*
Breast and Cervical Cancer Treatment	*This program is for women diagnosed with certain breast or cervical cancer or pre-cancerous conditions of the breast or cervix. An eligible woman must be under 65 years old, not have insurance considered to be 'creditable coverage,' meet citizenship or qualified alien requirements, be a Montana resident, and have been screened through the Montana Breast and Cervical Health Program. Countable income cannot exceed 250% of the FPL.*
Medically Needy	*Certain individuals or families whose income exceeds the Categorically Needy income standards, but who have a significant medical need may be eligible for Standard Medicaid benefits. The individual or family is obligated to incur medical expenses or make a cash payment (spenddown) for the difference between their countable income and the Medically Needy Income Level each month. The resource limit is $2000 for an individual, and $3000 for a couple or family.*
Autism Services	*This program provides intensive treatment services for Medicaid members up to age 21 with a diagnosis of autism spectrum disorder or related condition.*
Montana Medicaid for Workers with Disabilities (MWD)	*MWD allows certain individuals who meet Social Security's disability criteria to receive Medicaid benefits through a cost share. The cost share is based on a sliding scale according to an individual's income. MWD resource and income standards are significantly higher than many other Medicaid programs: $15,000 for an individual and $30,000 for a couple; while the*

	countable income limit is 250% of the FPL.
Additional healthcare services	
Medicaid Expansion	*On January 1, 2016, Montana expanded healthcare coverage to thousands of state residents through the Montana Health and Economic Livelihood Partnership (HELP) Act. Individuals who receive healthcare coverage through the HELP Act are either eligible for Standard Medicaid benefits or HELP Plan benefits. Help Plan benefits are administered through Blue Cross Blue Shield (BCBS) of Montana, a third-party administrator (TPA).* *Section 9 of the HELP Act includes provisions to provide health care services for individuals who are in the custody of the Department of Corrections or who are residents by commitment or otherwise residents of the following facilities.* *Montana State Hospital* *Montana Mental Health Nursing Care Center* *Montana Chemical Dependency Center* *Montana Developmental Center*
Mental Health Services Plan (MHSP)	*This program provides state funded benefits for individuals who have severe and disabling mental illness and meet income limits establish by the state but do not qualify for Standard Medicaid.*
Emergency Alien Medical Coverage	*This program provides limited benefits for emergency services such as labor and delivery. Other emergency services may be covered from the time treatment is first given for a condition until that same condition is no longer considered an emergency. These services must be determined an emergency by Medicaid department staff.*
Medicare Savings Program (MSP)	*MSP benefits may be provided to individuals who are low income Medicare beneficiaries.* *Qualified Medicare Beneficiary (QMB) –Medicare premiums, co-payments and deductibles are covered for individuals who have QMB eligibility.* *Specified Low-Income Medicare Beneficiary (SLMB) – Medicare premiums are covered for individuals who have SLMB eligibility.* *Qualified Individuals (QI) – Part B premium payments are covered for individuals who have QI eligibility.*
Montana Waiver Programs	*Montana has a number of waiver programs that provide services to supplement existing Standard Medicaid benefits that include the following waivers:* *Section 1115 waivers* *1115 Plan First* *1115 Health and Economic Livelihood Partnership (HELP) Demonstration* *1115 Basic Waiver for Additional Services and Populations* *Section 1915 (b) waivers* *1915(b) Health and Economic Livelihood Partnership (HELP)* *1915(b) Passport to Health* *1915(b)(4) Montana Big Sky Waiver Case Management* *1915(b)(4) Montana Autism Evaluation Services* *Section 1915 (c) waivers* *0208 HCBS Comprehensive Services Waiver for Individuals with Developmental Disabilities* *1915(c) Montana Big Sky* *1915(c) HCBS Severe Disabling Mental Illness (SDMI)*

Team CNSI has implemented and operated Medicaid Enterprise systems in multiple states. Team CNSI understands that Medicaid is an umbrella for many underlying programs and waivers that implement State healthcare policies and objectives. From our experiences, we have deep familiarity with a variety of Medicaid programs and their associated system components.

Team CNSI has deep experience implementing solutions for a variety of programs including Medicaid, CHIP, and waiver programs across multiple states. We have also played a key role in implementing the Medicaid expansion program in the State of Michigan. Our evoBrix platform's configurability enabled Medicaid business staff to define programs and business rules that supported the expansion. The expansion increased Michigan's Medicaid beneficiary population by over 25% yet the MMIS system was able to scale seamlessly without major system changes or infrastructure expansion.

3.5.1 Montana Healthcare Program Benefits

Montana Healthcare Programs Standard Medicaid benefit plan meets federal guidelines for mandatory benefits. In addition, Montana has chosen to cover a number of other cost-effective optional services. Table 3.5.1 represents some of the services covered by Standard Medicaid (services covered for other programs under the Montana Healthcare Programs umbrella may vary).

Table 3.5.1 Example of Standard Medicaid Covered Services

Standard Medicaid Covered Services	
Inpatient hospital services (excluding inpatient services in institutions for mental disease)	*Durable medical equipment, prosthetics and supplies*
Outpatient hospital services	*Optometric, optician and eyeglasses*
Laboratory and X-ray services	*Transportation and per diem*
Nursing facility	*Ambulance*
Early and Periodic Screening, Diagnosis and Treatment (EPSDT)	*Specialized non-emergency transportation*
Physician & Nurse Practitioner services	*Family Planning*
Podiatry services	*Home and community services*
Physical therapy	*Mid-level practitioner*
Speech therapy	*Hospice*
Occupational therapy	*Licensed psychologist*
Audiology and hearing aids	*Licensed clinical social worker*
Personal care services	*Licensed professional counselor*
Home dialysis	*Inpatient psychiatric*
Federally Qualified Health Centers	*Mental health center*
Rural Health Clinics	*Outpatient Drugs*
Dental and denturist services	*Case management*
Pharmacy	*Institutions for mental diseases for persons age 65 and older*
Home Health	*Indian Health Services (IHS)*

The services are paid by a number of payment methodologies: fee for service, percent-of-charges, Resource-Based Relative Value Scale (RBRVS), Diagnosis Related Groups (DRG), Ambulatory Payment Classification (APC), Prospective Payment System (PPS), Relative Value for Dentists (RVD) and negotiated rates.

For additional information regarding Montana Healthcare Programs, please refer to the Montana Department of Public Health and Human Services Report to the 2017 Legislature available in the procurement library.

Team CNSI's evoBrix PMIS solution supports enrollment functionality for providers that deliver all of the above program services types. We have experience with all of the above program services in multiple states. PMIS solution configurability allows definition of program services and associated enrollment requirements such as specialty, license/certification, and documentation requirements as well as other business rules. The PMIS solution supports ACA compliant, NPI-based, and atypical provider enrollment including performing credentialing and conducting site visits.

The evoBrix Benefits Administration module provides rich functionality for modeling Programs and Associated Benefit Plans. This data can be leveraged in multiple modules across the Medicaid Enterprise to drive payment as well as analytical and reporting functions.

✓ Offeror has read, understands, and will comply with each requirement in this section.

3.6 Montana Healthcare Programs Enterprise

The Montana Healthcare Programs enterprise is comprised of multiple components and services that support activities related to provider enrollment and maintenance, population health management, care management, benefit management, claims adjudication, payments, reporting and other business processes necessary to administer Montana Healthcare Programs.

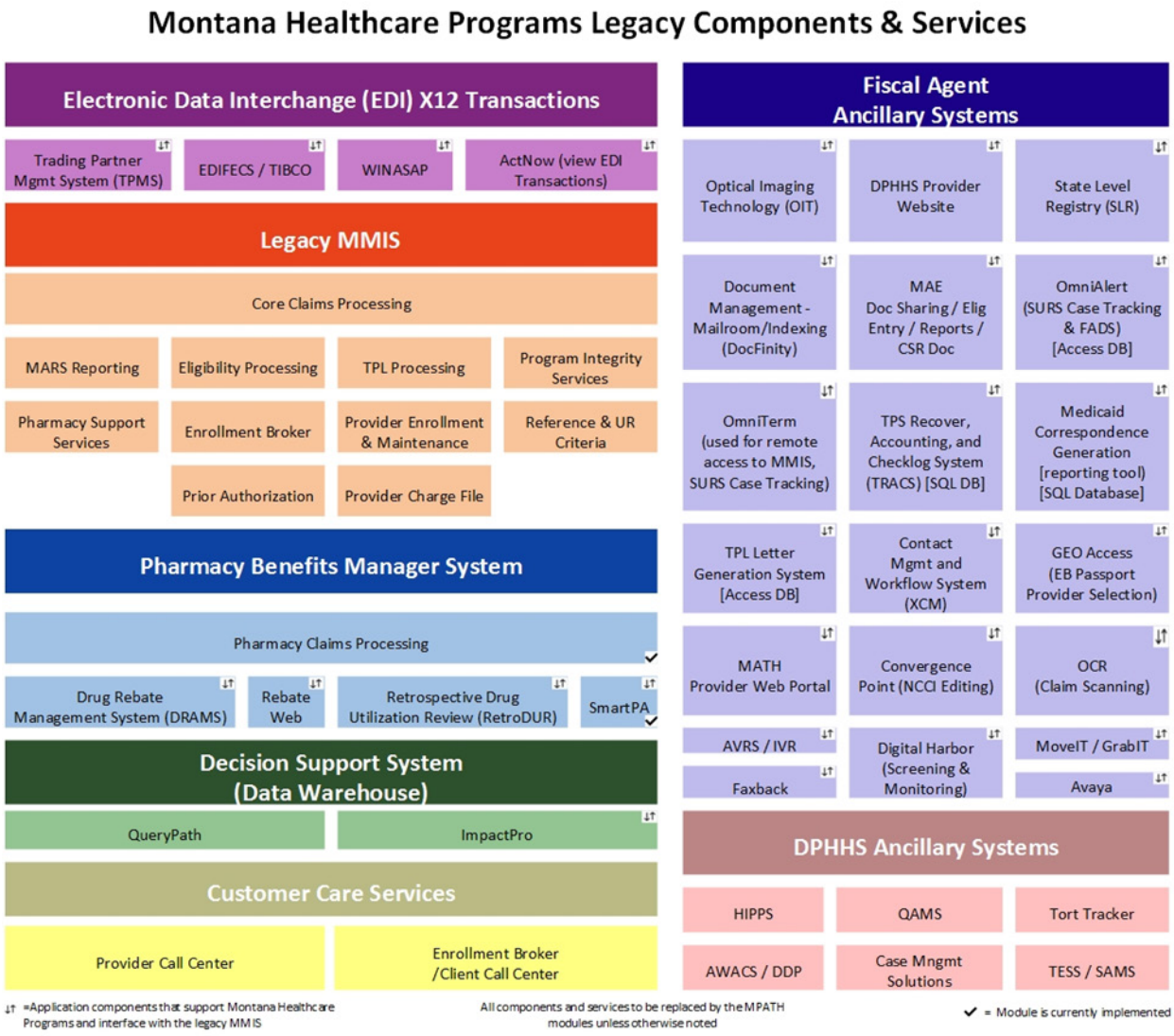
3.6.1 Current MMIS Environment

The current Montana Healthcare Programs enterprise is comprised of a newly implemented pharmacy claims processing system, FlexibleRx, and a compilation of 48 other legacy systems and services.

Montana's core MMIS system is a mainframe Custom Information Control System/Virtual Storage Access Method (CICS v3 r1.0/VSAM v4.2) and utilizes Common Business-Oriented Language (COBOL v4.2) legacy language that has been in operation since 1985. The MMIS was updated in 1997 and certified by CMS in 1998. Conduent is contracted with the State to provide fiscal agent operation services. The State has found it necessary to replace the current MMIS with more modern solutions and services due to the old technology and data integrity of the remaining legacy components. Ongoing system maintenance and enhancements are extensively delayed due to the dated technology and are further impeded by the limited number of knowledgeable resources familiar with the COBOL language.

In addition to the core MMIS, a number of other components are necessary to support Montana Healthcare Programs business objectives. Figure 3.6.1 represents the current Montana Healthcare Programs environment.

Figure 3.6.1 Montana Healthcare Programs Legacy Components and Services



Team CNSI understands the Montana Healthcare Programs legacy environment as depicted above. We have extensive experience migrating and interfacing with legacy systems operating in a variety of technologies from mainframe to modern architectures. Our experiences with legacy systems have led us to develop a series of best practices for identifying potential sources of data and integration. These practices aid us in performing data conversion and interface activities as well as executing migration tasks.

3.6.2 Legacy Components and Services

Table 3.6.2 represents the approximate number of Montana Healthcare Programs Legacy Systems Users.

Table 3.6.2 Montana Healthcare Programs Legacy Systems Approximate Users Count by Component Group

Component	*Users*
Legacy MMIS	*425*
Pharmacy Claims Processing and Management	*120*

Legacy DSS	*225*
DPHHS Ancillary Legacy Systems	*1855*
Fiscal Agent Ancillary Legacy Systems	*550*

Team CNSI understands the current legacy user base by component as depicted above.

3.6.2.1 Electronic Data Interchange (EDI) X12 Transaction Components/Services

Trading Partner Management System

The Trading Partner Management System (TPMS) is the system that is used to create and manage the types of EDI transactions that trading partners have enrolled to submit and receive.

EDIFECS/TIBCO
EDIFECS/TIBCO is the software used to verify the information contained in EDI transactions meet the necessary requirements.

WINASAP
WINASAP5010 is free billing software offered to providers enrolled with Montana Healthcare Programs to create, and submit X12 compliant EDI claims transactions.

ActNow
ActNow is software used by the customer care center to view and research EDI transactions.

Team CNSI has extensive experience with EDI technology in multiple states. We utilize the Edifecs series of products as COTS solutions integrated with our evoBrix platform. We have implemented a comprehensive set of EDI X12 transactions in evoBrix using the Edifecs components. Our Option A response to this RFP utilizes EDIFECS COTS components as a key component of the solution.

3.6.2.2 Pharmacy Benefits Management System Components/Services

FlexibleRx
FlexibleRx, the Pharmacy Claims Processing and Management module is an on-line, real time pharmacy claims adjudication system. Today, FlexibleRx receives member eligibility and provider information from the legacy MMIS. Adjudicated claims are sent to the MMIS for payment generation to providers. FlexibleRx was implemented December 2015 as the first legacy replacement module within the Montana Healthcare Programs enterprise and was certified by the Centers for Medicare and Medicaid Services (CMS) on February 15, 2017.

Drug Rebate Analysis and Management System (DRAMS)
The Drug Rebate Analysis and Management System (DRAMS) is an application which calculates and maintains records of rebate amounts paid for pharmacy claims to provide the necessary data for CMS for reporting on drug rebates.

Rebate Web
Rebate Web is a web based application where drug rebate invoices and associated claim level detail are uploaded for manufacturer drug rebate management.

Retrospective Drug Utilization Review
Retrospective Drug Utilization Review (RetroDUR) uses a member's drug utilization history to create a usage profile which is then used to help prevent instances of drug abuse, misuse, or fraud. This service is currently contracted to Mountain Pacific Quality Health.

Smart PA
SmartPA is a web based service that interfaces with the pharmacy claims processing system (FlexibleRx) and provides prior authorization validation services during adjudication for pharmacy claims.

Team CNSI has experience integrating and interfacing our MMIS solutions with PBM systems in multiple states.

3.6.2.3 Decision Support System Components/Services

Query Path
QueryPath is a secure web-based application used for ad hoc reporting and analysis of Montana Healthcare Programs data stored in the legacy data warehouse.

Impact PRO
Impact PRO is a Windows server/workstation-based application that analyzes Montana Healthcare Programs claims data for predictive modeling purposes to identify and member risk for care management activities.

Team CNSI has experience implementing and integrating with various Data Warehouse, Analytics, and Operational Data Store solutions which provide Decision Support capabilities. Our EvoBrix platform has Analytics and ODS modules including pre-payment predictive modeling and post payment claims analysis modules. We also have pre-built connectors for Data Warehouse and ODS solutions.

3.6.2.4 Customer Care Services

Provider Call Center
The provider call center are fiscal agent services contracted by DPHHS to assist providers with inquires related to enrollment, billing, member eligibility, claims and benefit limits.

Enrollment Broker/Member Call Center
The enrollment broker/member call center facilitates member enrollment into care management programs, assignment of a primary care provider/medical home, conducts outreach, and provides information and education to eligible Montana Healthcare Programs members. Additionally, this service performs provider enrollment outreach and education of the care management programs.

Team CNSI has experience integrating MMIS modules with Call Center and Enrollment Broker systems. The evoBrix platform includes a robust Call Center and IVR solution with integration connectors to Provider, Member, TPL, and Claims modules. Our Option B response to this RFP includes our Call Center and IVR solution built on Siebel and Avaya COTS solutions.

3.6.2.5 Fiscal Agent Ancillary Systems

Montana Access to Health Web Portal
Montana Access to Health (MATH) Web portal is a web based tool for providers to enroll with Montana Healthcare Programs, submit electronic claims, view remittance advices, check member eligibility, view claims based medical history, and as well as other provider self-service activities.

Automated Voice Response/Integrated Voice Response System
The Automated Voice Response /Integrated Voice Response system (AVR/IVR) is a provider self-service tool used to verbally supply member eligibility information, provider payment and claims status.

FaxBack
Faxback is another provider self-service tool used to supply member eligibility information or claims status to providers via fax machine.

Avaya
Avaya is used by the current fiscal agent for automated call distribution and supports customer relationship management.

Digital Harbor
Digital Harbor is a tool used by the current fiscal agent to complete automated provider screening and monitoring activities required by the Affordable Care Act (ACA) for new provider enrollments, revalidating providers and monthly monitoring of all actively enrolled providers.

Optical Imaging Technology
Optical Imaging Technology (OIT) is used by the current fiscal agent to capture, store, and retrieve imaged documentation in electronic form that are stored in a document repository.

Optical Character Recognition
Optical Character Recognition (OCR) software is a tool used by fiscal agent resources to scan claims for automated input into the MMIS.

DPHHS Provider Website
The DPHHS Provider Website is a provider resource, administered by the current fiscal agent that houses provider manuals, fee schedule and notices. Additional resources include; claims and electronic billing instructions, provider FAQs, training, program information, provider newsletter (Claim Jumper) as well as links to the MATH Web Portal and other helpful provider resource information.

DocFinity
DocFinity is used by the fiscal agent for document management which includes document scanning, indexing, searching and viewing.

Montana ACS Extranet
Montana ACS Extranet (MAE) is a secured website, hosted by the fiscal agent that provides a venue for DPHHS and the fiscal agent to view, exchange and store information including reports, reference documentation, formal correspondence and provider communication logs. MAE also serves as an eligibility entry portal for certain Montana Healthcare Programs. Customer service requests (CSRs) and file update requests (FURS) are also managed and stored in MAE.

OmniAlert
OmniAlert provides statistical peer group comparison as a tool to analyze behavior patterns of healthcare providers and members to investigate possible fraud, waste and abuse.

OmniTerm
OmniTerm is a terminal server used to obtain remote access to fiscal agent applications including SURS case tracking, MAE and the MMIS.

Third Party Recovery and Checklog System
The Third-Party Recovery and Checklog System (TRACS) is an SQL database used by the fiscal agent to manage recovery activities such as carrier billing, provider credit balances, member TPL verification work items and trauma letters.

Medicaid Correspondence Generation Tool
The Medicaid Correspondence Generation Tool is a SQL database used by the fiscal agent used to generate Montana Healthcare Programs correspondence to providers and members.

Third Party Liability Letter Generation Tool
The Third-Party Liability (TPL) Letter Generation System is an access database used to generate letters specifically for recovery activities, i.e., credit balance, trauma letters)

State Level Registry
State Level Registry (SLR) is an application used to administer the Electronic Health Record (EHR) provider incentive program.

Conduent Case Management
Conduent Case Management (CCM) is a cloud based workflow automation tool which is also used for contact management.

GEO Access
GEO Access is used by the MMIS Managed Care subsystem to geographically map providers who are near to a member's physical address.

MoveIT/GrabIT
MoveIT/Grab IT is used to provide secure file processing, storage and transfer.

Convergence Point
Convergence Point is the tool used for claim NCCI editing as a part of the claims adjudication process.

Team CNSI understands the Fiscal Agent Ancillary systems as outlined above. We have migrated and/or interfaced with many of the components listed in our existing state Medicaid projects.

3.6.2.6 DPHHS Ancillary Systems

Health Insurance Premium Payment System
The Health Insurance Premium Payments System (HIPPS) is a tool used by DPHHS staff for evaluating and tracking health insurance premium payment activities.

Quality Assurance Management System (QAMS)
QAMS is used to track trends, medication errors, and reporting critical incidents.

Tort Tracker
The Tort Tracker is database utilized by DPHHS staff for third party liability recovery activities.

Agency Wide Accounting Client System (Developmental Disabilities Services)
The Agency Wide Accounting Client System (AWACS) is the system used by the waiver program for case tracking, budgeting, creating and maintaining member plans of care and invoicing.

Case Management Solutions
DPHHS has a number of disparate case management solutions to support current waiver and member care management services.

Shortgrass- *This system is used for overall case management, developing and maintaining plans of care, cost plans and wait lists for two waiver programs.*

Therap-*This system is used for incident reporting.*

The Eligibility Screening System
The Eligibility Screening System (TESS) is used to perform eligibility entry for individuals covered under the Mental Health Services Plan state funded eligibility and Mental Health Services Crisis Stabilization Program.

Substance Abuse Management System
The Substance Abuse Management System (SAMS) is used to track substance abuse treatments and outcomes for Federal Reporting and provider payment.

Web Infrastructure for Treatment Services
Web Infrastructure for Treatment Services (WITS) is a web based application used to collect reporting requirements and manage primary prevention programs for substance abuse prevention and treatment

Team CNSI understands the Montana legacy environment as depicted. We have extensive experience in migrating legacy systems to our modern platforms in multiple states. Some of the key aspects for successful migrations include:

- Data Conversion
  - Begin data conversion activities from the start
  - Conduct exhaustive data source discovery early on
  - Be flexible in data source formats but standardize early on
  - Adopt an iterative approach
  - Focus on data cleansing throughout
- Interfaces
  - Conduct exhaustive interface discovery early on
  - Establish working relationships with internal and external agency interface partners
  - Provide flexibility in interface protocols since many legacy systems have not implemented modern web service architecture
- Provider Outreach and Training
  - Begin outreach early
  - Provide multiple iterations of training
  - Deliver training through the web for the broadest availability and adoption
- Program Governance
  - Establish strong governance early in the program
  - Build well defined communication, status reporting, and escalation protocols
  - Encourage transparency at all program levels

Team CNSI will leverage its experience in legacy migrations to enable successful transitions for DPHHS and other participating states.

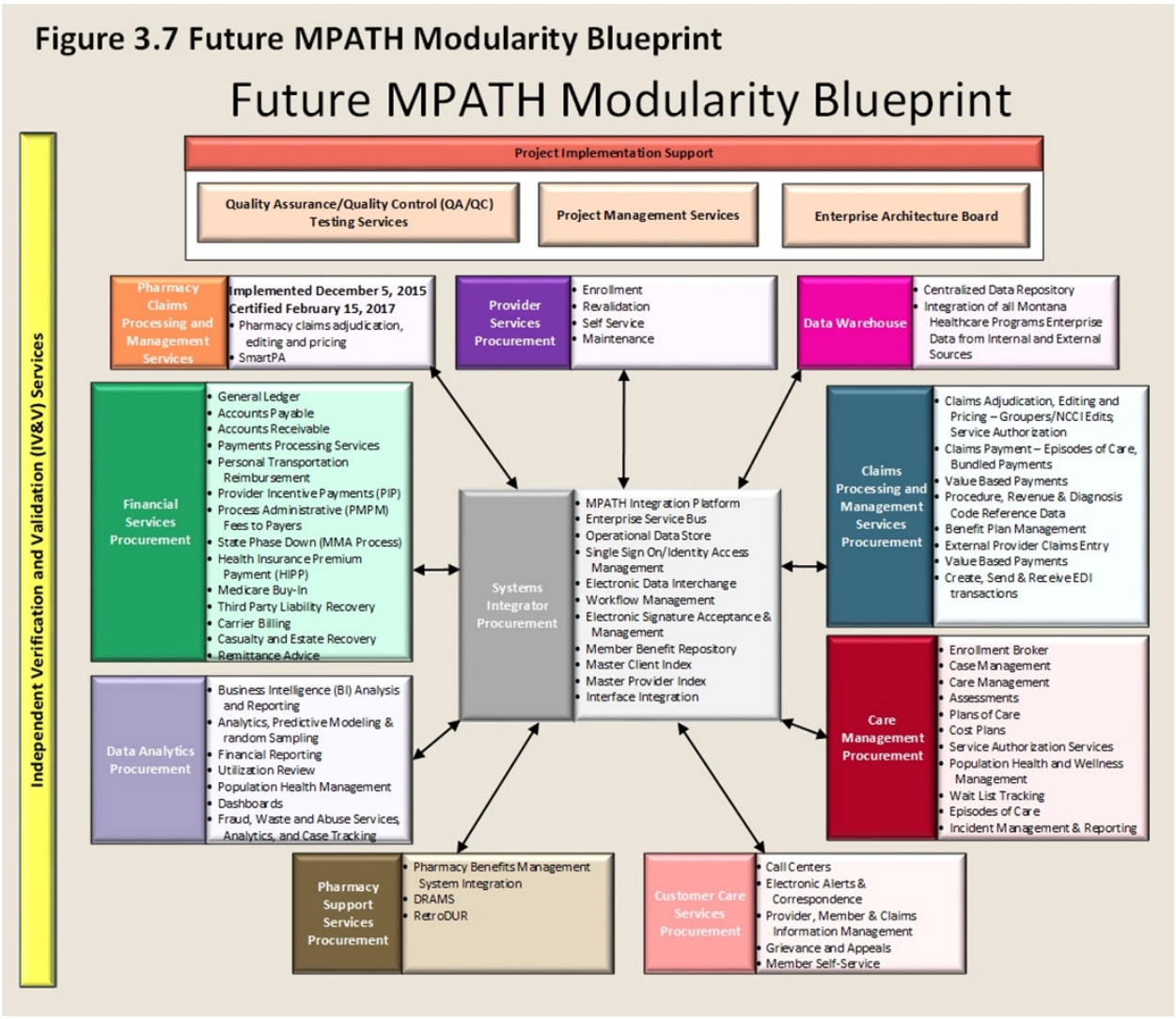
✓ Offeror has read, understands, and will comply with each requirement in this section.

3.7 Future MPATH Environment

The future MPATH environment will be an enterprise framework of integrated systems and services enabled by an enterprise services bus (ESB). The exact composition of the enterprise framework will evolve over time as existing legacy solutions are replaced with more modern, flexible solutions that better meet DPHHS' current and future business needs.

DPHHS will contract with multiple vendors who will each provide a discrete set of components and/or services to support the MPATH modules and components. Each contractor will be responsible to operate and maintain its provided solution and will work with the Systems Integration Services Contractor to integrate the solution with rest of the MPATH Integration Platform. Figure 3.7 below illustrates a high-level view of the to-be future MPATH Modularity Blueprint Environment.

Figure 3.7 Future MPATH Modularity Blueprint



Team CNSI acknowledges the blueprint for the future MPATH environment and is excited to participate in the realization of a truly modular Medicaid enterprise. We have been at the forefront of modularity, multi-state implementations/operations, and SaaS for five years and are well positioned to deliver to this new paradigm, as we have already demonstrated in multiple states.

Team CNSI's evoBrix platform includes a broad set of modules and features for the Medicaid enterprise. Our platform includes modules and sub-modules that can be plugged in and out and integrated with other modules through our evoBrix Integrator framework to enable a high degree of interoperability. Our platform uses a variety of standard protocols such as SOAP and REST as well as flat file interfaces to achieve integration between our modules and/or third-party modules or technology. Our evoBrix platform will provide a stable, high performance, and scalable foundation for all MPATH modules.

Team CNSI's module offerings are aligned with the following MPATH modules:

- Provider Services
- Claims Processing and Management Services

- Care Management
- Customer Care Services
- Financial Services
- Pharmacy Claims Processing and Management

Team CNSI also offers additional value added modules including but not limited to:

- Consumer Engagement – Mobile and web applications for Medicaid members to view and manage their Medicaid information
- ClaimsSure – Pre-payment predictive modeling analytics for claims processing and program integrity
- Audit Studio – Post-payment analytics for claims processing and program integrity
- MCTrack – Managed care compliance analytics and tracking
- eMIPP – EHR incentive payment entry, integration and tracking

✓ Offeror has read, understands, and will comply with each requirement in this section.

3.8 Stakeholders and Governance

3.8.1 Governing Stakeholders

The following stakeholders will contribute to decisions guiding and impacting the MPATH Program

Center for Medicare and Medicaid Services (CMS): CMS is the government entity responsible for authorizing enhanced federal funding for the design, development and installation or enhancement of a state's MMIS. The Mechanized Claims Processing and Information Retrieval Systems (90/10) Final Rule, effective January 1, 2016, expanded the definition of mechanized claims processing and information retrieval systems to include a "System of Systems". This "System of Systems" allows enhanced federal funding for installation or enhancement of open source software, proprietary software, services, shared services, module, COTS software, and Software as a Service (SaaS) that comprise a State's MMIS enterprise. The Contractor and DPHHS will work with CMS and comply with all regulations to ensure the combination of solutions are certified and meet all federal reporting requirements necessary to ensure CMS authorization of enhanced federal funding.

Department of Public Health and Human Services (DPHHS): DPHHS is responsible for the administration of Montana Healthcare Programs and for the administration and oversight of the MPATH modules and components. The following Divisions are directly involved in the MPATH Program.

1. *The Medicaid and Health Services Branch of DPHHS is responsible for contractual administration and Fiscal Agent management responsibilities.*

2. *The Human and Community Services Division (HCSD) is responsible for Member eligibility determinations.*

3. *The Business and Financial Services Division (BFSD) is responsible for the accounting and financial functions of Montana Healthcare Programs.*

4. *The Health Resources Division (HRD) is responsible for overseeing and managing the Acute, Physician and Hospital programs. The care management, Healthy Montana Kids (HMK) and Montana Health and Economic Livelihood Partnership (HELP) programs are also located in this Division.*

5. *The Senior and Long-Term Care Division (SLTC) is responsible for overseeing and managing the Nursing Facility Services and Home and Community Based Services programs.*

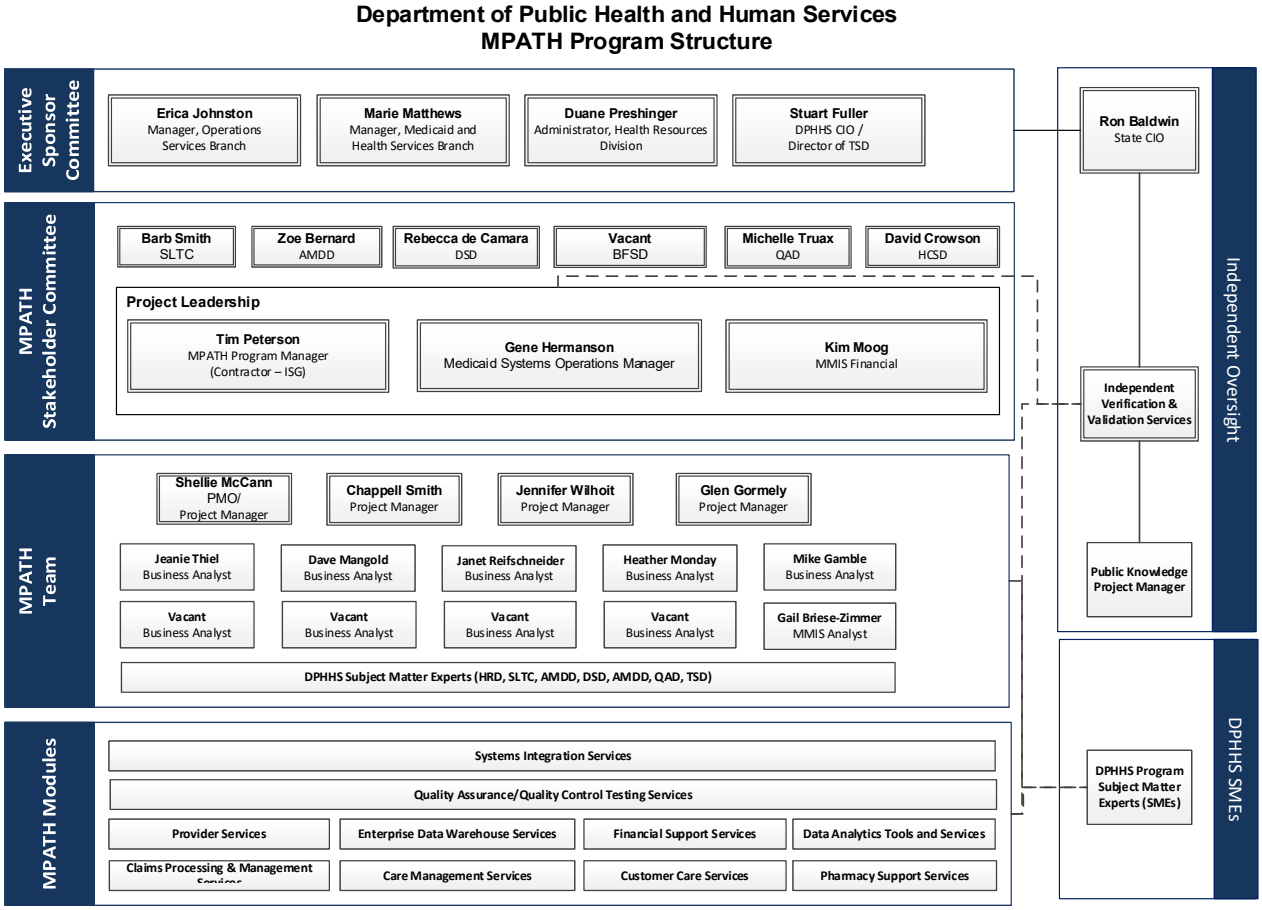
6. *The Addictive and Mental Disorders Division (AMDD) is responsible for overseeing and managing the adult mental health, behavioral health, home and community services, and chemical dependency programs. The State funded MHSP is also located in this Division.*

7. *The Quality Assurance Division (QAD) is responsible for all activities related to Program Integrity and third-party liability programs.*

8. *The Disability Services Division (DSD) does not currently reimburse providers through the MMIS system. However, the DSD will be utilizing the new systems and services procured via the MMIS Replacement Program. This division is responsible for overseeing the Developmental Disability, HCBS waiver and the Children's Mental Health program.*

9. *For additional information on the State programs and a DPHHS organization chart, please refer to the DPHHS website at https://dphhs.mt.gov/Portals/85/Documents/bureauorgchart.pdf*

Table 3.8.1 MPATH Program Structure



Executive Sponsor Committee: *The Executive Sponsor committee members include Erica Johnson, Manager of the Operations Services Branch, Marie Matthews, Manager of the Medicaid and Health Services Branch, Duane Preshinger, Administer of the Health Resources Division, and Stuart Fuller DPHHS CIO/and Director of the Technology Services Division (TSD). The committee's role is to make enterprise wide decisions regarding the modularity program, set priorities, provide recommendations and guidance, and monitor modularity program status and issues.*

MPATH Stakeholder Committee: *The MPATH Stakeholder Committee is made up of the division administrators from each DPHHS division and the MPATH Program leadership. The division administrators advise the MPATH Program Leadership on business requirements, program rules and*

policies. The Division administrators also ensure subject matter experts are available to MPATH DDI Team as necessary to provide detailed insight into specific processes or procedures.

Medicaid Systems Operations Manager: *The Medicaid Systems Operations Manager, Gene Hermanson, administers the Medicaid modularity modernization effort, and will be a primary point of contact for contractual matters, in conjunction with the Program Manager. The Medicaid Systems Operations Manager provides program updates to the MPATH Stakeholder Committee members and supervises the program personnel in addition to the oversight and administration of the MMIS legacy contracts.*

Program Manager: *The Program Manager, Tim Peterson, coordinates each module project across the Montana Healthcare Programs Modularity Program. The Program manager monitors scope, schedule, issues, risks, issues and quality for all module specific projects. The Program Manager is responsible for reporting project status to the Medicaid Systems Operations Manager, the MPATH Stakeholder Committee and the Executive Sponsor Committee. The Program Manager will also oversee the Contract and will be a primary point of contact for contractual matters, in conjunction with the Medicaid Systems Operations Manager.*

MPATH Program Management Office: *The MPATH Program Management Office is comprised of the Medicaid Systems Operations Manager, Program Manager, the PMO Manager and the MPATH module Project Managers. The Program Management Office will meet regularly to review Program status, scope, schedule, issues, risks, and quality and will make recommendations to the DPHHS Stakeholder Committee and the Executive Sponsor Committee.*

Project Governance Team: *For each MPATH module there will be a project governance team comprised of the Medicaid Systems Operations Manager, the Program Manager, and the module specific Project Manager. The project governance team will meet regularly with the Contractor to review project status, scope, schedule, issues, risks, and quality and will make recommendations to the DPHHS Stakeholder Committee and the Executive Sponsor Committee. The project governance team will also be responsible for approving project deliverables and change requests.*

Project Manager: *For each MPATH module, a Project Manager will be designated by the Medicaid Systems Operations Manager to work with the Contractor's project manager to coordinate DPHHS activities related to the project. The Project Manager will be responsible for day-to-day contract administration and ensuring compliance with the contract, monitoring scope, schedules, issues, risks and quality.*

Lead Business Analyst: *For each MPATH module, a lead business analyst will be designated by the Medicaid Systems Operations Manager and Program Manager to work with the Contractors to participate in requirements validation, solution review sessions and other project meetings. The Lead Business Analyst will be responsible for research and provide timely responses to Contractor inquiries and requests, completing deliverable reviews and conducting parallel and user acceptance testing.*

Independent Validation and Verification (IV&V) Contractor: *The State's IV&V Contractor, Public Knowledge LLC., is responsible for assessing project management methodologies and project execution and validates conformance of the product and project to RFP requirements and to the contract. The IV&V Contractor further assists the MPATH Program Management Office in monitoring project schedule, scope, quality, risk and completing MECT milestone reviews and Certification activities for each project.*

Team CNSI acknowledges the broad group of stakeholders for MT PSM and MPATH, and will leverage our compelling combination of solution, process, and organization to successfully deliver solutions and services to all stakeholders. We work closely with both Medicaid and Technology agencies in multiple states to ensure our solutions and processes are providing value to their business and technology teams.

Team CNSI has extensive experience in collaborating with and supporting stakeholders. Our approach is to forge a partnership relationship with our customers that encourages teamwork while maintaining clear lines of responsibility and accountability. We have built strong relationships with our customers by focusing on delivering successful business outcomes. We work closely with PCO and IV&V teams at the project level to ensure smooth interactions with governance organizations. We also spend considerable effort in understanding the technology landscape of each state to ensure that our solutions are aligned to the state's technology standards and can be integrated with other state systems. We continuously monitor changes in state technology policies and proactively update our systems to maintain alignment to those policies.

Our participation in the Michigan Medicaid-as-a-Service (MIMaaS) multi-stated cloud program demonstrates our ability to partner with stakeholders across multiple states. This program involves Medicaid, Budget, and Technology agencies from multiple states and includes many vendors and partners. Team CNSI's role in forging working relationships with all these entities together has been instrumental in the success of the program.

3.8.2 Impacted Stakeholders

The following stakeholders will be directly impacted by the Montana Healthcare Programs Modularity Program:

Members: *The MPATH Program will provide stakeholder-centric solutions that improve outcomes for Montana Healthcare Program members and provide timely and accurate communications to members.*

Providers: *The MPATH Program will provide stakeholder-centric solutions that enable providers to enroll in Montana Healthcare Programs, revalidate and maintain their enrollment information, to submit claims, to receive timely and accurate reimbursements, and to resolve inquiries through self-service tools where possible.*

From a provider perspective, Team CNSI has a strong record for a decade of delivering highly automated self-service solutions for the provider community in multiple states. Our solutions have enabled providers to efficiently manage their Medicaid enrollments, EHR attestations and payments, claims, and prior authorization activities. Our subject matter experts work closely with provider enrollment, support, training, and outreach teams in multiple states to ensure our solutions are meeting the needs of state and provider stakeholders. We are constantly bringing improvements and innovations to our solution to stay ahead of compliance deadlines and achieve greater levels of business efficiency and effectiveness.

From a member perspective, Access to Care is always our top priority. We have built high availability, redundant solutions for Eligibility Inquiry to ensure that our technology is never the reason a member is denied care at the point of service. We also have built ground breaking applications as part of our Consumer Engagement modules which allow the members to view and manage their Medicaid related information. We also provide many helpful tools for members to help improve their healthcare choices and outcomes.

✓ Offeror has read, understands, and will comply with each requirement in this section.

3.9 High Level Scope of Work

The Provider Services solution will replace and modernize provider enrollment and management functionality provided by the legacy MMIS and the Montana Access to Health (MATH) Web Portal. The Provider Services solution will meet Montana's "to be" vision, for the Provider Eligibility and Enrollment, Provider Management, as well as other applicable MITA business areas, detailed in the MITA 3.0 State Self-Assessment found in the Procurement Library.

The Provider Services module will support a web-based self-service tool, for providers to electronically enroll and revalidate provider record information. The self-service enrollment and maintenance portal must be configurable by provider criteria that includes at a minimum, provider role (e.g., ORP, Rendering, Attending, and Billing/Pay-to Providers, Trading Partner) provider risk level, and provider classification (e.g., physician-family practice, physician-oncologist, hospital-acute care, registered nurse-pediatrics) and other required criteria detailed in Attachment F, Requirements Matrix. In addition, the Provider Services module must also support provider maintenance activities for external and internal users that are founded on business process driven workflow automation principles.

The web-based application will collect required information to support decisions regarding approval or denial of a provider's enrollment request. The online application will accept the electronic attachment of supporting documentation and collect required electronic signatures. The solution would leverage integrated automated workflow so that data and documentation are routed to appropriate unit responsible for decisions on provider enrollment applications. In addition, providers may complete periodic updates and revalidation of their enrollment information via the self-service web portal.

The web-based application(s) will adhere to NIST security standards and all federal and state requirements and all laws, rules, and regulations such as HIPAA and the Affordable Care Act (ACA).

The Provider Services module procurement is a multi-state cooperative procurement initiative through NASPO ValuePoint. NASPO ValuePoint® is a cooperative purchasing program among states. This solicitation is managed by a multi-state Sourcing Team, led by Montana. Other sourcing team states include Oregon, South Dakota, South Carolina and Wyoming. As such, there is functionality within the Provider Services module scope that are not required by every participating state. Therefore, Optional Services have been included to be priced separately which will allow each state to determine if the optional functionality and/or services should be included in their specific scope of work. If the Optional Services cannot be implemented with the Core Services without affecting the Core Services timeline, the State may consider adding an additional implementation phase to the Provider Services schedule. Below is a list of the Optional Services detailed further in Section 3.10. Requirements for the base Provider Services Module and Optional Services are also included in Attachment F - Provider Services Requirements Matrix.

Additional Provider Services Option A

- *Self-Service Member Eligibility and Limit Verification Inquiry*
- *Self-Service Claim Status Inquiry*
- *Claims Based Medical History*
- *Upload Files*
- *View/Download Files*
- *Online Provider Appeal Request*
- *Self-Service Primary Care Case Management (PCCM) Member Display*
- *Online access to enter claims*

Additional Provider Services Option B

- *Conduct Provider Site Visits*
- *Include Reference Documentation*
- *Provide Technical Help Desk Support*

- *Provider Services Call Center*
- *Staffing*
- *Collect and Enter State Auditor's Office Financial Information*
- *Provider Services Call Center Management System*
- *Integrated Voice Response System/Automated Voice Response System*

A successful Provider Services solution will provide a variety of self-service options with a seamless end-user experience for Montana Healthcare Programs providers. If the vendor selected for the Provider Services module does not provide the optional services, these services will be provided by the Customer Care Services vendor.

The Team CNSI Advantage

Team CNSI is a trusted partner to Montana; we bring mature processes, industry best practices, and a streamlined SDLC to work with Montana to achieve its project objectives.

- Institutionalized project management processes based on standards and best practices from PMBOK, CMMI, ITIL, and ISO/EIA/IEEE that are fully aligned to the HHSC templates and standards
- Continuous improvement in the processes, products, and services we deliver to the State
- Fully integrated project management methodology and approach with our iVision360 SDLC framework, which covers every task and phase of the project
- Modern, modular, cloud hosted, 100% web-centric automated solution compliant with the latest CMS standards
- Fully-aligned with CMS MITA
- Proven SaaS operations model in over two years of successful multi-tenant operations

MTPSM-3-090

Team CNSI understands that the State seeks a discrete module that aligns with the Final Rule for Mechanized Claims Processing and Information Retrieval Systems as described in 42 CFR 433.111 to help maximize its efficiency and cost effectiveness. Team CNSI also understands that this procurement includes additional services (Option A and Option B) to expand provider self-service capabilities and support states in meeting the needs of their provider communities. Team CNSI offers innovative solutions and approaches based on our extensive experience in MMIS project management, specifically bringing successes and lessons learned from other similar projects, including implementations for the states of Michigan, Illinois, Washington, and Utah. The cloud-based evoBrix PMIS is supporting nearly 420,000 active provider enrollments in a SaaS platform hosted in a FedRAMP Cloud for the states of Michigan and Illinois, and has been in production since July 2015. We are committed to bringing our Medicaid-focused project team, proven project management methodology, and proven solution to satisfy the requirements of the RFP through configuration rather than risky new development. Team CNSI's core approach objectives for the system include the following:

- To leverage our highly configurable, modular, web-centric evoBrix platform, developed specifically for Medicaid programs
- To configure our evoBrix PMIS solution, based on a solution certified by CMS in the state of Michigan, and supporting services to meet the functional needs of Montana DPHHS
- To take advantage of our prior experience and proven system to complete the certification activities specified by CMS as efficiently as possible
- To deliver an automated provider credentialing and site visit tracking platform to improve business performance, reduce manual intervention, and be fully ACA compliant
- To support the State's modularity business objectives and interoperability with other Montana's Program for Automating and Transforming Healthcare (MPATH) modules
- To align with MPATH guiding principles as follows: flexible enterprise technology platform, centralized data repository, business-driven enterprise transformation, process automation, data integration and interoperability, data consistency across the enterprise, progressive technology, member and provider centric focus, and cost efficiency and effectiveness
- To leverage proven business operations that will ensure a low-risk implementation and ongoing support for DPHHS business services for years to come

Team CNSI is proposing the highly configurable, modular, web-centric evoBrix platform to meet the state of Montana's Medicaid Program objectives. Team CNSI's proven evoBrix PMIS provides out-of-the-box configurable provider enrollment business processes to meet the State's requirements while establishing a state-of-the-art framework aligned to Medicaid Information Technology Architecture (MITA) 3.0 and the Seven Conditions and Standards principles. Powered by a business-driven architecture, the solution enables the State to efficiently administer Medicaid provider enrollment, while offering the necessary system agility to meet the demands of state and federal policy.

evoBrix PMIS supports all the processes identified in MITA's Provider Management business process area. Figure 3.9-1 shows evoBrix PMIS functions supporting MITA-identified processes for provider enrollment and disenrollment; management of provider information; multiple functions supporting provider inquiry, including inquiry by business users and other system functions inquiring about the status of providers; and support for provider communications. Figure 3.9-1 also shows a summary of the functions available to providers, DPHHS, and business operations staff.

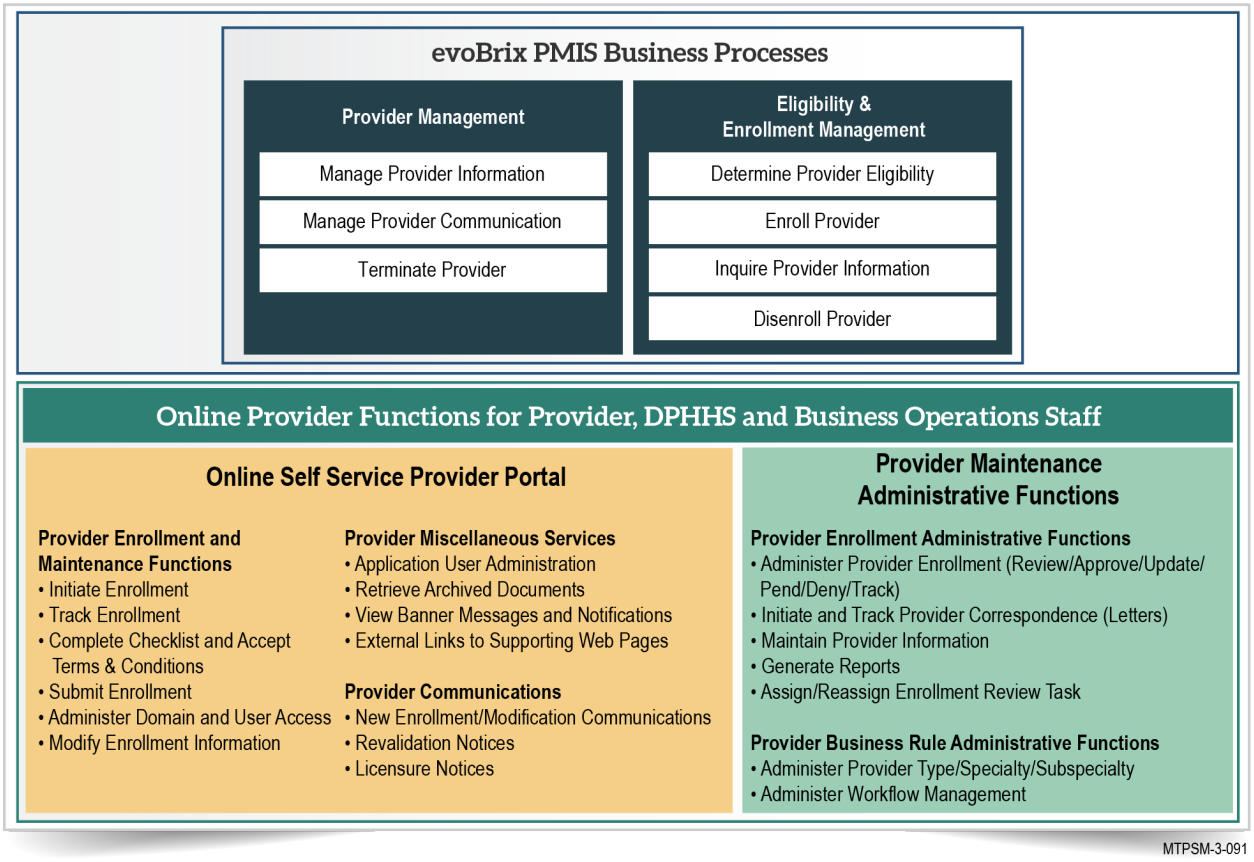


Figure 3.9-1. evoBrix PMIS Business Process Areas. Provider Management business process area architecture shows key interactions and provider information exchange.

Meeting Montana's "To Be" Vision

Team CNSI understands that the DPHHS vision of the new Montana Healthcare Programs enterprise is to improve access to healthcare and treatment outcomes for Montanans. Team CNSI's evoBrix solution brings the technology and proven ability to manage efficient administrative services necessary to achieve this vision. Team CNSI is the recognized leader in bringing cloud technology to the Medicaid market and is the vendor with the proven SaaS implementation and operations experience to support it. Team CNSI

will demonstrate that its solution and delivery approaches will meet DPHHS' objectives and position the state of Montana to deliver best-in-class services to its citizens through effective and efficient provider management.

Team CNSI understands that the state of Montana Provider Services Module (PSM) module is built for implementation to support multiple states. Team CNSI has extensive experience in implementing and operating Provider Management systems in a multi-state, SaaS model. Team CNSI's technology, processes, and organization have already been transformed to deliver services in this evolutionary model. In addition, Team CNSI's evoBrix PMIS solution is configurable for each state, which allows features to be enabled and disabled based on the state's requirements. Adopting this approach enables participating states to implement the features that they need through a streamlined and efficient process.

The cloud-based evoBrix PMIS being offered to Montana was the first in the nation to become fully Affordable Care Act (ACA)-compliant. It is supporting over 420,000 active provider enrollments in a multi-tenant SaaS platform for the states of Michigan and Illinois, and has been in production since July 2015. Team CNSI's evoBrix PMIS provides a rich set of MITA-aligned features for provider enrollment, provider information management, and provider support functions, and will serve to address the State's PSM requirements.

Web-based Self-service Tool

The solution combines a full-featured, secure, self-service provider portal with a comprehensive administrative framework to manage enrollment, disenrollment, revalidation, inquiry, provider information maintenance, and provider support. The solution provides State staff and providers with a full range of online, real-time inquiry and update functions that replace legacy paper-driven processes with web-based data entry screens. The solution maximizes the opportunity to collect valid and complete information throughout the provider's association with the DPHHS. The solution provides a 100 percent browser-based, interactive, and modern PSM supporting the day-to-day business needs of the providers and DPHHS user communities. evoBrix PMIS, including Provider Enrollment, Provider Credentialing Service (PCS), and SiteVisitPro (SVP) modules, is the only true web-centric automated provider enrollment solution with comprehensive provider credentialing service in the State Medicaid market that is in production and running successfully.

The evoBrix PMIS supports the processes identified in MITA's Provider Management business process area that will position DPHHS to meet its objectives, including:

- Online web capabilities for external and internal users including providers. The solution offers the unique provider portal that allows providers to access many services 24 hours a day, 7 days a week (24x7x365). The portal enables providers to enter new enrollment applications, maintain their provider data, and perform periodic revalidations.
- User-friendly, rules-based structure to support provider enrollment and reenrollment policies.
- Configurable Security Framework that provides a secure environment for information management and protects against unwanted loss or disclosure of data using role-based access control (RBAC) method.
- Excellent audit trail features identifying who initiated the change, what changed, when the change was requested, who approved or denied the change, and when was it was approved or denied.
- Outstanding filtering and inquiry capabilities allowing authorized users to search for and retrieve provider information based on user-supplied search criteria.
- Compliance with and use of the National Provider Identifier (NPI) for provider enrollment and automatic assignment of atypical provider IDs for providers who are not eligible for NPIs.

- Fully service-oriented platform with a seamless integration of industry leading COTS products for letter generation, content management, reporting, and enterprise service bus to support the file exchange process.
- Proven automated workflow solution with configurable rules, task routing, assignment, and tracking capabilities to appropriate enrollment unit.
- Configurable enrollment process workflow per state-defined criteria based on role, enrollment type, specialty, and risk category.
- Acceptance of electronic forms, supporting documents/attachments, electronic signatures to collect information to support decision regarding approval or denial of a provider's enrollment request.

Meeting Federal and State Security Requirements

The protection and safeguarding of electronic protected healthcare information (ePHI), requires management, operational, and technical security controls to be fully implemented. Team CNSI's proposed solution is built on a multi-layered security approach that protects the back-end client data at rest and data in transit, complying with security standards, such as FedRAMP, HIPAA, HITECH, FISMA, and NIST, to prevent unauthorized access. Our straightforward approach to regulatory compliance begins at the onset of the solution phase with itemizing all controls; safeguards; applicable local and federal regulations, such as all FISMA and HIPAA regulations; and all applicable DOD, OMB, and NIST standards. We will accomplish this using Trusted Integration's TrustedAgent platform. Team CNSI will use the TrustedAgent platform to provide direct traceability for each regulatory, policy, and control requirement, as well as full transparency for the State's security officer through shared access and reporting. By establishing our compliance framework at the onset of the system's development, we will be able to ensure that security controls and safeguards are integrated into every module of the system from the onset and not just bolted-on after the fact.

Team CNSI's proposed solution is built to comply with provisions of Patient Protection, ACA, and Medicaid Provider Enrollment Compendium (MPEC). The system meets these provisions from the rule published in the Federal Register – CFR 42, Part 455, Subpart E – "Provider Screening and Enrollment" for provider screening, in-state and out-of-state license verification, revalidation, site visits, criminal background checks, and federal database check for SAM (formerly EPLS) and List of Excluded Individuals and Entities (LEIE) exclusions. The system also meets the MPEC requirements, which are the guidelines for State Medicaid Agencies on the implementation of parts and subparts of 42 CFR. In addition, all the updates to the provider information are stored and retained for audit purposes and are accessible based on the State requirements. Team CNSI asserts that DPHHS meets all applicable state and federal requirements for regulatory policy compliance, audit compliance, and security.

The system will:

- Comply with security and safeguard requirements of the following Federal agencies/entities:
  - Health & Human Services (HHS) Center for Medicare & Medicaid Services (CMS)
  - Administration for Children & Families (ACF)
  - NIST 800-53r4, MARS-E, and DOD 8500.2
  - All applicable NIST security guidelines, including but not limited to the below guidelines
    - NIST Special Publication 800-66 Revision 1
    - NIST Special Publication 800-47
    - NIST Special Publication 800-88 Revision 1
    - NIST Special Publication 800-111

- Federal Risk and Authorization Management Program (FedRAMP)
- Internal Revenue System (IRS) Publication 1075
- Center for Internet Security (CIS) Benchmarks for Database v2.1.0
- Federal Information Security Management Act (FISMA) of 2002
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009
- Privacy Act of 1974
- e-Government Act of 2002
- Patient Protection and Affordable Care Act of 2010, Section 1561 Recommendations

- Comply with all applicable State and Federal laws and regulations, including 42 CFR Part 2 and HIPAA, including privacy and client consent for release requirements
- Follow HIPAA standards for the electronic exchange of information between providers and the State
- Conform to and support the Medicaid Information Technology Architecture (MITA) v3.0 or later and align with CMS' Seven Conditions and Standards
- Comply with all applicable State security policies and adhere to all legal, statutory, and regulatory requirements
- Implement security controls in accordance with all federal and state security policy and regulations
- Meet:

  - NIST 800-53A and NIST 800-53 rev4 moderate baseline
  - IRS pub 1075, which points back to NIST 800-53 rev 3
  - NIST 800-53A rev1 guidance and Harmonized Security and Privacy Framework.
  - CMS requirements, which point back to NIST 800-53 rev3 moderate baseline
  - Guidance from CMS including MITA Framework 3.0 and Harmonized Security and Privacy Framework

Additional Provider Services Option A

Team CNSI understands that Option A Provider Services requirements provide flexibility to DPHHS or Agencies who may desire to procure the components or services outlined in Option A as a part of this procurement versus a separate procurement. The proposed solution and our extensive experience in MMIS project management experience is the foundation for the Option A Provider Services:

- Self-Service Member Eligibility and Limit Verification Inquiry
- Self-Service Claim Status Inquiry
- Claims Based Medical History
- Upload Files
- View/Download Files
- Online Provider Appeal Request
- Self-Service Primary Care Case Management (PCCM) Member Display
- Online access to enter claims

Team CNSI's proposed modular and extensible technical architecture provides out-of-the-box features to meet services outlined in Option A. For Option A, Team CNSI will leverage its existing user interface components from the evoBrix Provider, Eligibility, and Claims modules to implement the fully-featured Provider Self-Service module envisioned by DPHHS. The back end of the Provider Self-Service module will be based on standard EDI transactions sets implemented in the Edifecs platform and delivered through the ESB via web services. This innovation will achieve a standards-based interoperability framework between the front-end Provider Self-Service portal and the back-end modules that house Eligibility and Claims data.

Option A – High Level Solution components in Team CNSI's proposed solution as follows:

1. evoBrix Self Service Portal follows responsive web design principles allowing the users to securely inquire eligibility, claims, Remittance Advice data and allow for Direct Data Entry (DDE) of claims.
2. evoBrix Data Translator to convert the JSON business objects accumulated from the web based forms to standard HIPAA transactions. evoBrix leverages industry standard EDIFECS translation engine to achieve desired HIPAA translations.
3. evoBrix Integrator to allow for logging and SOA based integrations with DPHHS System Integrator. Integrator allows capability for the providers to directly submit HIPAA transaction files wherever applicable. DPHHS Integration Hub will receive HIPAA files and return HIPAA responses for evoBrix to consume.

Section 3.10.13, Option A Provider Services provide further details for each of the services.

Additional Provider Services Option B

Team CNSI has partnered with Noridian Healthcare Solutions, LLC (Noridian) to bring mature and scalable CRM and IVR solutions backed by experienced call center operations and business operations teams. Noridian Healthcare Solutions, LLC is a well-known vendor in the Medicaid and Medicare market with a record of service excellence, currently holding the record for national provider satisfaction in Medicare administrative services, and a longtime partner with CNSI. As a trusted partner to CMS for decades, Noridian brings approaches and deep experience interpreting, applying, and complying with complex health care regulations to claims processing operations and key functional areas such as electronic data interchange (EDI), provider enrollment, and customer contact centers. A unique aspect of Team CNSI's solutions is that we have experience with successful implementations in a multi-state environment. We understand the details of configuring multi-tenant, cloud hosted, rules-based solutions specifically for Medicaid programs. Option B requirements includes a combination of requirements that are realized in systems-based solutions, business services, technical services, staffing, and service level agreement (SLA) monitoring and reporting.

Three major solution components that provide the foundation of our business operations to meet the requirements of Provider Services in Option B are: Siebel CRM, Avaya IVR, and evoBrix SiteVisitPro (SVP). These proven solutions are in production and are already integrated with our evoBrix PMIS solution. Our business operations staff establishes a longitudinal record of all provider interactions with CRM and IVR. IVR call trees are designed to rapidly route the provider to the right location. These solutions enable Team CNSI business operations to focus on provider satisfaction and drive to continually improve them based on monitoring calls and interactions with the provider community. We go well beyond contractually defined SLAs to measure our work and eventual customer satisfaction. Efficiency and automation are additional themes of our solutions. Minimizing data entry and automating workflow within our systems enables us to focus on strategic priorities and service delivery. Our business services are standardized and aligned with MITA to provide consistent engagement with the states that comprise NASPO ValuePoint. In addition, Team CNSI's business operations are based on ISO 9001:2015-certified processes.

Section 3.10.14, Option B Provider Services provides further details for each of the Option B Provider Services:

- Conduct Provider Site Visits
- Include Reference Documentation
- Customer Relationship Management (CRM)
- Provider Call Center

- Interactive Voice Response (IVR)
- Staffing
- Collect and Enter State Auditor's Office Financial Information
- Performance Requirements

3.10 Detailed Scope of Work

The Department of Public Health and Human Services (DPHHS) defined the scope of work stated in the Requirements Matrix which is included as Attachment F of this RFP. Unless otherwise noted as Option A or Option B requirements, Attachment F requirements are Mandatory requirements and may only be changed through written approval of DPHHS and the Contractor. The requirements in section 3.10, unless otherwise noted, shall apply throughout the life of the Contract. Additionally, the Contractor's scope of work must be performed within the proposed cost for each project phase as defined in Attachment G – Provider Pricing, Schedule B – DDI Payment Milestones.

Team CNSI has reviewed the detailed scope of work stated in RFP Section 3.10 and the requirements matrix which is included as Attachment F of the RFP, and has described in respective sections our approach to successfully deliver the desired services for DPHHS. Team CNSI understands that these requirements are mandatory and can only be changed through written approval of DPHHS and the contractor. Team CNSI understands DPHHS' objectives for the PSM implementation and is uniquely positioned to deliver the services that support these objectives. Team CNSI will leverage our Solution, Configure and Implement (SCI) methodology to meet DPHHS' objectives through a streamlined service implementation.

CMS has called for a transformation in how an MMIS is built, implemented, and operated, enforcing the adoption of modularity for Medicaid Enterprise Systems. The NASPO multi-state collaboration is an excellent vehicle to advance this vision. Additionally, on a state level, transforming its legacy system to the modular MPATH vision will enable DPHHS to achieve its needs for reduced cost and quicker implementation of system changes to keep pace with the changes in Medicaid regulations by increasing the transparency of its program.

Team CNSI has led the way in multi-state Medicaid Enterprise implementations with our projects in Michigan and Illinois, and we have developed an extensive set of best practices as a result. Team CNSI has used our experience in multi-state implementations and operations to build a robust and scalable service delivery model that can be leveraged for any of the participating states. Team CNSI understands the dynamic nature of the healthcare industry, and is well positioned to manage change effectively and efficiently. Team CNSI has built a strategy for incorporating changes through our Operations phase that eases the burden of states to keep up with changing federal regulations and policies. This is achieved through our evoBrix modular platform architecture, which provides the ability to incorporate these regulations, policies, and standards through maintenance updates across multiple states. Team CNSI's successful track record implementing SaaS Provider Management modules in multiple states in multi-vendor environments provides DPHHS and the other NASPO participating states a low-risk and repeatable option for implementing their Provider Management modules and associated options.

Key highlights of the evoBrix PMIS modular and MITA-aligned platform include:

- Functionally rich Provider Management Information System (PMIS), Option A, and Option B solutions are based on previously CMS-certified modules in State of Michigan.
- Modular and extensible technical architecture that utilizes configuration capabilities, including a rules engine, to enable DPHHS to quickly and cost-effectively adapt to the changing environment of Medicaid
- As a MITA-aligned solution, evoBrix PMIS will enable DPHHS to demonstrate overall alignment to the CMS technology vision and adherence to CMS standards and guidance, thereby fully realizing the business benefits resulting from such compliance
- Individual solution components are Service Oriented Architecture (SOA)-based and loosely coupled to each other, enabling a high level of reuse and interoperability within the DPHHS ecosystem

- As a fully scalable and automated solution, intrinsically designed for high availability, evoBrix PMIS offers a low-risk solution, maximizes business and system performance, and reduces the complexity and cost of operations and maintenance while providing the ability to scale up to support business growth
- Flexibility to modify business rules to support business and policy changes with minimal involvement of developers, greatly improving time-to-market of solutions to meet business requirements

3.10.1 Technical and Information Architecture Requirements

The Systems Integration Services Contractor, will define the common data model, establish the MPATH Integration Platform, including use of the ESB, and provide an inventory of Application Programming Interfaces (APIs) as well as performing other systems integration efforts. Module Contractor(s) must work with the Systems Integration Services Contractor to integrate with the MPATH Integration Platform. The "to-be" technical architecture and supporting technology requirements for the MPATH modules and components are defined in Attachment F, Requirements Matrix.

Montana DPHHS is fundamentally transforming its Medicaid operations through a well-defined vision for a modular Medicaid enterprise solution built around established architectural principles. Team CNSI offers an advanced technical solution through a proven SaaS service delivery model to enable DPHHS to meet its technical objectives and business services needs.

The Team CNSI Advantage

evoBrix is an industry-leading, low-risk solution for delivering business services to Montana DPHHS.

- Modular and modern, extensible architecture
- Service Oriented Architecture (SOA) integration layer for module independence
- Cloud-enabled and deployed with multi-tenancy
- Configurable and rules driven
- Feature rich with input from multiple states
- MITA-aligned
- Numerous real-time features for monitoring, credentialing, and integration
- Responsive UI portals compaitable with various mobile device sizes

MTPSM-3-270

Team CNSI proposes evoBrix, a Modular Medicaid Platform, to serve as the MT PSM solution within MPATH. Team CNSI's evoBrix is fully backed by its solid track record of enabling the states of Michigan, Illinois, and Utah to successfully run provider management functions in a multi-vendor implementation environment. evoBrix leverages a comprehensive set of previously certified components and federally compliant functional modules. As an early adopter of CMS' modularity vision, Team CNSI's evoBrix is cloud- and SOA-enabled, positioning it as the most advanced Medicaid platform in the market.

Key highlights of the evoBrix modular and MITA-aligned platform include:

- Functionally rich Provider Management Information System (PMIS) which is based on the CMS-certified modules in the state of Michigan and Washington
- Modular and extensible technical architecture that utilizes configuration capabilities, including a rules engine, to enable MT PSM to quickly and cost-effectively adapt to the changing environment of Medicaid
- As a MITA-aligned solution, evoBrix will enable MT PSM to demonstrate overall alignment to the CMS technology vision and adherence to CMS standards and guidance, thereby fully realizing the business benefits resulting from such compliance
- Individual solution components are Service Oriented Architecture (SOA)-based and loosely coupled to each other, enabling a high level of reuse and interoperability within the MPATH ecosystem
- As a fully scalable and automated solution, intrinsically designed for high availability, evoBrix offers a low-risk solution, maximizes business and system performance, and reduces the complexity and cost of operations and maintenance while providing the ability to scale up to business growth

- Flexibility to modify business rules to support business and policy changes with minimal involvement of developers, greatly improving time-to-market of business requirements

Team CNSI understands Montana's desire to have a functionally rich business solution supported by a highly flexible and scalable technical architecture. As a MITA-aligned solution, evoBrix will assist PSM as a solution that enables the state to receive favorable treatment for Federal matching funds for implementation and ongoing maintenance. The modular architecture will provide the state with flexible procurement options to leverage the best fit solution.

Team CNSI's solution will follow the standards-based integration approach established through the planned reference technical architecture to be governed by MPATH and managed by the system integrator vendor. Team CNSI will establish a partnership with the State and the MPATH vendors and build a collaborative culture. This will position Montana to realize its enterprise vision and allow for the addition of new business modules and technical components, as future needs emerge.

To create the MPATH modular solution, evoBrix is integrated with several COTS solutions to further enrich its functional and technical capabilities. The COTS-integrated architecture of evoBrix will enable the MPATH solution to integrate with other modules in the MPATH Enterprise environment, such as the Claims Processing and Management System, Shared Fiscal Services Layer (SFSL) Payment System, Offender Management Information System (OMIS), and several other major contracted systems and solutions, based on SOA principles.

Each module and COTS product was carefully chosen to be part of the evoBrix PSM solution based on the business needs and functional requirements in the RFP. However, Team CNSI also looked at the functional capabilities required to meet business objectives and goals that may be necessary over and above what is explicitly requested in the RFP to achieve the intended business outcomes.

Key Capabilities of the Technical Solution

Figure 3.10.1-1 highlights and communicates the key features and related benefits of the proposed MT PSM solution. Montana DPHHS will greatly benefit from the proven, innovative evoBrix solution, as it aligns well with DPHHS' vision to create a modular Medicaid solution focused on business outcomes.

Features and Capabilities	Benefits
Modularity	Maximizes flexible procurement options supported by Modularity Eliminates vendor lock-in
Interoperability	Enhanced interoperability allows for increased information exchange among trading partners and other agencies
Configurability	Rules-based architecture enables changes to business rules through configuration
Accessibility	Ensure enterprise-wide access to services through various access channels
Adaptability and Extensibility	Agility to adapt to changes in DPHHS business and regulatory environment Modules are highly configurable to support evolving business needs with the portfolio of business and technical services
Security	Secured access to information, information exchange, secure communication, protection of privacy, and data security

Features and Capabilities	Benefits
Scalability	Scale up functional and technical capacity based on business demands Support business growth
Alignment to Industry Standards	Leverage business process improvement opportunities through MITA business process maturity

Figure 3.10.1-1. Key Features. Illustrates Team CNSI's proposed Technical Solution's features and their benefits to the State.

Modularity

evoBrix's modularity capability includes:

- Security components and infrastructure that facilitate information exchange, data sharing, and data access in a distributed environment
- Alignment to technology and data standards
- Interoperability and accessibility for information access, ease of integration, and information exchange aligned to service-oriented principles
- Scalable infrastructure architecture, design, and technology components to provide horizontal and vertical scalability
- Business agility driven by a flexible, extensible platform for rapid adoption of changes
- Performance and system monitoring of the modular components at business and technology levels

One of evoBrix's inherent strengths is its modular design for handling changes or system modifications efficiently. The system is highly configurable via the use of rules engines and configurability tools. The modularity and configurability has enabled our customers to adapt to changes as necessitated by mandates, policies, or market needs, as well as the introduction of new programs or modifications to existing programs.

Interoperability

The key interoperability capabilities of the PSM solution are as follows:

- SOA/Standards-based integration approaches using protocols including REST, SOAP, and COTS APIs.
- Support for standard content formats such as documents, XML, JSON, EDI for user- and machine-readable and -understandable content.
- REST APIs leveraging Swagger specifications for producing, consuming, and visualizing APIs. Used to support service inquiries.
- SOAP APIs leveraging WSDL specifications for data exchange with business partners for post services. Versioning through the Mediation layer allows for rapid adoption of change. Web-services-based information exchange for real-time integration capabilities.
- COTS APIs expose COTS functionality as internal and external interfaces through standard APIs. Examples include Document Management API, Workflow API, Correspondence API, and Siebel API.
- EDI gateway support for standards-based information exchange for EDI transactions (e.g., HIPAA ANSI X12 standards). Support for secure FTP gateway. Compliance with CORE rules.
- File-based information exchange for standard and non-standard file based integration.
- Secure information exchange using API keys, web service security 1.0 standards, and other security protocols for ensuring data during transit.

Accessibility

evoBrix Accessor provides multi-channel access to business information for user access and communication through web portals, other devices, and channels. Accessibility services are integrated with security services to ensure that only authorized users are provided with access to secured information. Accessibility layer services leverage the evoBrix UI responsive layout for creating an engaging user experience aligned to usability standards including W3C and ADA guidelines. Key components of Accessor include:

- Portal for internal State/business operations staff
- Provider access through Provider Portal
- Support for multi-channel devices and interfaces including:
    - Web Portals
    - Mobile/Tablet devices
    - Phones/IVR

Adaptability & Extensibility

evoBrix adaptability and extensibility capabilities will allow PSM to add new functionality and modify existing functionality due to changes in policies, mandates, and business needs, providing the necessary agility for the Medicaid enterprise. Key capabilities in this area include:

- Adaptability to business process changes via configurability by leveraging rules-based architecture utilizing our rules engine, RuleIT.
- Adaptation and extensions of business rules, via rules configurator and rule authoring tools.
- Automation of business processes via workflow services.
- Business process configurability and workflow management via workflow enablement tools.
- evoBrix Configurator supports configurability of business process variations and changes and extending business rules via meta-data driven design. Extendible Message Management for application and business messages.
- Configurable user interfaces and services.

Security

evoBrix security framework will be responsible for ensuring secure access to information, information exchange, secure communication, protection of privacy, and data security. Key security capabilities of evoBrix security framework include:

- Protection of health information – Controlled access to data and secure communication. Adequate security controls for existing and emerging threats and vulnerabilities.
- Application Security – Authentication controls including single sign on, identity proofing, two-factor authentication, separation of web layer and application layer via secure deployment, data security in transit via validation and encryption. Authorization controls including role-based access control (RBAC) up to data element level, user account audit, audit trail, and history.
- Data Security – Data at rest and in-transit encryption, Oracle Encryption Technology, and data de-identification (masking).
- Infrastructure Security –All hardware components including servers, switches, storage appliances, backup storage appliances, and firewalls are hosted in HIPAA and FedRAMP compliant data centers that are complaint with most current version of NIST standards.

Scalability

The evoBrix architecture provides application-level as well as infrastructure-level scalability capabilities to support business growth. Team CNSI's private cloud is elastic and scalable to allow for both short-term capacity spikes as well as long-term growth as needs evolve whose key capabilities include:

- Vertical Scalability – Team CNSI's hosting platform supports cloud bursting and it is cost effective. It permits additional capacity usage at a metered rate, when the demand for computing capacity spikes.
- Horizontal Scalability – Team CNSI's hosting platform allows IT resources (infrastructure components), that are of the same type, to be added or removed quickly. This flexibility is because all infrastructure components are build using Platform as a Service (PaaS) services, Infrastructure as a Service (IaaS) services, or SaaS services, thereby creating a highly flexible and elastic environment. Additional PaaS or IaaS services in Team CNSI's private cloud can be subscribed or cancelled to, on an ad-hoc basis, using the "Pay as you go" subscription model.
- Virtualization – Virtualization using Oracle VM with Oracle Linux consolidates servers and provides efficiencies that help to decrease capital and operating expenses. Based on proven Xen hypervisor technology, Oracle VM offers reliability and scalability for enterprise applications.
- Provisioning – Team CNSI's hosting platform are in highly available and scalable configurations rapidly provisioned and ready for use in minutes. Monitoring components for management of virtual infrastructure for application consolidation.
- Availability – Team CNSI's IaaS/PaaS/SaaS based hosting platform allows for scalable configurations to be rapidly provisioned and ready for use in minutes.

Alignment to Industry Standards

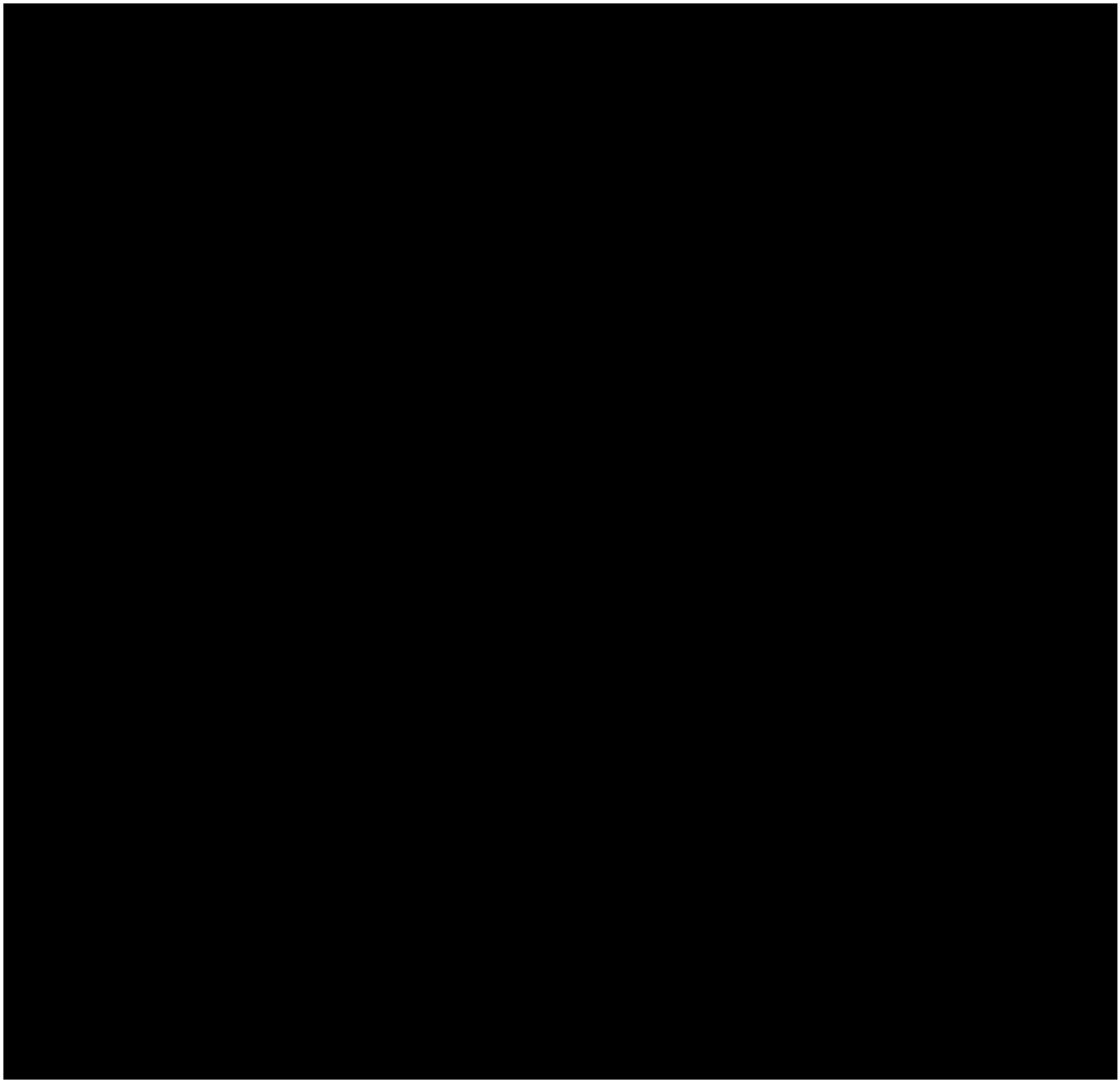
Team CNSI continues to participate in MITA, HL7 standards, and other standards-related forums to promote and adopt standards. The evoBrix solution is aligned to industry standards, including the following key components:

- Data Standards
  - HIPAA X12 standards for EDI transactions and code sets such as ICD10
  - Compliance to CORE Rules and NCPDP data standards
- Interoperability Standards
  - Swagger and WSDL SOAP specifications for web services
  - SOA architecture standards
  - Web service security standards (1.0) for web services security
- Web/Usability Standards
  - W3C Standards
  - ADA guidelines
- Compliance to security, privacy, and data standards
- Alignment to MITA standards
- Adherence to CMS' Seven Standards and Conditions

Technical Architecture View of the Proposed Solution

Team CNSI's proposed solution, was engineered from the ground up based on service-oriented architecture principles, wherein business and functions are available as services across various architecture layers, promoting reuse and interoperability in an enterprise integration environment.

As shown in Figure 3.10.1-2, the evoBrix technical architecture view depicts a layered architecture comprising accessibility services; integration services; technical, configuration, and monitoring services; data and reporting services; and COTS services which operate in a highly secure and interoperable technical environment.



The technical architecture capabilities of the proposed solution will allow for interoperability between the evoBrix solution and the other MPATH modules in the DPHHS enterprise environment. The technical

architecture and design of the solution adopts service-oriented principles for modularity and interoperability, and the core technology components are distributed across various architecture layers as depicted in the following exhibit. Service orientation, interoperability, reuse, and extendibility are foundational to the proposed technical architecture as can be evident from the constructs of the architecture layers. The key service layers and their role as part of the technical architecture are shown in Figure 3.10.1-3.

Services	Service Description
Accessibility Services	■ Includes services that enable user access to various users of the MPATH solution via web portals and mobile devices ■ Responsive UI technology for multi-device, multi-browser support ■ Compliant to web and ADA standards ■ Multi-channel support including web, mobile, Computer Telephony Interface (CTI)
Integration Services	Set of Integration services, Integration gateway, and SOA mediator for enabling service oriented integration between MT PSM and other systems in the DPHHS Enterprise environment through the MPATH system integrator.
Technical Services	Set of services leveraged across the evoBrix modules that ensure standardization and reuse of key technology functions in the areas of configuration services, processing services, technical COTS services, and monitoring services.
Security Services	Includes a core security framework responsible for application security, including authentication, authorization based on RBAC, application data security, audits, and other security controls.
Data Services	Enterprise data repository services that facilitate secure storage and efficient retrieval of enterprise data. Includes highly secure data security components and services.
Reporting & Analytics Services	Includes reporting services and advanced analytics services which can be leveraged across MPATH.

Figure 3.10.1-3. evoBrix Service Layers. evoBrix service layers encapsulate a modular and integrated solution stack.

Base System

Team CNSI understands the State's requirements for a user-friendly, convenient, dynamic, feature-rich portal with extensive self-service functionality for enrollment and maintenance activities. evoBrix PMIS provides a rich set of MITA-aligned features for provider enrollment, provider information management, and provider support functions that will serve to address the State's requirements. The solution combines a full-featured, secure, self-service provider portal with a comprehensive administrative framework to manage enrollment, disenrollment, inquiry, provider information maintenance, and provider support. The solution provides State staff and providers with a full range of online, real-time inquiry and update functions through web-based data entry screens. The solution maximizes the opportunity to collect valid and complete information throughout the provider's association with DPHHS. The solution provides

The CNSI Advantage

Team CNSI's certified implementations in the states of Michigan and Washington will bring the State a proven and mature Provider Management Information System (PMIS).

- evoBrix PMIS is a modern, web-centric provider enrollment and management solution, based on the fully CMS-certified solution in Michigan
- evoBrix PMIS supports both NPI and non-NPI compliant providers
- Rich enrollment options include online enrollment through secure self-service provider portal and offline enrollments through email, traditional mail, telephone or fax to facilitate higher process maturities and provider adoption rate
- Business process wizards powered by rules engine facilitate step-by-step provider enrollment and maintenance process with built-in validation
- One-stop credentialing platform provides improved automation and reduced manual intervention
- Mobile enabled application streamlines site visit processing using a real-time system, eliminating paper

MTPSM-3-021

a browser-based and interactive system supporting the day-to-day business needs of the providers and DPHHS user communities. evoBrix PMIS, including Provider Enrollment, Provider Credentialing Service (PCS), and SiteVisitPro (SVP) modules, is the only true web-centric automated provider enrollment solution with comprehensive provider credentialing service in the State Medicaid market that is in production and running successfully. Figure 3.10.1-4 shows provider enrollment statistics of CNSI's previous implementations of the Provider Enrollment system.

	Michigan	Illinois	Washington	Utah
Enrolled Provider Volume	165,000	255,000	201,000	25,000

Figure 3.10.1-4. Enrolled Provider Volume in CNSI's Previous Implementations. Provider volume range from 25,000 to 250,000 across the four states.

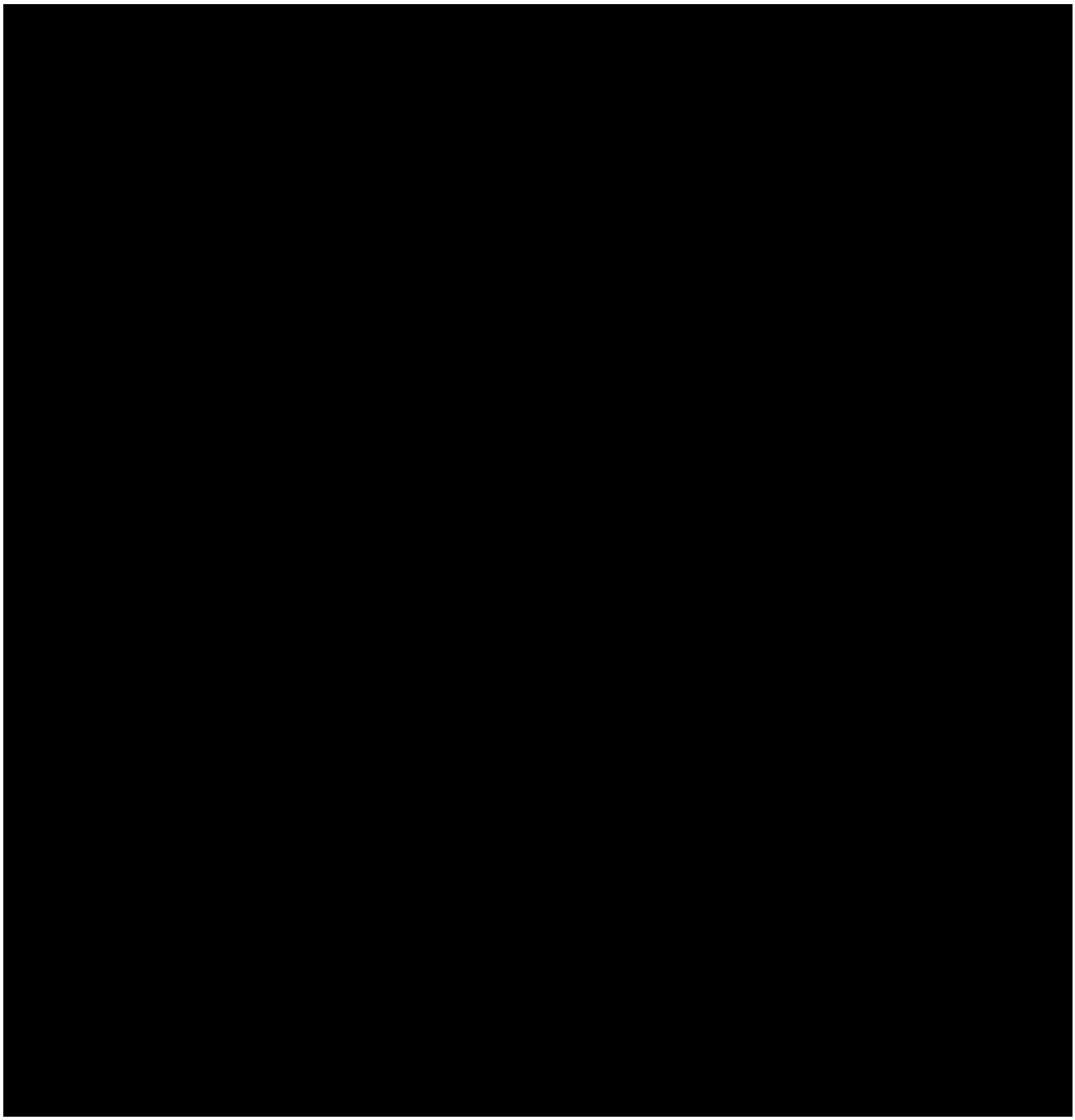
evoBrix PMIS supports the processes identified in the MITA's Provider Management business process area and comes with the built-in capabilities listed below:

- Online web capabilities for all users including providers. The solution offers the unique provider portal that allows providers to access services online. The portal enables providers to enter new enrollment applications and maintain their provider data.
- User-friendly, rules-based structure to support provider enrollment and reenrollment policies.
- Proven audit trail features identifying who initiated the change, what changed, when the change was requested, who approved or denied the change, and when.
- Outstanding filtering and inquiry capabilities allowing authorized users to search for and retrieve provider information based on user-supplied search criteria.
- Compliance with and use of the National Provider Identifier (NPI) for provider enrollment and automatic assignment of atypical provider IDs for providers who are not eligible for NPIs.
- Fully service-oriented platform with a seamless integration of industry leading COTS products for letter generation, content management, reporting, and enterprise service bus to support the file exchange process.

Overall, the evoBrix PMIS module benefits DPHHS by modernizing and streamlining the ability to respond to provider requests and improve customer service. Figure 3.10.1-5 shows the overall evoBrix PMIS business architecture. This figure depicts a summary of the functions available to providers and business operations staff, as well as the various enrollment types supported in the solution. This figure also shows the integration with external systems, evoBrix application security, and COTS products. The evoBrix PMIS module interacts with external systems through an automated communication channel using real-time web-services and file exchange process.

evoBrix PMIS has built-in functionality to allow new user registrations for both providers and State-authorized users, a workflow feature to route new user registrations to authorized State staff for their review, a feature to enforce a password reset policy, functionality to actively monitor user accounts for prolonged period of inactivity for automated locking of those accounts, and functionality to maintain demographic information of all users. The evoBrix PMIS solution also provides functionality that allows State staff to request for security profiles based on their job duties.

evoBrix PMIS offers a configurable Security Framework that provides a secure environment for information management and protects against unwanted loss or disclosure of data. Authenticated access and RBAC enforces security in the evoBrix PMIS solution. The security framework maintains extensive user audit logging for the audit trail in support of HIPAA Security and Privacy. The Security Framework supports role-based security and limits access to users by domain and user ID.



As depicted in Figure 3.10.1-5, the evoBrix PMIS will provide secure access to State users, providers, and other authorized business users via multiple user access channels. evoBrix will integrate with the Access and Identity Management infrastructure in the MPATH environment and provide secure access to all user-facing portals. The functional modules of evoBrix will offer the core business services, which are functionally rich, aligned to MITA, and federally compliant. Each functional module in evoBrix comprises a set of business processes partitioned as discrete, scalable, and reusable components. The modular design and service-oriented assembly of these processes are aimed at promoting flexibility, adaptability, and rapid response to changes to the business needs.

evoBrix, with its SOA-based integration engine, will seamlessly integrate with other systems, external agencies, and business partners in the MPATH's enterprise environment via the System Integration platform. The MPATH System Integration Platform will be leveraged for establishing bi-directional integration with other systems, trading partners, data providers, and data consumers as needed to achieve the desired modularity Montana has envisioned.

Option A Provider Services

Team CNSI is pleased to participate and provide the Option A solution for MT PSM. Team CNSI's configurable evoBrix platform out-of-the-box modular design is engineered to augment the Provider services solution that DPHHS is optionally seeking to procure. solution successfully and making modularity and interoperability vision of DPHHS a reality.

The Team CNSI Advantage

Team CNSI's evoBrix PMIS is a comprehensive solution based on proven technologies.

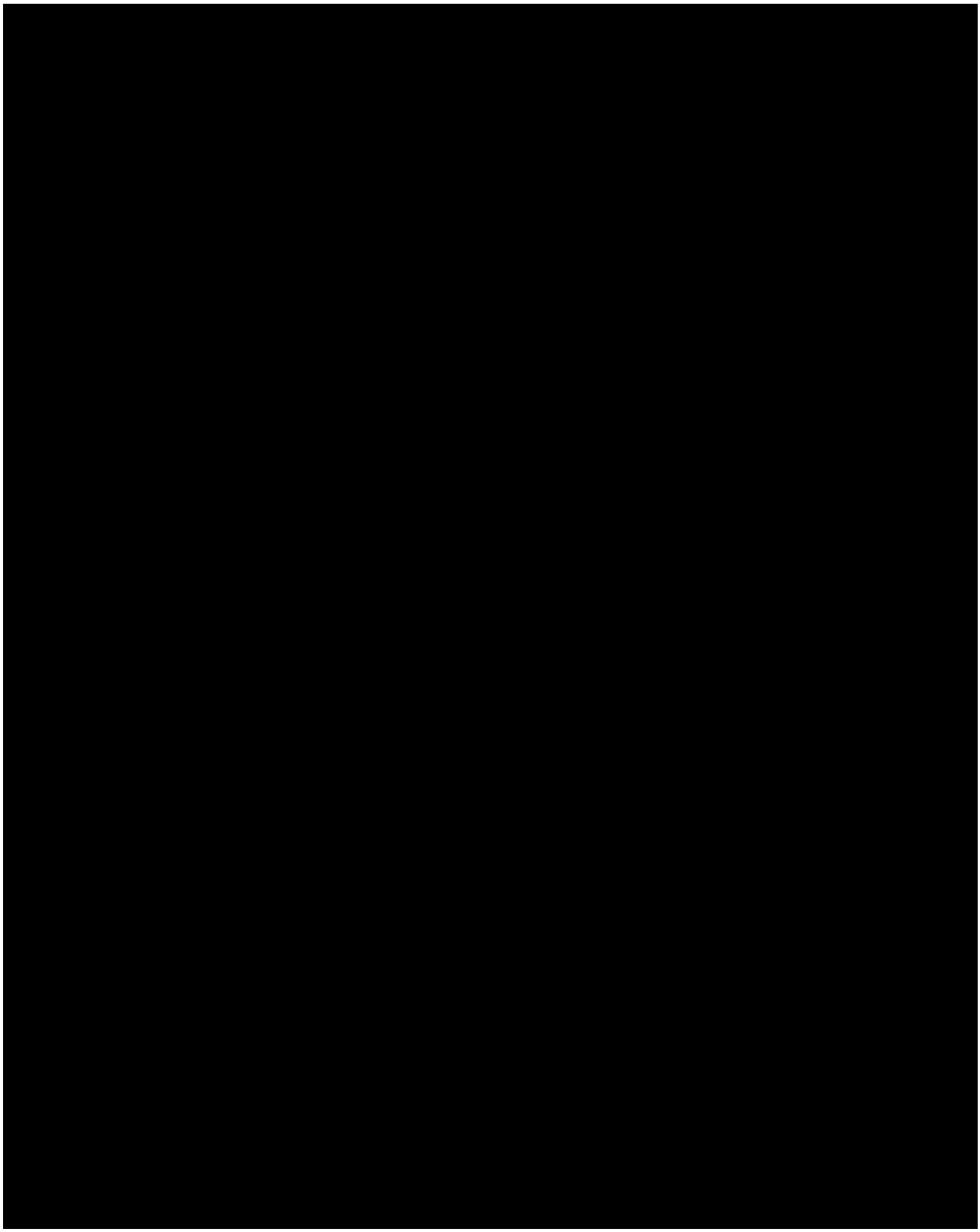
- Alignment of proposed solution's modular and interoperability capabilities with that of the needs of Montana DPHHS enterprise environment
- Functionally rich claims and business related services
- Business enabling services to support claims and provider related services and support functions
- High degree of information exchange capabilities between evoBrix PMIS and other data providers/consumers
- Proven experience working in a multi-vendor environment will reduce implementation risks for the State

MTPSM-3-269

Following are the salient features of the evoBrix platform that will help provide DPHHS achieve desired integration with their as-is or to-be DPHHS MMIS modules:

- Micro-services architecture enabling plug-and-play features that will help integrate evoBrix with the ESB.
- evoBrix Translator translate EDI standard based transaction to JSON and vice-versa.
- Validation of EDI transaction files. Validations will be performed as a service request to the DPHHS vendor system responsible for processing the specific transaction. The requests will be routed via the evoBrix Integrator.
- Modularity enabled by the micro-services architecture as described above.
- Standardized HIPAA transaction support. evoBrix out-of-the-box provides support for HIPAA X12 transactions by leveraging Edifecs translation engine.
- In flight transaction translation thereby providing real-time downstream data push.
- evoBrix Integrator provides auditing framework for logging all requests and responses thereby meeting all auditing requirements.
- evoBrix's Integrator supports integration protocols as requested in the INT86 (Attachment F requirement).
- evoBrix Responsive web design providing all the capabilities to support web based queries and allow for Direct Data Entry (DDE). Dynamic on screen validations are performed during DDE in evoBrix self-service portal.

Figure 3.10.1-6 illustrates evoBrix's high level solution architecture supporting Option A requirements and how it will achieve the integration with DPHHS MMIS modules.



The proposed solution achieves real-time operation by leveraging SOAP and REST web services, which has the potential to transform MT PSM into a real-time enterprise. In fitting with the MT PSM enterprise

service bus vision, our proposed solution's REST API or SOAP services would be exposed through MPATH ESB for consumption by relevant trading partners. Team CNSI's evoBrix solution offers a secured channel access to business information for user access and communication via self-service web portals.

- **Self-service Portal**: CNSI's evoBrix solution offers self-service portal for the provider community developed with W3C Web based standards. The rich user interface is designed to work on most commonly used internet browsers. The portal is designed with a UI framework that has different tiers for business logic and content representation, and also has Responsive UI to show different layouts on various device sizes (e.g., tablets and smart phones). It is designed and developed to be robust and highly scalable, as it is accessible through the public internet where multiple users may access it at any given time.

  Team CNSI's evoBrix self-service portal will integrate with the State's existing Identity and Access Management (IAM) infrastructure to provide a seamless IAM experience for the provider community. This solution will provide the ability to identify users in different contexts, such as time, day of week, location of access, and type of access method, allowing State policies and user preferences to be applied consistently across system. Our solution will employ Oracle Access manager to provide integration with the MPATH System integration platform. It will consume identities provided by MPATH identity provider. The identity federation will use SAML 2.0 and OAUTH. Figure 3.10.1-7 describes various services included in the self-service portal.

Self-Services	evoBrix Capability	evoBrix Technology Component
Member Eligibility Inquiry	■ Allow providers: to enter query via the evoBrix User Interface screen to view query results	Self-service portal's Direct Data Entry web forms, translation services converting request to a HIPAA 270 transaction. Self-service portal capability to consume 271 response HIPAA transaction from System Integrator
Claim Status Inquiry	■ Allow providers: to enter query via evoBrix User Interface screen to view query results	Direct Data Entry inquiry from the User Interface, translation services converting request to a HIPAA 276 transaction. Self-service portal capability to consume 277 response HIPAA transaction from System Integrator
Warrant and Remittance Advice Inquiry	Allow providers: ■ to enter query via evoBrix User Interface screen ■ to view query results	Direct Data Entry inquiry from the User Interface, translation services converting request to a custom webservice transaction. Self-service portals capability to consume and translate 835 HIPAA transaction responses from System Integrator
Claims Based Medical History	Allow providers: ■ to enter query via evoBrix User Interface screen ■ to view query results	Direct Data Entry inquiry from the User Interface, translation services converting request to a 276 HIPAA transaction. Self-service portal capability to consume 277 HIPAA transaction from System Integrator
View, Upload and Download HIPAA Compliant Healthcare Transactions	Allow providers: ■ to submit HIPAA batch transaction requests ■ Web service batch HIPAA transaction submission ■ HIPAA data download capability	Self-service portals HTML File upload capability Self-service portals web service batch file submissions. Self-service portals evoBrix standard data translation controls like excel, pdf, csv download features
Online Provider Appeal Request	Allow providers: ■ to request appeals ■ route the request to the appropriate user/unit ■ to view status of appeals	Direct Data Entry from the User Interface request translated to a custom web service request. Self-service portal workflow capability leveraging configurability. Self-service portal web form to display status of appeals.

Self-Services	evoBrix Capability	evoBrix Technology Component
PCCM Member Inquiry	Allow PCCM providers: ■ to query PCCM members ■ to download and view PCCM member registries	Direct Data Entry inquiry from the User Interface, translation services converting request to a custom web service transaction. Self-service portal web form capability to view PCCM member data.
Online Claims Entry	Allow providers: ■ to submit claims via user interface	Direct Data Entry using web forms, translation services converting to HIPAA 837.

Figure 3.10.1-7. Option A-Specific Requirements. Table highlighting how evoBrix technology components will address Option A-specific requirements.

evoBrix Translator: Team CNSI's evoBrix Translator converts the web based form data accumulated in the form of Business Objects (JavaScript Object Notation [JSON]) to standard HIPAA transactions by leveraging Edifecs translation engine. In similar fashion, it also converts standard HIPAA transaction to respective Business Objects (JSON) to be displayed in self-service portal. This component also utilizes Edifecs XEngine capabilities to achieve validations and translations to HIPAA standard transactions. Edifecs XEngine Server delivers unparalleled performance to validate transactions for syntax, semantics, and custom business rules, thereby ensuring operational integrity of information exchange with trading partners. Edifecs XEngine Server's enterprise-strength throughput capabilities enable fast and accurate validation of transactions at the edge of the enterprise. By catching errors early, XEngine Server can separate good data from bad data, thus allowing organizations to comply with legislative and company mandates. Good data can be further split into smaller logical units for efficient processing and routed to multiple downstream systems, based on the contents of the transaction.

evoBrix Integrator: Team CNSI's evoBrix Integrator will support automated data exchanges with various MMIS business process areas and interface partners. The evoBrix Integrator architecture uses an enterprise-class service bus (Oracle SOA Suite) as the core orchestration tool of business processes across the different applications that support Medicaid operations. The solution can scale for growth in data volumes and transaction volumes seamlessly, and can take advantage of the rich features of the underlying hardware and software resources. The solution can be configured to meet the data transfer needs as per DPHHS requirements.

Team CNSI also supports data trading with MMIS modules in real-time via evoBrix Oracle Service Bus (OSB) web services. The evoBrix architecture uses an enterprise class service bus (Oracle Fusion SOA) as the core orchestration tool of business processes across the different applications that support Medicaid operations. evoBrix supports robust authorization, authentication, and validation features using Oracle Service Bus. The solution is capable of handling common industry standard service requests such as SOAP and REST. Also, evoBrix can change the various attributes of the service without impacting existing clients. The Oracle Fusion SOA infrastructure will allow the Option A solution to avoid point-to-point communication between different system components and will streamline the flow of all information.

Option B Provider Services

Team CNSI recognizes the criticality of providing solutions that directly impact the State of Montana's Medicaid provider and other stakeholders. Our solution for the System provides a robust architecture for creating correspondences, rich Interactive Voice Response (IVR) and a user-friendly, efficient graphical user interface for the call center agents.

Team CNSI's solution is comprised of the following components:

- Oracle's Siebel Public Sector Enterprise Customer Relationship Management (CRM)
- Avaya Aura Communication Manage
- Avaya Call Management System
- Avaya Voice Portal
- Avaya Application Enablement Services
- Avaya CT for Siebel
- Avaya Communication Manager Messaging
- Avaya Aura Workforce Optimization
- Avaya Aura Callback Assist
- Nuance for Automatic Speech Recognition and Text To Speech

Our solution delivers quicker, better, and more efficient customer service than the legacy contact centers. Team CNSI has implemented CRM and IVR solutions in the states of Washington and Michigan as a part of our MMIS implementations. In the states of Washington and Michigan, 160 and 400 call center personnel, respectively, use our solution to support providers and recipients and other stakeholders. Our solution provides the call center service representative a complete view of the caller, including the caller's call history, other correspondence, and any key metrics. Team CNSI's solution allows the call center representative to view multiple inquiry transactions in a single page, reducing overall call handling time and increasing customer satisfaction. One call center supervisor using the application stated that "Three months after go-live, one of the agents took more calls that day than she had any day of the week before go-live." Another call center agent using the application stated, "It's easier to use, which makes my day!"

Figure 3.10.1-8 illustrates evoBrix's high level solution architecture supporting Option B requirements and how it will achieve the integration with DPHHS MMIS modules.



Customer Relationship Management (CRM)

Team CNSI's CRM Siebel system delivers a rich user experience and helps the Customer Service Representative (CSR) agent to better understand and address the needs of the customers in an effective and efficient manner. The application provides the CSR a complete, 360-degree view of the caller, including the caller's call history, correspondence history, and key metrics. The application provides full-featured request tracking, configurable correspondence templates and configurable notification and alerts. The CRM module is fully integrated with the evoBrix claims, provider, and member modules for visibility of related transactional and reference data.

Team CNSI's Customer Relationship Management solution, leverages Oracle's Siebel CRM product to create a scalable and tightly integrated CRM system. Our solution incorporates Siebel Open UI Financial Services Vertical Application Version 8.1.1.14 as the main CRM component.

The CRM system integrates member, provider, and customer support and other MMIS information to facilitate researching provider and member inquiries without requiring a separate sign-on, toggling

between the systems, or dual entry of information. The system will have the ability to associate in screens with caller information, such as caller demographics and other critical key elements, and has the ability to access correspondence history. Team CNSI's CRM solution will be able to manage and track interactions with providers and members across communication channels, including phone, IVR, paper, fax, e-mail and chat. It will track each call that is received by auto-generating and assigning a ticket to each call, route and transfer the call to the appropriate staff, maintain call history, and track call statistics. Team CNSI's CRM system can automatically link tracked calls and tickets to providers and members.

The Team CNSI Advantage

Team CNSI's CRM solution delivers the most comprehensive customer experience that enables the State to maximize the growth of their organization and deliver exceptional experiences to their customers across all channels.

- Comprehensive view of critical information about a customer
- Modular screen navigations to track the interactions and activities
- Configurable workflow policies and event process to meet business needs
- Secured real-time integration with evoBrix module using Web services
- User configurable alerts and notification specific to Providers
- Seamless integration between IVR and CRM through CTI component

MTPSM-3-284

The following describes the major components of our solution, provides an overview diagram, and highlights the unique features of our CRM Siebel Application.

- **Oracle's Siebel CRM:**

Team CNSI has selected Oracle's Siebel CRM for the following reasons:

- Popular and proven CRM product using best-of-breed technology
- Easy-to-find resources knowledgeable to manage Siebel Code base
- Robust and flexible integration capabilities with other COTS products due to industry standard enterprise application integration (EAI) framework

- **Siebel Open UI**:

  Team CNSI's CRM application will be deployed using Siebel Open UI is an extension of the user interface (UI) for the Siebel application, utilizing open web technologies (HTML, CSS, JavaScript, and JQuery). It removes the need for Active X controls and allows Siebel to present a transformed and richer UI based on modern web technology.

  Some of the features of the Siebel Open UI are:

  - Removes device restrictions to accessing CRM data so it can be used on Mac, Linux, Windows, and Android
  - Runs on any modern browser that supports JavaScript, including Internet Explorer, Google Chrome, Firefox, and Safari
  - Fewer key strokes and clicks
  - Allows open extension of functionality using JavaScript API
  - Other usability features: user-managed default themes such as Tab or Tree layout to view screens, escape key to undo, less use of horizontal scrollbar, drag and re-size fields, WAI-ARIA standard compliant
  - Easy upgrade to newer version without any additional license and software costs

Figure 3.10.1-9 compares the ActiveX UI architecture that a high-interactivity client uses to the restriction free architecture that Siebel Open UI uses.

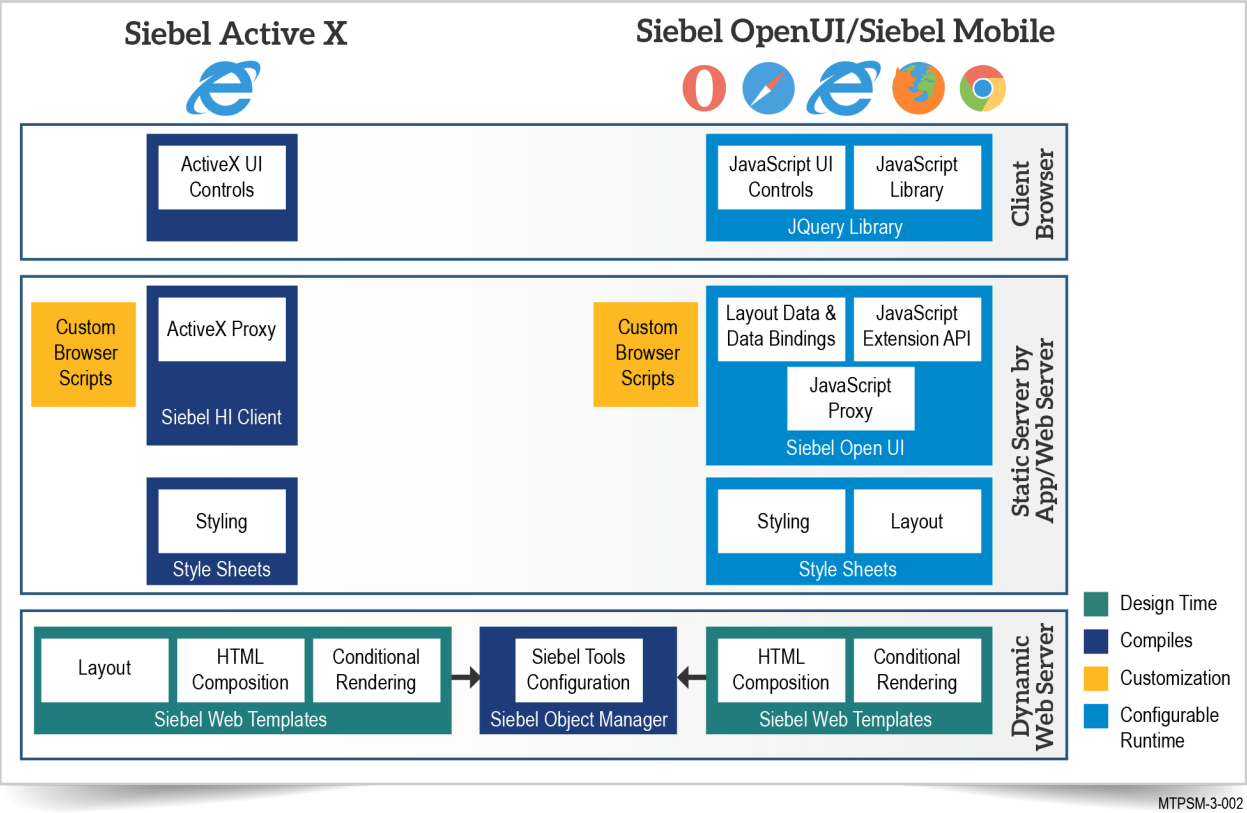


Figure 3.10.1-9. Comparison of Open UI Architecture Overview with Previous Client Version. A UI that provides configurable, modular deployment and reduced code dependency.

Avaya Interactive Voice Response

- The Team CNSI Avaya IVR is a scalable, configurable, robust solution that employs the principles of service-oriented architecture (SOA) and handles all eligibility inquiries through the telephony interface, composed of an integrated system with distributed services. For example, calls are initially handled by the IVR system; however, to play back certain information to the caller or to authenticate the caller a pre-published service is invoked to fetch the information in real-time. Similarly, real-time activity tracking of the caller is accomplished by invoking the tracking service within the Oracle Siebel CRM application. The use of pre-published services helps to improve scalability and shortens the time for integration because the services can be ingested by a disparate set of applications that adhere to common standards.
- Team CNSI's EVS solution incorporates a tightly-integrated architecture between our IVR, our CRM system, and evoBrix. The IVR solution uses Application Service Interface (ASI) to integrate with the CRM solution. ASIs are accessed via Web services using information protocols (such as HTTPS) and data formats (such as XML). Using Web services, our EVS solution uses the SOAP communication protocol over HTTPS to communicate with evoBrix to furnish a wide variety of dynamic, real-time information on demand. An overview of the EVS business architecture is shown in Figure 3.10.1-10.

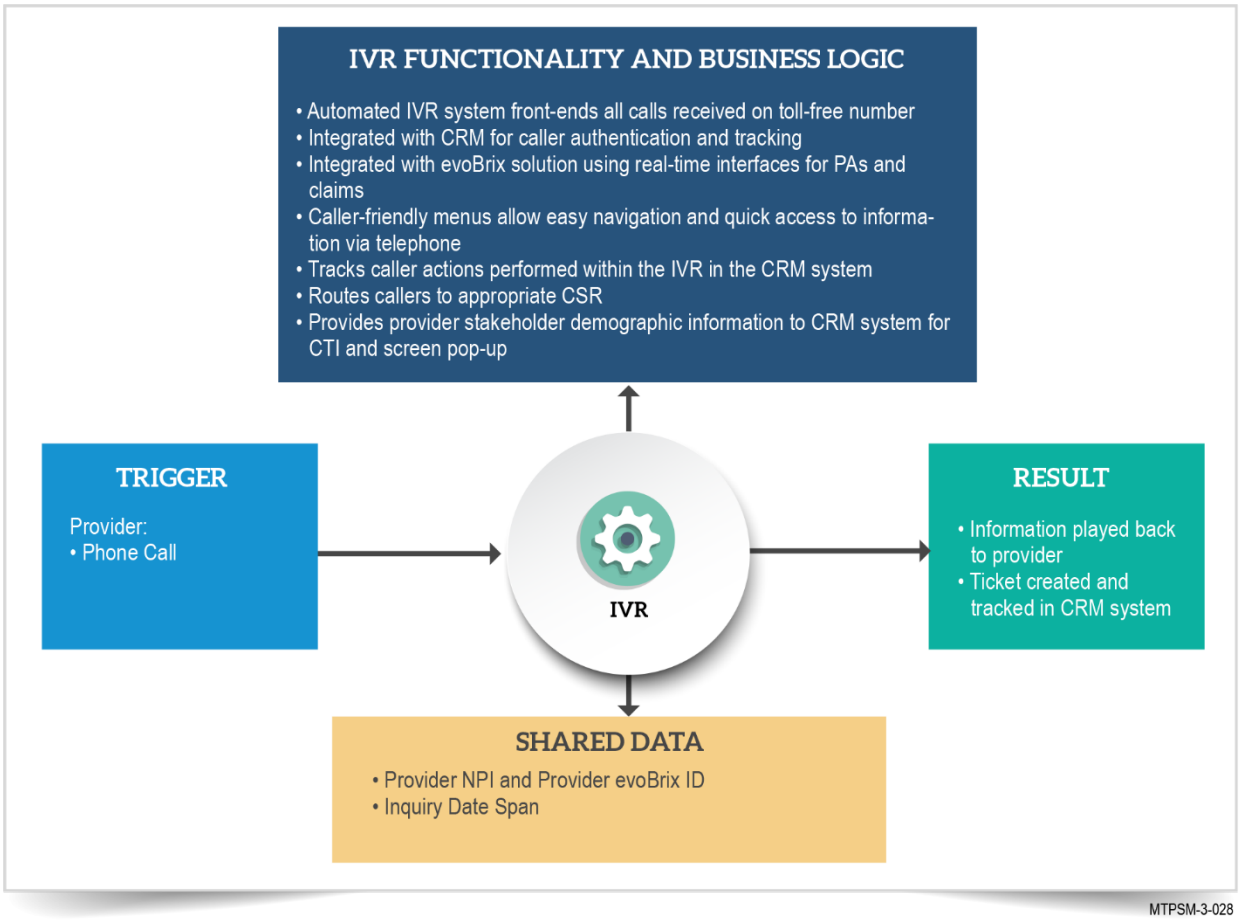


Figure 3.10.1-10. Business Architecture for the Proposed Team CNSI's IVR Solution. Our Business effective IVR process flow solution provides a cost-efficient and scalable model.

- The architecture is designed to avoid unnecessary replication of data. The IVR stores only data pertaining to the serviced call and information required as part of logging and reporting.
- The IVR system supports a menu-driven interface that is inherently intuitive for the caller and can be tuned to give the best caller experience. It supports dual-tone, multi-frequency (DTMF) signaling inputs and automatic speech recognition, enabling the recognition of voice prompts.
- Complex messages, such as coverage and phone numbers, are played back to the caller using a text-to-speech engine instead of pre-canned or pre-recorded messages, providing flexibility and scalability.
- Our IVR solution can be easily configured to support multiple languages as required in the RFP. In addition to tracking the caller within the system, the system sends relevant information about the caller to agents via the CRM solution. This feature, also known as the CTI screen pop, enables the agent to save time and better serve the customer because all relevant information about the caller is already presented on the agent's screen.

The IVR telephony infrastructure uses a high-availability, real-time interface with the CRM system and the system to accomplish the following:

- Create tickets in the CRM system for all calls
- Track caller actions within the IVR and report them to the CRM application
- Authenticate callers with information provided by the caller against the CRM and system databases

- Retrieve and play back information requested by the caller by fetching the most current data from CRM and the system
- Transfer the call to a customer service representative using CTI so that the customer service representative has the relevant caller information available on the screen

Features and Benefits of the Proposed Solution

Figure 3.10.1-11 highlights and communicates the key features and related benefits of the proposed MPATH solution. DPHHS will greatly benefit from the proven, innovative evoBrix solution, as it aligns well with DPHHS' vision to create a modular Medicaid solution focused on business outcomes.

Features and Capabilities	Benefits
MPATH solutions alignment to Enterprise architecture	■ Leverage the State's existing investments *Ensure enterprise-wide access to services through access channels*
Modularity of evoBrix	■ Ability for DPHHS to pick the best fit solution *High degree of interoperability*
evoBrix alignment to MITA Seven Conditions and Standards	■ Maximize federal funds for enhanced FFP ■ Leverage business process improvement opportunities through MITA business process maturity *Proven solution reduces risk to the state*
Configurability	■ Agility to adapt to changes in DPHHS business and regulatory environment ■ Modules are highly configurable to support evolving business needs with the portfolio of business and technical services *CNSI's RuleIT rules engine for business rules processing offers flexibility and adaptability*
Reusable technical services	*Services such as logging, error handling, and data access can be consumed by higher level business services*
Business Process Performance Management and Monitoring capabilities	■ Enhance business effectiveness and efficiency by providing visibility to key business metrics *Provide operational transparency*
Modularity & Alignment to MITA Seven Conditions and Standards of the proposed solution	■ Maximizes flexible procurement options supported by Modularity ■ Eliminates vendor lock-in ■ Improved business scalability owing to a scalable architecture *Alignment to MITA and CMS' Seven Conditions & Standards maximizes inflow of federal funds*
Proposed next generation Medicaid platform	■ Optimal cost of operations and maintenance owing to superior architecture ■ Future-proofs DPHHS technology investments *Aligned to CMS vision*
Workflow enablement	Improved efficiencies due to business process and workflow automation.
Standards Compliance	■ Reduced cost of integration and total cost of ownership Enhanced alignment to CMS
SOA and Interoperability capabilities	■ Enhanced interoperability allows for increased information exchange among trading partners and other agencies *Multiple integration capabilities for flexible integration with external systems*
Configurable rules-based design	■ Agility of changes or modifications to system ■ Quick and cost-effective implementation of changes *Maximized configurability via online screens and the RuleIT rules engine that allow for quick realization of program and policy changes*

Features and Capabilities	Benefits
Scalable architecture	■ Scale up functional and technical capacity based on business demands *Support business growth*
Cost avoidance capabilities	■ Cost avoidance of anomalous claims in a pre-pay mode until the payment integrity of the claim is verified *Improved cost savings, as opposed to expensive pay and chase recoveries*
Real-time business monitoring	■ Enhanced transparency and insights into business and technical operations for all stakeholders *Improved business effectiveness*
Fully web-based system	■ Anytime, anywhere access of all business functionalities without additional client software *Real-time access to information and business transactions*

Figure 3.10.1-11. Key Features. Illustrates Team CNSI's proposed Technical Solution's features and their benefits to the State.

Team CNSI supports the DPHHS Enterprise vision and brings highly relevant experience, best practices, and a proven and advanced technical solution that directly aligns with the objectives and requirements of this engagement. Team CNSI brings both a technology solution and operational business experience working in similar multi-vendor environments, possessing the end-to-end capabilities required from the MT PSM vendor – a key value to DPHHS.

3.10.1.1 Compliance

This section addresses compliance with state and federal statutes, policy, mandates as well as industry standards required for the Contractor's Scope of work. Offerors must describe how their solutions and operational approach meet each of the Compliance requirements detailed in Attachment F, Requirements Matrix.

Team CNSI's evoBrix PMIS solution provides a rich set of MITA-aligned features for provider enrollment, provider information management, and provider support functions, and will serve to address the State's PMIS requirements. The solution combines a full-featured, secure, self-service provider portal with a comprehensive administrative framework to manage enrollment, disenrollment, inquiry, provider information maintenance, and provider support. The solution provides State staff and providers with a full range of online, real-time inquiry and update functions with web-based data entry screens. The solution maximizes the opportunity to collect valid and complete information throughout the provider's association with the DPHHS. The solution provides a 100 percent browser-based, interactive, and modern Provider Services Module (PSM) supporting the day-to-day business needs of the providers and DPHHS user communities.

The Team CNSI Advantage

The evoBrix PMIS solution meets technical and operational policies, standards and regulations.

- Aligned with CMS' MITA and Seven Conditions and Standards
- Integrated with industry standard COTS solutions and APIs
- Complies with privacy, security, and regulatory standards such as HIPAA, HITECH, NIST, etc.

MTPSM-3-328

Our straightforward approach to regulatory compliance begins at the onset of the solutioning phase with itemizing all controls, safeguards, applicable local and federal regulations such as all Federal Information Security Management Act (FISMA) and Health Insurance Portability and Accountability Act (HIPAA) regulations, and all applicable DOD, OMB, and NIST standards. We will accomplish this using Trusted Integration's TrustedAgent platform. Team CNSI will use the TrustedAgent platform to provide direct traceability for each regulatory, policy, and control requirement, as well as full transparency for the

State's security officer through shared access and reporting. By establishing our compliance framework at the onset of the system's configuration, we will be able to ensure that security controls and safeguards are integrated into every module of the system from the onset and not just bolted-on after the fact.

The evoBrix PMIS and Team CNSI meet all applicable State and Federal requirements for regulatory policy compliance, audit compliance, and security.

The system will:

- Comply with security and safeguard requirements of the following Federal agencies/entities:
  - Health & Human Services (HHS) Center for Medicare & Medicaid Services (CMS)
  - Administration for Children & Families (ACF)
  - NIST 800-53r4, MARS-E, and DOD 8500.2
  - All applicable NIST security guidelines, including but not limited to the below guidelines
    - NIST Special Publication 800-66 Revision 1
    - NIST Special Publication 800-47
    - NIST Special Publication 800-88 Revision 1
    - NIST Special Publication 800-111
  - Federal Risk and Authorization Management Program (FedRAMP)
  - Internal Revenue System (IRS) Publication 1075
  - Center for Internet Security (CIS) Benchmarks for Database v2.1.0
  - Federal Information Security Management Act (FISMA) of 2002
  - Health Insurance Portability and Accountability Act (HIPAA) of 1996
  - Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009
  - Privacy Act of 1974
  - e-Government Act of 2002
  - Patient Protection and Affordable Care Act of 2010, Section 1561 Recommendations
- Comply with all applicable State and Federal laws and regulations, including 42 CFR Part 2 and HIPAA, including privacy and client consent for release requirements
- Follow HIPAA standards for the electronic exchange of information between Providers and the State
- Conform to and support the Medicaid Information Technology Architecture (MITA) v3.0 or later and align with CMS' Seven Conditions and Standards
- Comply with all applicable State security policies and adhere to all legal, statutory, and regulatory requirements
- Implement security controls in accordance with all Federal and State security policy and regulations
- Meet:
  - NIST 800-53A and NIST 800-53 rev4 moderate baseline
  - IRS pub 1075, which points back to NIST 800-53 rev 3
  - NIST 800-53A rev1 guidance and Harmonized Security and Privacy Framework.
  - CMS requirements, which point back to NIST 800-53 rev3 moderate baseline
  - Guidance from CMS including MITA Framework 3.0 and Harmonized Security and Privacy Framework

In addition to meeting the above standards, Team CNSI has designed the solution to support all facets the MITA initiative. The evoBrix platform aligns with the Seven Conditions and Standards inherently and by design. It is not only aligned to the architectural requirements but also the software engineering aspects of

the Seven Conditions and Standards guidance. Team CNSI has also closely followed CMS guidelines and directives regarding modularity and Medicaid implementations and has kept up its solution via the evolution of the MITA standards over the years, based on the practical experience gained working with multiple states, CMS, and other stakeholders.

Team CNSI understands DPHHS' desire to have a MITA-aligned solution, which will enable DPHHS to secure Federal funds for implementation and ongoing maintenance. In fact, Team CNSI delivers a complete mapping of the software-as-a-service (SaaS) evoBrix PMIS base design documentation, which includes a crosswalk of PMIS functionality to MITA business areas and business processes. This is updated throughout the solution analysis and solution modeling sessions where needed. The PMIS to MITA crosswalk is an essential part of Team CNSI's strategy to support CMS certification of the MT PSM.

CMP01

The Contractor shall, upon request by the State or at the end of the contract, transfer or destroy all documentation in the custody of the Contractor. The Contractor shall provide the transferred records and data in a format agreed upon by the State.

Team CNSI affirms and agrees to transfer or destroy all documentation within our custody at the end of the contract. In addition, we agree to transfer the records and data in a format agreed upon by the State.

CMP03

The Contractor shall notify the State in writing within five (5) business days following initial detection of suspected fraud or abuse and provide supporting documentation.

Team CNSI will notify the State in writing within five business days following initial detection of suspected fraud or abuse and provide supporting documentation. Our solution is designed to identify potential fraudulent or improper enrollments through the evoBrix Provider Credentialing Service (PCS) which will provide real time insight into any potential fraud or abuse. The information will be provided to the appropriate business operations staff for further review and action.

The evoBrix Provider Credentialing Service (PCS) solution is comprised of pre- and post-enrollment screening processes that integrate the system with a real-time credentialing service. This one-stop solution provides improved automation and reduced manual intervention. Pre-enrollment screening results are available in real time within evoBrix PCS web pages, also evoBrix PMIS solution automatically set indicators on the enrollment during screening process for the provider enrollment specialist to review and make appropriate decisions regarding whether to approve or deny the enrollment application. The evoBrix PCS solution provides ability to track screening results to meet audit requirements for the following screening criteria:

- State/Federal Death Verification
- Sanctions
- OIG Sanctions
- General Services Administration (GSA) Exclusion list (EPLS/SAM)
- License Board Sanctions
- NPI Verification
- SSN, EIN/TIN Verification

- National Council for Prescription Drug Programs (NCPDP) Verification
- License/Certification Verification
- In/Out-of-state professional license
- DEA, CLIA, Board Certification Verification with American Board of Medical Specialties
- Criminal History and Sex Offense check

The PCS common features are as follows:

- Integrates with LexisNexis credentialing service
- Integrates with other State-specific data sources provided by DPHHS
- Ability to view screening results in real time
- Real-time, on-demand screening capabilities anytime during enrollment application review or modification review
- Supports audit capabilities
- Screening of individual practitioners, hospitals/entities, disclosed entities (such as board of directors, office managers, corporate, agents), etc.

For additional information, please see Section 3.10.10, Enrollment.

CMP04

The Contractor's solution shall have full integration of the MITA initiative with business, architecture and data required to support the State's healthcare programs.

Team CNSI understands DPHHS' desire to have a MITA-aligned solution, which will enable the agency to secure Federal funds for implementation and ongoing maintenance. Specifically, our proposed evoBrix PMIS solution's alignment to MITA will maximize enhanced FFP for the state and provide flexible procurement options to leverage the best fit solution.

Team CNSI's evoBrix platform aligns with the Seven Conditions and Standards inherently and by design. It is not only aligned to the architectural requirements but also the software engineering aspects of the Seven Conditions and Standards guidance. Team CNSI has also closely followed CMS guidelines and directives regarding modularity and Medicaid implementations and has kept up its solution via the evolution of the MITA standards over the years, based on the practical experience gained working with multiple states, CMS, and other stakeholders.

To support this proactive approach, Team CNSI delivers a complete mapping of the SaaS evoBrix PMIS base design documentation which includes a crosswalk of PMIS functionality to MITA business areas and business processes. This is updated throughout the solution analysis and solution modeling sessions where needed. The PMIS to MITA crosswalk is an essential part of Team CNSI's strategy to support CMS certification of the MT PSM.

Figure 3.10.1-12 summarizes how the proposed solution addresses the Seven Conditions and Standards, showing each of the seven conditions and standards as colored hexagons. Next to each, we explain how evoBrix aligns with that condition/standard.



Figure 3.10.1-12. evoBrix PMIS solution alignment with Seven Conditions and Standards. evoBrix has been designed from the beginning to support the goals of the CMS initiative's Seven Conditions and Standards.

CMP05

The Contractor shall adhere to data retention requirements cited in 45 CFR 164.316 and Administrative Rule 37.85.414. The Department may require a longer retention period on an exception basis to support ongoing business needs (e.g., TPL recovery and drug rebate).

Team CNSI will adhere to data retention requirements cited in 45 CFR 164.316 and Administrative Rule 37.85.414. evoBrix PMIS has the capability to store data for longer retention periods. Team CNSI will comply with the retention policy defined by the DPHHS.

CMP06

The Contractor shall have written policies governing access to, and duplication and dissemination of all individual or entity information.

Team CNSI's Privacy and Security policies and procedures ensure that only those assigned to the project and/or corporate support have access to government information, personally identifiable information (PII), or protected health information (PHI). These policies and procedures are maintained in a shared area and are constantly updated. Some examples of policies and procedures are:

- Team CNSI's Ethics and Legal Compliance Policy, which requires every employee to take various trainings as mandated by Federal Government (e.g., security awareness, HIPAA).
- Team CNSI's Supplier Agreement Management policy, which requires that the company hold subcontractors responsible for security, and flow down contract provisions to them.

Team CNSI prepares and maintains an active and effective Information Security Plan for each information system under their purview. The Information System Security Plan is required prior to the start of certification and accreditation, and it shall be reviewed and updated, if needed, once a year.

Team CNSI conducts a privacy impact assessment on all systems under their purview that process personally identifiable information in accordance with Office of Management and Budget (OMB) Memorandum 03-22 and the E-Government Act.

The Team CNSI Office of Procurement and Contracts (OPC) and Contracting Officers (CO) ensures that all solicitation documents, Statements of Work (SOWs), and applicable contract vehicles identify and document the specific security requirements for IT services and operations that are required of the contractor. The OPC and COs ensure that:

- The security requirements shall include how sensitive information is to be handled and protected at the contractor's site. The requirements apply to any information stored, processed, or transmitted using the contractor's computer systems, as well as background investigations, clearances, and/or required facility security.
- The SOWs and contracts specify that at the end of the contract, the contractor must return all information and IT resources provided during the life of the contract, and must certify that all information has been purged from any contractor-owned system used to process Team CNSI information.

The Team CNSI OPC and COs shall ensure that all solicitation documents, SOWs, and applicable contract vehicles contain a statement requiring contractors to adhere to Team CNSI's Information

Security policies. The Team CNSI Senior Information Security Officer (ISO) and Program Offices that outsource Information Security services shall do so in accordance with NIST Special Publication (SP) 800-35, Guide to Information Technology Security Services.

Team CNSI conducts reviews in accordance with NIST SP 800-53A "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," and NIST SP 800-53 "Recommended Security Controls for Federal Information Systems," once a year to ensure that contract Information Security requirements are implemented and enforced for systems under their purview.

In addition, all Team CNSI employees must take the Privacy & Security Awareness Training and HIPAA Training prior to receiving access to PII or PHI, and refresher training is mandatory on an annual basis thereafter.

CMP07

The Contractor shall comply with all sections of the Americans with Disabilities Act (ADA), Section 508 of the Rehabilitation Act and ensure user interface standards account for the various forms of colorblindness.

Team CNSI's evoBrix PMIS solution is developed with W3C web-based standards and is designed to work on Internet Explorer, Safari, Firefox, and Chrome browsers. The PMIS user interface complies with usability standards such as the ADA, Older Americans Act, and the Rehabilitation Act Section 508 subpart B Section 1194.21. PMIS web pages are supported by most commonly used screen readers such as JAWS and Microsoft Narrator. Our solution also complies with the accessibility color scheme specific to Windows operating systems.

CMP08

The Contractor and its services, work products and final deliverables provided by the Contractor applicable to the services described in the scope of work shall be knowledgeable of and in compliance with pertinent State and Federal Statutes, CIO Promulgated Rules, State IT policies, rules, and standards for required system hardware, software and development tools and processes, and operational procedures when completed and accepted by the Department. The Contractor shall also be aware of upcoming changes to existing rules and regulations as well as new rules and regulations that may impact the scope of work.

Team CNSI makes all reasonable efforts to maintain compliance with pertinent State and Federal Statutes, CIO Promulgated Rules, State IT policies, rules, and standards for required system hardware, software and development tools and processes, and operational procedures so far as they can be known. In addition, Team CNSI actively scans the environment for potential changes in policy, economic shifts, social and technological trends as well as the legal environment that could influence our clients and solutions. As a matter of practice, Team CNSI understands that maintaining compliance with pertinent standards, policies, rules and regulations is necessary and beneficial to both Team CNSI and our clients.

CMP09

The Contractor shall adhere to recognized best practices during the execution of the scope of work including the latest version of the National Institute of Standards and Technology (NIST) Special

Publication (SP) 800 series related to cyber security.

Team CNSI evoBrix solution has been built to adhere to recognized best practices and complies with the following standards as it relates to cyber security:

- IRS pub 1075, which points back to NIST 800-53 rev 3
- CMS requirements, which point back to NIST 800-53 rev3 moderate baseline
- Guidance from CMS including MITA Framework 3.0 and Harmonized Security and Privacy Framework
- All applicable NIST security guidelines, including but not limited to the below guidelines
    - NIST Special Publication 800-66 Revision 1
    - NIST Special Publication 800-47
    - NIST Special Publication 800-88 Revision 1
    - NIST Special Publication 800-111
    - NIST 800-53A and NIST 800-53 rev4 moderate baseline
    - NIST 800-53A rev1 guidance and Harmonized Security and Privacy Framework.

CMP10

The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions-MITA Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data.

Team CNSI supports the "to be" vison of the MITA 3.0 Standards and Conditions – MITA Condition and has been built with the MITA vision in view.

The evoBrix PMIS module provides a rich set of MITA-aligned features for provider enrollment, provider information management, and provider support functions. The solution combines a full-featured, secure, self-service provider portal with a comprehensive administrative framework to manage enrollment, disenrollment, inquiry, provider information maintenance, and provider support. The PMIS solution comes with a cross walk from evoBrix PMIS functions to the related MITA Business Area/Business Process. Team CNSI updates this crosswalk as the solution is being configured for a specific implementation to capture demonstrate the relationship between MITA Business Area/Business Process the MECT checklists.

CNSI has developed expert knowledge of all applicable industry and federal government standards, models and practices related to security of state Medicaid systems, including HHS and CMS directives, HIPAA, FISMA, FIPS, NIST, and DOD standards and guidelines, as well as the most recent standards outlined by HITECH and ACA. Our security architecture and design is based on a Defense in Depth approach rooted in industry best practices and honed through years of experience in design and development of MMIS solutions in Michigan, Washington, Illinois, and Utah.

CMP11

The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions - Industry Standards Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data.

The Contractor shall ensure alignment with, and incorporation of, industry standards, HIPAA, privacy and transaction standards; accessibility standards, and standards that provide greater accessibility for individuals with disabilities and standards under the Affordable Care Act.

Team CNSI affirms and agrees to support DPHHS to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions – Industry Standards Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data.

Our evoBrix PMIS solution is compliant with the following:

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-19, Title II, Sections 261-264
- Federal Security Standards for Security and Privacy (NIST)
- The HIPAA Administrative and Simplification Provisions for Privacy (2002) and Security (2003), Code of Federal Regulations (CFR) 45, parts 160, 162, and 164
- The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (enacted as part of the American Recovery and Reinvestment Act of 2009)
- Standards adopted by the Secretary under Section 1104 of the Patient Protection and Affordable Care Act (PPACA)
- Standards and protocols adopted by the Secretary under section 1561 of the Affordable Care Act
- Compliance to CORE Rules and NCPDP data standards
- Support for interoperability standards
- Web and usability standards aligned to W3C and ADA standards

Team CNSI's processes ensure that all systems and services related to this procurement, including transactions, common identifiers, and privacy and security standards, continue to remain in compliance as stipulated in legislation or other regulatory requirements.

CMP12

The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions - Leverage Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The Contractor shall promote sharing, leveraging, and reuse of healthcare technologies and systems within and among states.

Team CNSI affirms and agrees to support DPHHS to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions – Leverage Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data.

Typically, in the state infrastructure, the MMIS is a comparatively large investment and provides many infrastructure tools and enterprise services. The resources and software investments made for the MMIS can be leveraged by the DPHHS divisions and the other state agencies. The evoBrix PMIS solution is a SOA-based system. Facilitated by evoBrix Integrator Services, our SOA capabilities are bi-directional; it is equally easy to expose the services built in the solution to external systems as it is to consume services from external agencies. The portfolio of business and technical services enables our solution to support business processes more effectively. Through the underlying framework, evoBrix Integrator Services enable the evoBrix PMIS solution to provide access to business process areas, to functions within the overall MMIS application, and to external components to facilitate exchange of information from external

agencies and entities as may be required. This modular solution will provide DPHHS with several options to leverage existing investments in legacy applications:

- Use outbound interfaces to provide data to external applications that need MMIS data to operate (e.g., operational data store [ODS], data warehouse, and external agencies).
- Use inbound interfaces to accept data from external applications that hold key data for MMIS needs, such as external eligibility systems and data from other State agency applications.
- Use evoBrix Integrator Services and orchestration services to provide services and consume services from legacy applications.

CMP13

The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions -Business Results Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The Contractor shall support effective communications with providers and the public.

Team CNSI affirms and agrees to support DPHHS to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions -Business Results Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data.

The evoBrix PMIS solution excels at supporting the Business Results Condition through making provider details available to the claims function so that claims can be adjudicated and, when Option A is added to the solution, Team CNSI provides a portal that interfaces with the claims functions to allow submission and inquiry of claims. This enables real time communication with providers of claims status.

CMP15

The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0-Standards and Conditions- Interoperability Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The Contractor's solution shall ensure seamless coordination and integration with components, other systems and allow interoperability with health information exchanges, public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services and federal data sources.

Team CNSI affirms and agrees to support DPHHS to maintain compliance with the "to be" vision of MITA 3.0-Standards and Conditions - Interoperability Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The solution is aligned with current and future industry interoperability standards through Team CNSI's participation in MITA and HL7 standards, as well as our continued participation in other key interoperability standards and projects.

Team CNSI's evoBrix ISR core architecture leverages ESB features within the SOA framework to integrate disparate systems effectively. This architecture provides an integration backbone that connects core applications and other systems and allow interoperability with health information exchanges, public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services and federal data sources using following standards:

- Swagger and WSDL SOAP specifications for web services

- SOA architecture standards
- Web service security standards (1.0) for web services security

CMP16

The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0-Standards and Conditions- Modularity Standard or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The Contractor's solution shall use a modular, flexible approach to systems development, including the use of open interfaces and exposed Application Programming Interfaces (API); the separation of standardized business rule definitions from core programming; and the availability of standardized business rule definitions in both human and machine-readable formats.

Team CNSI affirms and agrees to support DPHHS to maintain compliance with the "to be" vision of MITA 3.0-Standards and Conditions - Modularity Standard or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data.

At the core of the evoBrix solution is a system based on SOA principles. It has a portfolio of business and technical services that enable our solution to support business processes more effectively. These services are accessible through multiple channels and are available across business process areas, based on requirements, through the evoBrix Integrator Services. Business services are more contained within a business process area or related process areas; technical services are common and shared across all or most business process areas. Our PMIS solution's alignment with MITA provides services that enable better and more efficient business processes. Through this framework, these services enable the evoBrix solution to provide access to business process areas, to functions within the overall MMIS application, and to external components via evoBrix Integrator, which facilitates the exchange of information from external agencies and entities as may be required. The solution has been architected to support and advance the Modularity Standard through:

- Web service interfaces such as REST, SOAP, and COTS APIs
- Well-defined, open interfaces with service definitions conforming to WSDL, Swagger RESTful API Documentation specifications
- SOA mediation layer leveraging Oracle Service Bus (OSB)
- Rules engine with an integrated rules repository to house all Medicaid rules
- Ability to submit business rules to HHS-designated repository
- COTS grade product configuration capabilities
- Systems Development Lifecycle methodologies confirming to CMMI product engineering standards

CMP17

The Contractor must provide the Department with compliance assurances for the Contractor scope of work.

Team CNSI is aware of and able to comply with all relevant state and federal statues, policies, and mandates, as well industry standards, that are relevant to the scope of work to be undertaken under the contract to be awarded pursuant to this RFP.

CMP18

The Contractor shall be fully compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-1919) and Administrative Simplification (Subset of Title II) requirements in effect as of the date of release for the RFP and with any changes that subsequently occur, unless otherwise noted.

Team CNSI affirms and agrees to maintain compliance with current Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-1919) and Administrative Simplification (Subset of Title II) requirements unless otherwise noted. HIPAA and HITECH established a set of federal standards intended to protect the security and privacy of PHI, and impose requirements related to the use and disclosure of PHI, appropriate safeguards to protect PHI, individual rights, and administrative responsibilities. HIPAA requires entities that handle electronic PHI (ePHI) to implement policies necessary to secure such information. In addition, the HITECH Act includes provisions that require organizations that store ePHI to implement procedures to report the breach of unprotected ePHI.

Due to the importance of maintaining compliance to these standards, Team CNSI performs regular assessments to protect the confidentiality, integrity, and availability of the information systems. The scope of the assessment covered Oracle Compute Cloud, Oracle Storage Cloud, Oracle Database Cloud, Oracle Java Cloud, Oracle Database Backup, Exadata Cloud, and GoldenGate Cloud.

More specifically:

- Administrative Safeguards security includes the overall security management process; assigned security responsibility; workforce security; information access management; security awareness and training; security incident procedures; contingency planning; evaluation; and business associate contracts or other arrangements
- Technical Safeguards security includes audit controls, integrity, personnel or entity authentication, and transmission security
- Physical Safeguards security includes facility access controls, workstation use, workstation security, as well as portable devices and media controls
- Policies and Procedures and Documentation Requirements implement reasonable and appropriate policies and procedures to comply with standards, implementation specifications, or other requirements

Team CNSI's solution also adheres to the following compliance standards, including National Institute of Standards and Technology (NIST) standards:

1. CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E)
2. Federal Information Security Management Act (FISMA)
3. Internal Revenue System (IRS) Publication 1075
4. Patient Protection and Affordable Care Act (PPACA) or (ACA)
5. All applicable NIST security guidelines, including but not limited to the below guidelines
   a. NIST Special Publication 800-66 Revision 1
   b. NIST Special Publications 800-53 and 800-53A
   c. NIST Special Publication 800-47
   d. NIST Special Publication 800-88 Revision 1
   e. NIST Special Publication 800-111
6. Center for Internet Security (CIS) Benchmarks for Database v2.1.0

Also, Team CNSI's existing MMIS implementation in Michigan undergoes independent security assessment conducted by external third parties involving NIST, MARS-E, and CIS audit controls. Additionally, Team CNSI performs internal CIS audits annually. As standards are updated, Team CNSI's solution is updated to fully comply with the changes. Any possible security issues discovered during audits are promptly remediated to maintain the most secure environment possible.

CMP19

The Contractor shall enter into a Business Associate Agreement (BAA) prior to the initiation of work. The Contractor and the Department acknowledge and agree that the Business Associate Agreement is subject to HIPAA, and the HIPAA implementation regulations thereunder, and the Health Information Technology for Economic and Clinical Health Act (HITECH), and the HITECH implementation regulations thereunder. Under the Agreement, both parties are responsible for security and privacy compliance and must take advantage of the appropriate security capabilities and measures and adequate data validation, as well as have appropriate policies and procedures in place to minimize or prevent unlawful access by any person who may have access to the entire database.

Team CNSI acknowledges and understands that we will enter into a BAA with the state prior to the initiation of work. Team CNSI takes a multi-faceted approach to ensure all applicable safeguards are in place to comply with HIPAA and HITECH implementation regulations. These include:

- Administrative Safeguards security includes the overall security management process, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency planning, evaluation, and business associate contracts or other arrangements
- Technical Safeguards security includes audit controls, integrity, personnel or entity authentication, and transmission security
- Physical Safeguards security includes facility access controls, workstation use, workstation security, as well as portable devices and media controls
- Policies and Procedures and Documentation Requirements implement reasonable and appropriate policies and procedures to comply with standards, implementation specifications, or other requirements

CMP20

The Contractor shall ensure all information not specifically identified as Protected Health Information (PHI) or Personally Identifiable Information (PII) as defined under HIPAA and/or HITECH is treated as privileged communications, held confidential, and must meet the terms and conditions specified in the RFP, BAA and Contract.

CNSI is vigilant in protecting information and has the necessary appropriate policies and procedures in place to ensure compliance with this requirement. CNSI's Privacy Officer reviews all privacy related terms and conditions in the RFP, BAA and contracts to ensure compliance. In addition to our HIPAA Policy and our Privacy Policy, CNSI's Code of Ethics and Business Conduct requires our employees to be diligent in protecting PHI, PII, CNSI's and our customer's confidential information. CNSI also conducts separate trainings on each of these policies, which means our employees are trained a minimum of three times a year on protecting this type of information (in addition to any project specific training). These trainings instruct our employees if they are ever uncertain whether information is PHI, PII or confidential, they are to protect it as if it is until they confirm otherwise. We also reinforce the importance

of protecting this information by creating awareness with Privacy and Security posters and email reminders.

CMP21

The Contractor shall ensure that except as provided by law, no information in the possession of the Contractor about any individual shall be disclosed without prior written consent.

Team CNSI affirms and agrees that, except provided as by law, no information in the possession of the Contractor about any individual shall be disclosed without prior written consent.

CMP22

The Contractor shall follow all applicable technical standards for site and system security policies and procedures to protect the Department's healthcare data and information systems.

Team CNSI affirms and agrees that it shall follow all applicable technical standards for site and system security policies and procedures to protect the Department's healthcare data and information systems.

CMP23

The Contractor's data management approach and operational policies shall meet HIPAA, HITECH, ARRA and other federal and State privacy and security requirements.

Team CNSI has extensive experience operating as a business associate under the provisions defined under HIPAA, HITECH and ARRA. As an approved business partner, Team CNSI employs various technical safeguards to prevent unauthorized access to government data. We use multiple technologies from diverse manufacturers to restrict and contain network traffic flow to and from its systems and components, including multiple firewall appliances from different vendors, as well as application-layer traffic control technologies. This reduces the risk that any vulnerability found in one protection layer would also exist in any subsequent protection layers. If an attack resulted in successfully breaching one layer due to an unmitigated vulnerability, the same attack would fail against the next layer. This approach substantially reduces the risk of network intrusion by greatly increasing the required complexity of any potentially successful attack.

Team CNSI's solution encrypts data at rest using Oracle Transparent Data Encryption (TDE). TDE is implemented at the tablespace level using AES-256 algorithm. A multi-tier backup strategy along with encrypted storage is provided for safeguarding the wallet.

Data that is replicated as a part of the Disaster Recovery solution will also be encrypted using TDE.

Additional safeguards include:

- All data export and import requirements using Oracle Data Pump Utility will also be encrypted using TDE.
- Data in flight is encrypted using Oracle Network Encryption, as well as with use of SSL/https for communication between applications and users.

- Data backups are de-duplicated and encrypted on the backup media using Oracle's Advanced RMAN Encryption.
- All systems in this environment are backed up with using a best-in-class next generation enterprise Actifio backup solution. All data running in the environment is backed up in its native format and stored on off-device dedicated storage appliances. All backup snapshots are kept on-site (Chicago, IL), and all production data in addition to being stored on-site is replicated to a geographically-diverse, dedicated application hosting stack (Ashburn, VA).
- All application traffic from end users is encrypted (SSL encryption).
- All HIPAA EDI transaction and interface files are encrypted at rest using NAS encryption technology.

Team CNSI's operational policies support data security strategy by maintaining data centers and project offices that provide all the necessary infrastructure to create productive, safe, and secure work environments.

- Team CNSI's data centers use a sophisticated Data Center Infrastructure Management (DCIM) to monitor all environmental systems (e.g., temperature, humidity, power usage, leakage, efficiencies of equipment, and systems)
- Physical access requires authorization and is monitored
- All employees and visitors must visibly wear official identification while on-site
- Visitors must sign a visitor's register and be escorted and/or observed while on-site
- Possession of keys/access cards and the ability to access the locations are monitored
- Staff leaving employment must return keys/cards
- Premises are monitored by CCTV
- Entrances are protected by physical barriers designed to prevent unauthorized entry by vehicles
- Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management

Team CNSI's project offices have security protocols in place to prevent unauthorized access in the form of ID badges, building access cards and/or biometric security access, and surveillance of entries.

CMP24

The Contractor's solution shall be compatible with multiple standard browsers in accordance to the State's IT Standards which can be found in the Procurement Library.

The solution shall allow access from standard browsers without requiring specialized plug-ins or applets to function.

Team CNSI's evoBrix PMIS solution is developed with W3C web-based standards and is designed to work on Internet Explorer, Safari, Firefox, and Chrome browsers. The PMIS user interface complies with usability standards such as the ADA, Older Americans Act, and the Rehabilitation Act Section 508 subpart B Section 1194.21. PMIS web pages are supported by most commonly used screen readers such as JAWS and Microsoft Narrator. It also complies with the accessibility color scheme specific to Windows operating systems. The solution does not require specialized plug-ins or applets to function.

CMP25

The Contractor shall retain, all original paper documents for fifteen (15) calendar days from the date the documents are received and have been scanned, indexed, stored in the ECM and meet verification

process standards. Original documents may be destroyed once indexed and stored in the ECM and the retention period is met in accordance with State and Federal guidelines.

Team CNSI affirms and agrees to retain original paper documents for fifteen (15) calendar days from the date the documents are received and have been scanned, indexed, and stored in the ECM. The PMIS solution provides the functionality to store and retain original paper documents in the ECM in accordance with the state-approved data retention policy.

CMP26

The Contractor shall maintain an auditing system and employ accounting/auditing procedures and practices that conform to GAAP and GAAS. All charges applicable to the contract shall be readily ascertainable from such records.

CNSI's financial accounting systems are in compliance with GAAP and GAAS auditing standards. The Company records all project costs directly to projects and can be verified and tracked in accordance with the contract work scope. The Company's financials and internal controls are audited on an annual basis by BDO with a clean opinion every year. All detailed project records are available at the corporate office in Rockville, MD.

CMP27

The Contractor will ensure that all technologies implemented are in compliance with any End User Licensing Agreements or other licensing arrangements.

Team CNSI affirms and agrees to maintain compliance to all licensing requirements for technologies implemented for the evoBrix PMIS solution.

CMP29

The Contractor shall comply with Affordable Care Act Section 1104 Administrative Simplification, and Section 1561 Health IT Enrollment Standards and Protocols.

Team CNSI affirms and agrees to comply with Affordable Care Act Section 1104 Administrative Simplification, and Section 1561 Health IT Enrollment Standards and Protocols as those regulations apply to the scope of the MT PSM module.

CMP30

The Contractor's solution shall ensure that all data necessary for legal requirements is retained.

evoBrix PMIS has the capability to store data for long retention periods. Team CNSI will comply with the retention policy defined by the DPHHS. Data known to be retained for legal requirements can easily be accommodated per the state-approved data retention policy.

CMP32

The Contractor shall provide a mechanism to purge source documents in accordance with HIPAA security provisions and State requirements.

Team CNSI affirms and agrees to provide a mechanism to purge source documents in accordance with HIPAA security and State requirements. CNSI will work with the State to define the Data Retention Policy for the system and will build a periodic purge/archival process to enforce the state-approved data retention policy.

3.10.1.2 Security

This section addresses security requirements for the Contractor's solution(s) and operations. Due to the nature of the information managed by the State, any event resulting in a potential loss of confidentiality, integrity and/or availability of government data is unacceptable. Offerors must describe their approach to security and describe how proposed solution(s) meet each of the Security requirements detailed in Attachment F, Requirements Matrix.

Team CNSI has implemented a robust security framework for ensuring Confidentiality, Integrity, and Availability. This is known as the CIA Triad and this provides multiple layers of external and internal security to protect sensitive and confidential information. This triad includes various administrative, physical and technical mechanisms that are required to protect the sensitive information. A combination of encryption solutions, multi-tiered network with layered security, intrusion detection and prevention systems enforces the Confidentiality area of the Triad while multi-factor authentication, auditing, access management and log management enforces the Integrity area of the Triad. High Availability architecture, multi-site design, robust system monitoring and alerting framework enforces the Availability area of the Triad. This approach ensures full protection of Protected Health Information (PHI) and Personally Identifiable Information (PII). We employ a defense-in-depth approach to security built on a simple set of key principles:

The Team CNSI Advantage

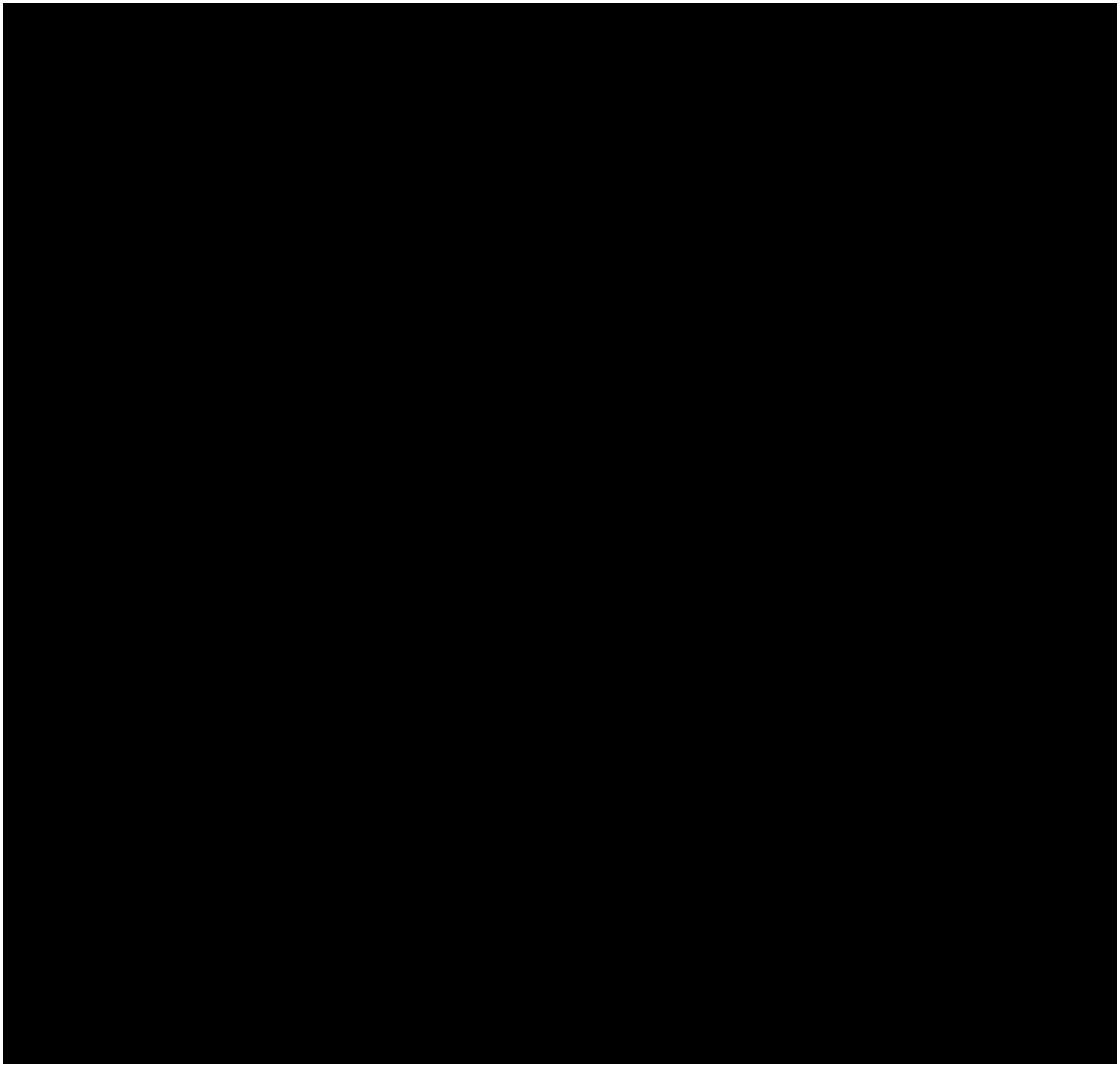
Team CNSI has over 18 years of experience with MMIS solutions, the security requirements for keeping them secure, and how to protect the privacy of PHI and PII information.

- Hosted in FedRAMP-compliant and HIPAA-compliant Oracle Government Cloud
- Three-tier application security architecture
- Compliant with FedRAMP, HIPAA, NIST, CMS MARS-E, FISMA, and IRS standards
- Annual third-party security assessments and penetration testing
- Proven dependable warm site disaster recovery design
- Multilayered monitoring and auditing tools with real-time alerting
- Role-based access control security
- Multi-tier encryption of data both at rest and in transit
- Complete audit trail of application, database, and system access

MTPSM-3-113

- Employee education and awareness – All employees go through annual security and privacy training
- Multiple layers of physical and environmental controls
- Multiple layers of logical controls and procedures
- Continuous monitoring and assessment
- Encryption of data transmission and stored data
- Role-based Access Control (RBAC) to ensure that information access is restricted to only appropriate access based on user's role
- Change management and configuration management to prevent security and stability issues from unauthorized changes
- Intruder Detection System (IDS) monitoring to prevent unauthorized access

Team CNSI's hosting platform is built on a robust security framework comprising of multiple security and encryption features. These security and encryption features are built using Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) services. Figure 3.10.1-13 provides an overview of the various PaaS and IaaS security services that forms the building blocks of Team CNSI's evoBrix PMIS solution.



These principles result in a comprehensive framework of procedures and policies, some examples of which are:

- Constructing and maintaining systems with a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information.
- Ensuring that the software used to install and update the system, independent of the mode or method of conveyance, will be certified free of malevolent software ("malware"). Team CNSI understands

that we have the option to self-certify compliance with this standard through procedures that make use of commercial malware scanning software.

- Supporting protection of confidentiality of all PHI/PII delivered over the internet or other known open networks via encryption using Advanced Encryption Standard (AES) and an open protocol such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), Internet Protocol Security (IPsec), XML encryptions, or Secure/Multipurpose Internet Mail Extensions (S/MIME) or their successors. Team CNSI understands that the system will be subject to external audit checks on this point.
- Additionally, supporting the use of a standards-based encrypted format using AES or their successors when storing PHI/PII on any device intended to be portable/removable (e.g., smartphones, portable computers, portable storage devices).
- Fully monitoring all access to both the data and the underlying systems.

SEC01

The System shall provide a physical and electronic environment that uses public key infrastructure to verify all transactions and the identity of all users and denies access to unauthorized users. For example:

a. Require unique sign-on (ID and password)

b. Require authentication of the receiving entity prior to a system-initiated session, such as transmitting responses to eligibility inquiries.

Team CNSI has more than 18 years of experience developing and operating MMIS and ensuring that those systems – and the highly sensitive data they process and store – meet or exceed State and Federal security standards. Our team will bring this wealth of experience and our extensive set of mature practices to the implementation of the evoBrix PMIS solution to help drive the secure design and implementation of all solution components, including IT infrastructure, systems, and application components.

Because of our experience and the maturity of our security practice, Team CNSI is accustomed to playing a key role in helping State and Federal agencies extend their own security practices. We have contributed significantly to agency and system security plans in the states of Michigan, Washington, Illinois and Utah, as well as CMS, the U.S. Census Bureau, and the DOD. Our approach to developing security controls and procedures for the DPHHS PSM solution is to tightly integrate the strategies and best practices we have developed with the existing DPHHS Single-Sign On (SSO) and extend or strengthen it wherever necessary.

User-initiated Access

Team CNSI's evoBrix PMIS solution will integrate with Montana's existing Identity and Access Management (IAM) infrastructure to provide a seamless IAM experience for internal and external users across the MPATH system. Our solution will integrate with the DPHHS system integration platform and consume identities provided by the DPHHS identity solution provider. The identity federation will use SAML 2.0. This solution provides the ability to identify users in different contexts (such as time, day of week, location of access, or type of access method), allowing State policies and user preferences to be applied consistently across the system. As shown in Figure 3.10.1-14, all user-initiated access will go through the following steps:

1. The user logs into the MT DPHHS portal.
2. Upon successful login, the user selects the option to go to the evoBrix application (Service Provider).

3. This generates and sends a SAML Auth Request to MT DPHHS SAML 2.0 (Identity Provider). This request will include attributes about the user. Team CNSI will work with MT DPHHS to identify the possible attributes expected by the Identity Provider.
4. The MT DPHHS SAML 2.0 (Identity Provider) verifies the user's identity against MT DPHHS Active Directory.
5. The MT DPHHS SAML 2.0 (Identity Provider) generates a SAML authentication response that includes assertions that identify the user and include attributes about the user. The client browser is redirected to the designated landing page of the evoBrix application. If the SAML authentication response includes attributes that map to multiple IAM roles, the user is first prompted to select the role to use for access to the evoBrix application.

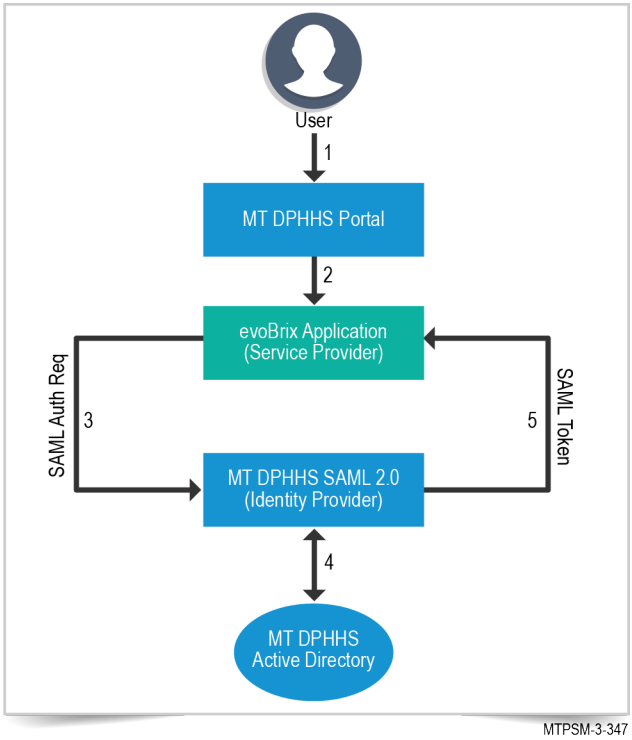


Figure 3.10.1-14. Identity Management Integration. Team CNSI will seamlessly integrate with DPHHS identity management (IDM) process.

Security is a major component of web portals that handle user authentication and authorizations. The evoBrix web portal leverages the DPHHS IAM security framework for integration, which allows the solution to offer a secure SSO experience without replicating user credentials across multiple directory stores. Duplicating user credentials increases the risk of account compromise, potentially leading to unauthorized access to highly-sensitive PHI or PII data in the system. DPHHS will handle the user authentication, and the evoBrix portal will handle the user authorization based on RBAC. The evoBrix web portal handles user sessions and user management, as well as coordinated back-end application functionality with full auditing capabilities. User analytics are captured and reported periodically, and are used in our performance fine-tuning to find areas of improvement and consumer engagement activities.

System-initiated Access

Team CNSI's evoBrix PMIS solution will integrate with DPHHS's Enterprise Service Bus (ESB) hub, as mandated by DPHHS's security requirements. A handshake is established first with the exchange of certificates between the PMIS and other state agencies. This establishes a 256bit SSL encrypted tunnel. Every web service request will need to contain a username/password that would have been provided to the account owner as part of registration/access to the application along with all the mandatory request fields as agreed to between Team CNSI and the State Agencies. A valid response is then provided to this web service request from the evoBrix PMIS solution upon a successful authentication and authorization.

Backend System Access

Access to backend servers for Team CNSI's administrators is only allowed after completion of the authorization process followed by multi-factor authentication to validate their identity. This connection is through Oracle Cloud Infrastructure FastConnect, which is a fully-encrypted VPN connection. This VPN connection isolates the workstation from any outside internet activity or access.

Additionally, all Team CNSI personnel have named user access to the system and no shared accounts are created. All Team CNSI personnel are fully trained on security and privacy laws and regulations. Therefore, all PHI and PII is fully protected per HIPAA and other federal and state regulations.

SEC02

The Contractor shall ensure that any data being transmitted or transported either physically or electronically will be encrypted.

Team CNSI employs a defense-in-depth approach to securing our solution by implementing multiple layers of network, system, and database encryption technologies to ensure all classified and potentially sensitive data is encrypted at rest and in transit. We have extensive experience with these encryption technologies, through our implementations in our Michigan, Illinois, Utah, and Washington MMIS solutions.

Figure 3.10.1-15 provides an overview of all the encryption solutions that are used in Team CNSI's evoBrix PMIS.

Tier	Component	Encryption Method	Encryption Algorithm
Database Tier	Data Files	Oracle Transparent Database Encryption	AES-256
Database Tier	Encryption Keys	Oracle Key Vault	PKCS#12 file
Database Tier	Backups	Oracle RMAN Encryption	AES-256
Storage Tier	Oracle Data Pump Exports	Oracle Data Pump Encryption	AES-256
Storage Tier	Flat Files (at rest)	Linux eCryptfs	AES-256
Storage Tier	Flat Files (in transit)	Titan SFTP	SHA-1
Network Tier	Data Traffic	Oracle Network Encryption	AES-256
Network Tier	Data Integrity	Oracle Data Integrity	SHA-1
Application Tier	Network Traffic	SSL Encryption	256 bit SSL
Physical Transmission	Disks/Disk Partition	IDRIX VeraCrypt	AES-256

Figure 3.10.1-15. Data Encryption Solutions. An overview of Data Encryption solutions that are used in Team CNSI's evoBrix PMIS.

Database Tier

At the database layer, Team CNSI leverages advanced Oracle security tools, which ensures strong encryption of databases containing sensitive information such as PII and PHI.

- Oracle Transparent Data Encryption (TDE): Team CNSI uses TDE to encrypt sensitive data at rest. Data is encrypted at the tablespace level using AES-256 algorithm. The encryption keys are stored in a wallet and the wallet is also secured, stored, and backed up using Oracle Key Vault.
- Oracle Key Vault: Team CNSI uses Oracle Key Vault to ensure protection of encryption keys. Oracle Key Vault is used to centrally authorize, secure, and manage all encryption keys. Oracle Key Vault is a FIPS 140-2 Level 3 compliant key management system, offering a strong and scalable solution.
- Oracle Backup Encryption: Team CNSI uses Oracle Recovery Manager (RMAN) and Local TDE master encryption key to encrypt all database backups including full backups, incremental backups,

and archive log backups. This ensures that backups, which are usually stored in offsite locations, are secured.

Storage Tier

- Oracle Data Pump Encryption: Team CNSI uses Oracle Data Pump for taking exports of database schemas and tables. The dump files that are generated by Oracle Data Pump are encrypted using Oracle Data Pump Encryption and the encryption algorithm is AES-256.
- Flat File Encryption at Rest: Team CNSI uses eCryptfs utility within Oracle Linux to encrypt a file system. This utility is used to encrypt individual files and directories using AES-256 algorithm.
- Flat File Transfer Encryption: Team CNSI uses Titan Secure FTP to ensure encryption of the file in transit.

Network Tier

- Oracle Database Network Encryption: Team CNSI uses AES-256 based network encryption to encrypt data in transit, thus ensuring that data is secure as it travels across the network
- Oracle Data Integrity: Team CNSI uses Secure Hash Algorithm 1 (SHA-1) based Data Integrity protection to safeguard data against data modification attacks and replay attacks
    - Data modification attack: An unauthorized party intercepting data in transit, altering it, and retransmitting it is a data modification attack
    - Replay attack: Repetitively retransmitting an entire set of valid data

Application Tier

At the application layer, all user sessions to and from the application are encrypted with 256bit SSL. This approach provides end-to-end network security, reducing the system's exposure to potentially malicious internet traffic and mitigating the possibility of internet-based attempt to defeat critical safeguards that could expose sensitive personal, health, or financial information.

Physical Transmission

Team CNSI's evoBrix PMIS solution does not normally require physical transmission of data using disks or disk partitions. However, when a need arises, then Team CNSI uses IDRIX VeraCrypt, which is an open source disk encryption tool. This utility is used to perform on-the-fly encryption of disks and disk volumes using AES-256 algorithms. VeraCrypt features optimized implementations of cryptographic hash functions and ciphers which boost performance. It can create a virtual encrypted disk within a file or encrypt a partition or (in Windows) the entire storage device with pre-boot authentication.

SEC03

The Contractor shall ensure that any unneeded hardware, software, and licenses have been decommissioned.

All Configuration Items (CIs) related to Hardware and Software Asset Management, are identified, documented, and tracked in the Configuration Management Data Base (CMDB). Team CNSI uses Combodo's iTOP as the CMDB tool for Hardware and Software Asset Management. Both manual and automated processes, that affects any CIs related to these components, generates a change notification and requires reconciliation to update the official record in the CMDB. This process keeps track of all the hardware and software assets as well as their usage.

Based on their usage, any unneeded hardware, software and licenses can be decommissioned by going through the Change Control Board (CCB) process. Direction is determined by consensus of all organizations represented at the CCB including, at a minimum, personnel from Team CNSI and DPHHS PMO. The CCB represents the interests of project management by ensuring that a structured process is used to decommission any unused hardware, software and licenses.

The Change Control Board:

- Reviews the current hardware, software and license assets monthly
- Requests that impact analysis of proposed hardware and software changes be performed including changes to operational and acquisition costs
- Decommission process is started for any unneeded hardware and software assets and procurement process is started for any new hardware and software requests
- Reviews the hardware or software changes for both decommission and procurement processes
- Makes decisions and monitors progress of the hardware and software installation or deinstallation
- Communicates decisions made to affected groups and individuals

Team CNSI maintains the hardware for evoBrix PMIS solution and it is listed in iTOP CMDB maintained by Team CNSI personnel. Figure 3.10.1-16 shows a snapshot of a list of hardware CIs available in the CMDB.

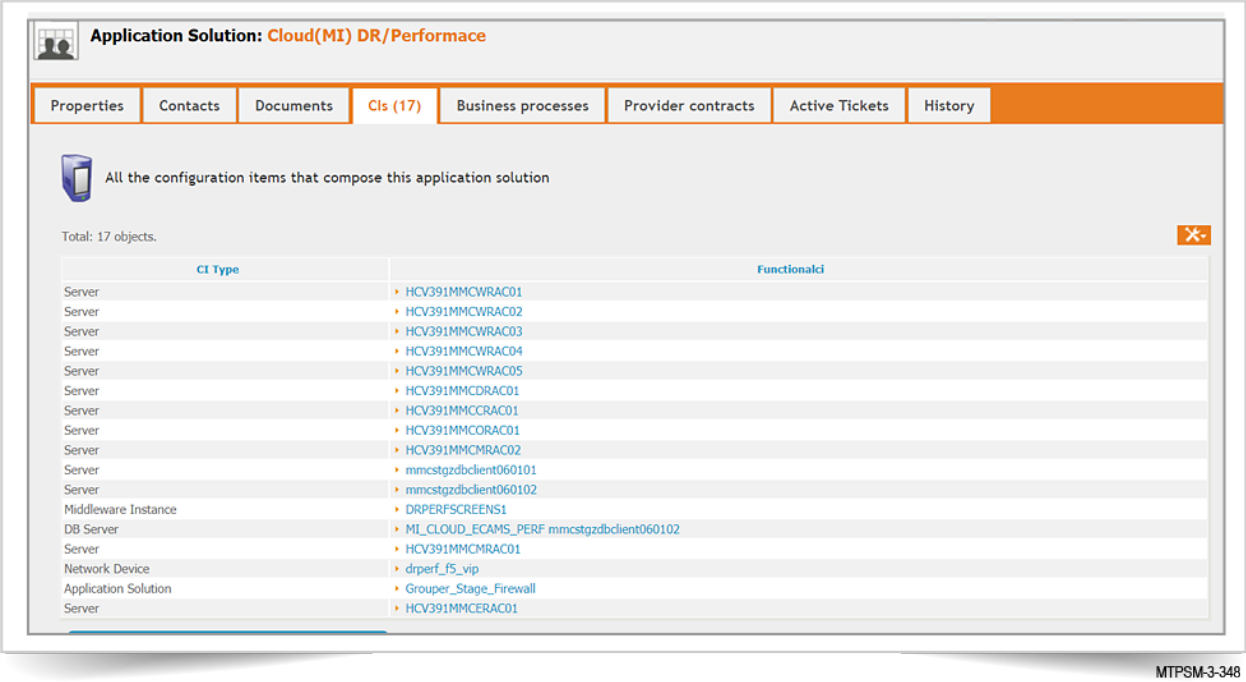


Figure 3.10.1-16. iTOP CMDB. Team CNSI's tool for tracking Hardware CIs.

Once all the CIs are entered, the CMDB tool allows team members to establish relationships among them showing a layout of all the hardware CIs that constitute a logical environment as shown in Figure 3.10.1-17. The tool records the time and action to provide an audit trail of changes made to a CI.

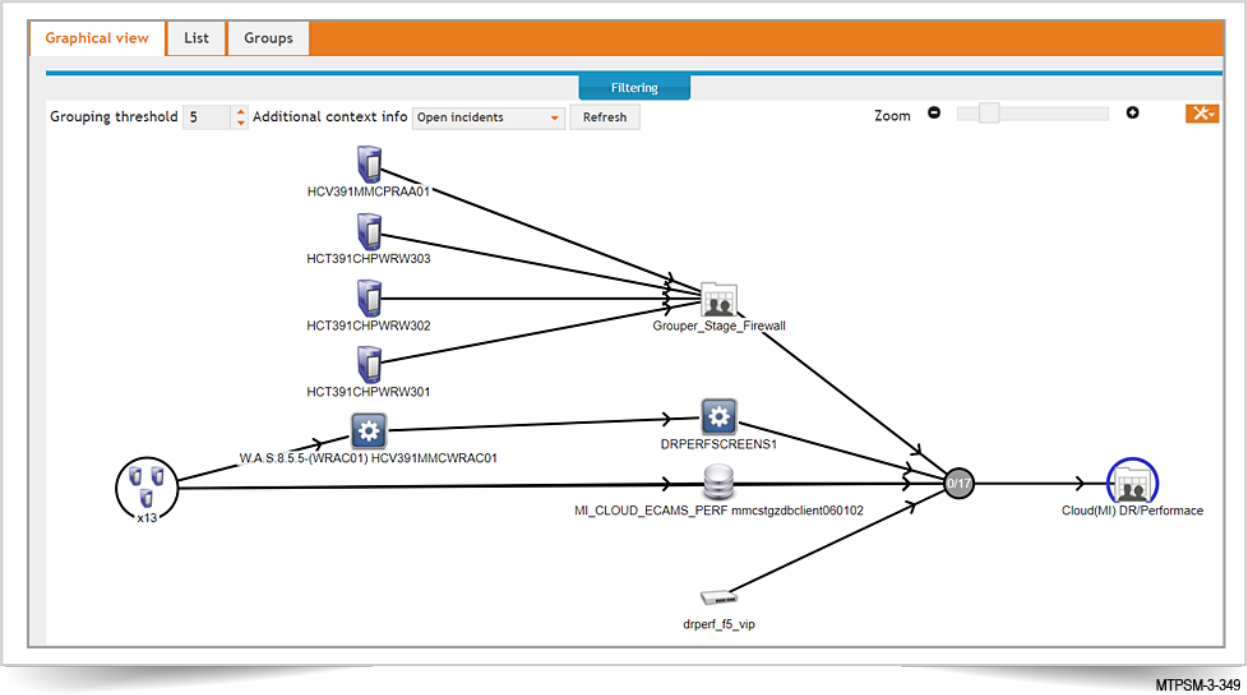


Figure 3.10.1-17. Graphical Representation of Hardware CIs Constituting a Logical Environment. Helps plan for maintenance, availability, and system health of a given logical environment.

SEC04

The Contractor shall protect all government data from loss or unauthorized disclosure.

Team CNSI's private cloud is hosted in the Oracle's FedRAMP Government Cloud. Figure 3.10.1-18 describes a multi-layered security approach that protects the backend client data from unauthorized access. The Team CNSI solution is designed using a three-tier industry standard approach.



- Presentation Tier

User access to the system is only granted after being authenticated through the Montana identity management system. Once the user is positively identified, the credentials are handed off to Team CNSI's application to be used for authorization to the appropriate modules and data in the backend of the system, based on RBAC in the software. The users first access an authentication/authorization tier in front of the presentation tier to authenticate into the system. Once the user is authenticated into the system they interface with the presentation tier, which presents to them the access to the site.

- Application/Services Tier

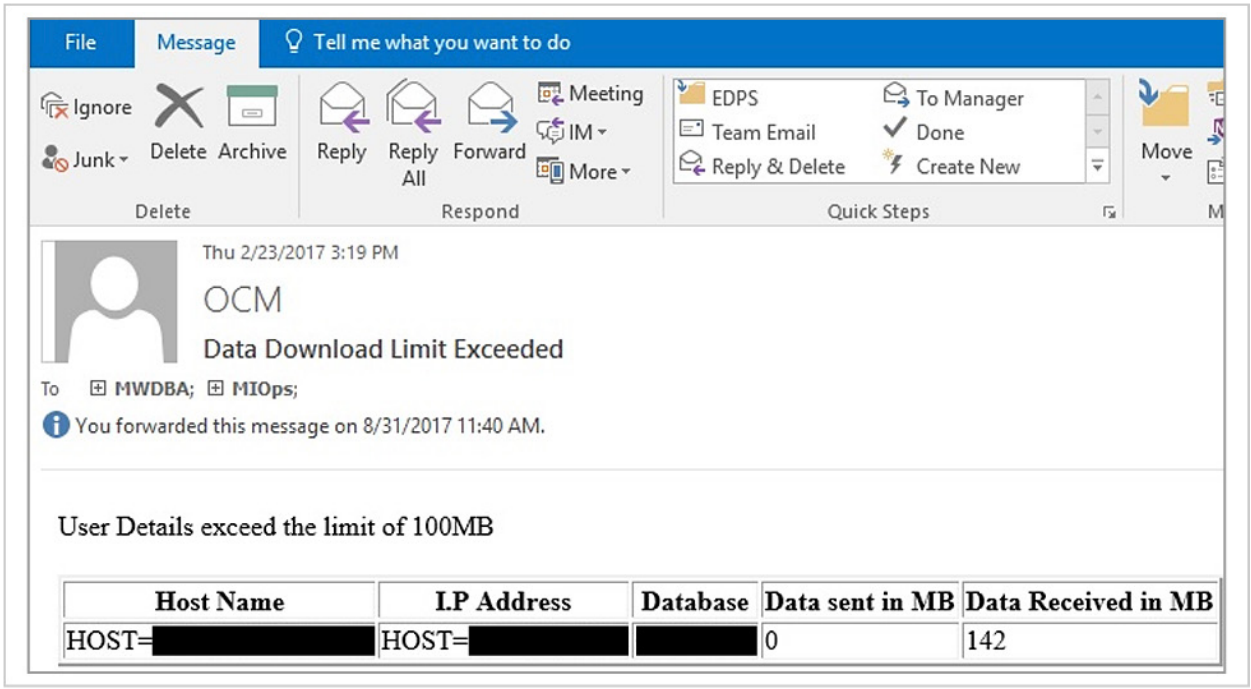
The presentation tier servers interact with the application/services tier. The user does not have any direct access to the application/services tier. The applications then access the data tier. Each tier is protected from the others using firewalls to protect the more sensitive environments from the frontend systems.

- Database Tier

There are also tight controls in the system for access by Team CNSI's administrative personnel to the system. Access to backend servers is only allowed after completion of multi-factor authentication to validate their identity. This connection is through a fully encrypted VPN connection that isolates their workstation from any outside internet activity or access. All personnel are fully trained on security and privacy laws and regulations. Therefore, all PHI and PII is fully protected per HIPAA and other federal and state regulations.

Oracle Connection Manager

Additionally, access to the Oracle databases by Team CNSI personnel is monitored and audited using Oracle Connection Manager (OCM). All client and application access to the databases must flow through the OCM. Data download limits are enforced via OCM to prevent mass download of information from the system. This prevents intruders from doing a wholesale data dump limiting exposure if there is an account that has been compromised. Any requests out of the proper norms automatically triggers alerts to operations staff. Access to data for download is bound by RBAC rules to prevent access to information the person is not authorized to access. All data access is logged, and unusual activity generates alerts. A sample alert email is described in Figure 3.10.1-19, where a user is trying to download more than 100 MB of data.



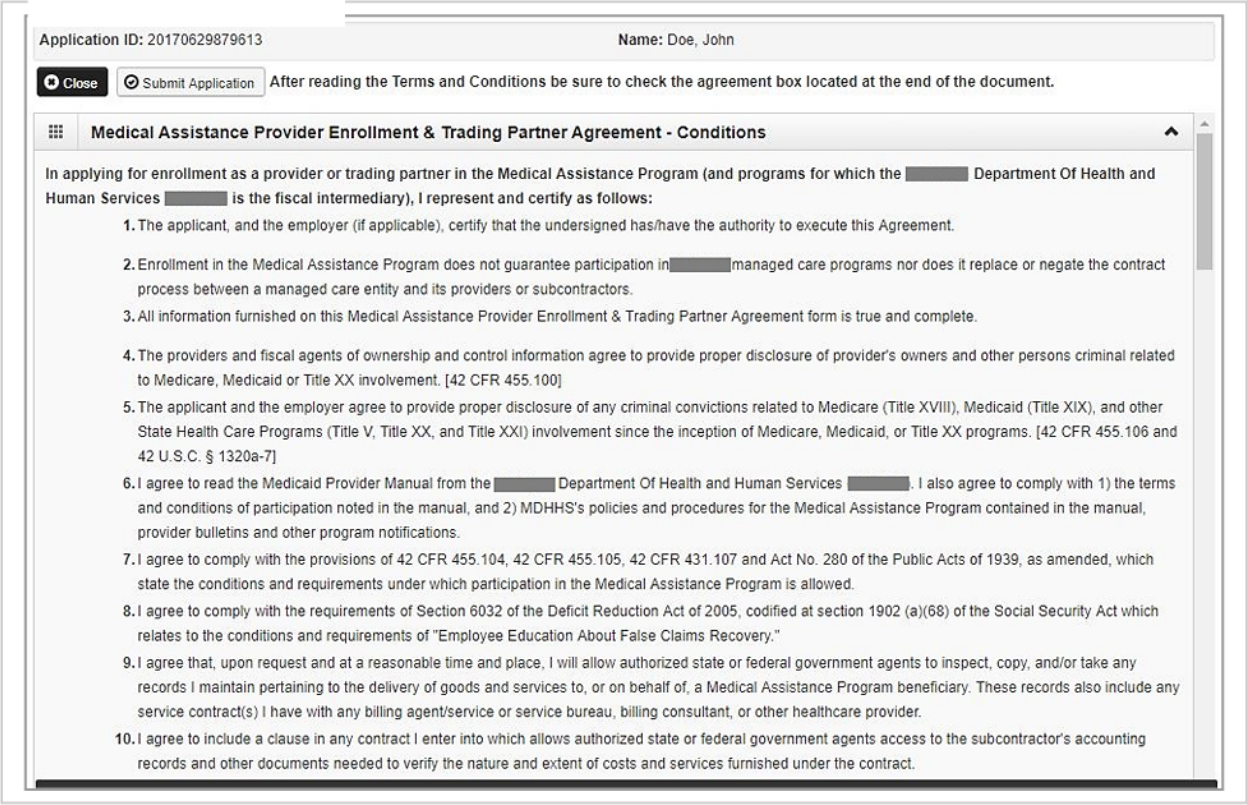
MTPSM-3-350

Figure 3.10.1-19. Data Download Limit Tool. Backend Access to Data tier is monitored and audited using the Data Download Limit tool configured within OCM.

SEC05

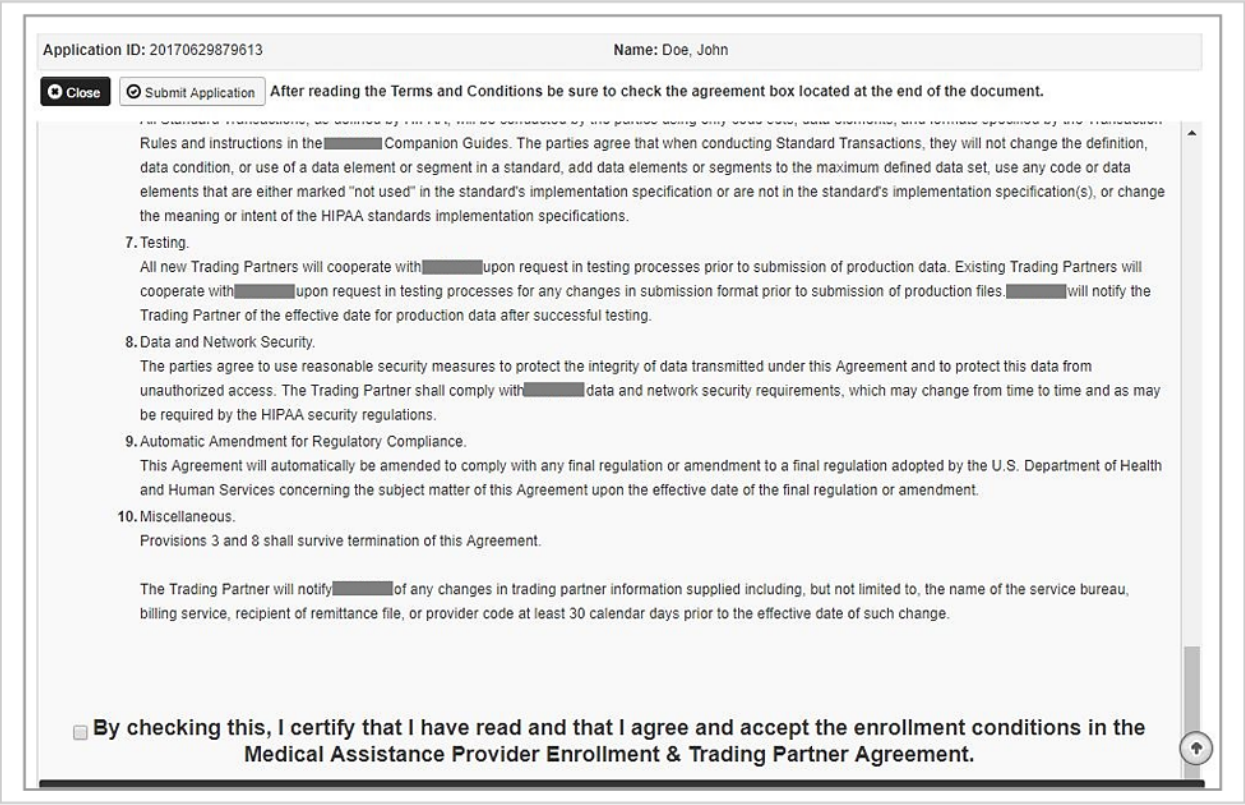
The Contractor's solution shall streamline electronic transactions by incorporating electronic and digital signatures compliant with HIPAA and other State and federal statutes.

The evoBrix PMIS solution streamlines electronic transactions by requiring an electronic signature from providers during the enrollment process to ensure that their intent to accept the terms of the agreement is captured against their enrollment record. This helps ensure compliance with HIPAA and other State and federal statutes. The solution provides ability to configure the language for terms and conditions by effective date range. The solution also keeps track of the terms and conditions accepted by the providers for audit compliance. Team CNSI will configure the terms and conditions language in the system defined by DPHHS. Once the provider has completed all the enrollment steps, the provider is presented with the terms and conditions they need to review and acknowledge, as shown in Figure 3.10.1-20 and Figure 3.10.1-21.



MTPSM-3-428

Figure 3.10.1-20. Electronic Signature - Terms and Conditions Screen. Team CNSI's evoBrix solution supports electronic signatures thus making the electronic transactions compliant with HIPAA and other State and federal mandates.



MTPSM-3-429

Figure 3.10.1-21. Electronic Signature - Second half of the Terms and Conditions Screen. The evoBrix PMIS solution streamlines electronic transactions by requiring electronic signature from providers during the enrollment process to ensure that their intent to accept the terms of the agreement is captured against their enrollment record.

Team CNSI's evoBrix PMIS solution will integrate with the Montana State's existing IAM infrastructure to provide a seamless IAM experience for internal and external users across the MPATH system. Our solution will employ Oracle Access Manager to provide integration with the DPHHS system integration platform. It will consume identities provided by the DPHHS identity solution provider. The identity federation will use SAML 2.0. This integration along with secure communication uses SSL 3.0/TLS 1.2, thus ensuring message integrity, non-repudiation and user authentication. The system requires trading partners to digitally sign their application for enrollment in to the system thus making it compliant with HIPAA and other State and federal statutes.

SEC06

The Contractor's solution shall provide tools (e.g., alerts or reports), which identifies usage anomalies or users who may have misused the system.

Team CNSI's evoBrix PMIS solution is monitored and protected by various PaaS services within the security suite of the Oracle Cloud. These PaaS services help to identify usage anomalies and system misuse. The solution suite includes Oracle Security Monitoring and Analytics (SMA) Cloud Service, Oracle Log Analytics Cloud Service and OCM. These tools enable rapid detection, investigation, and remediation of the broadest range of security threats across Team CNSI's cloud IT assets. Figure 3.10.1-22 provides an architecture overview of these PaaS services.

If a breach or system misuse is detected, these security tools records and attempts to shut down the breach. Alerts are generated to the operations staff, who contacts all appropriate Team CNSI staff. Upon resolution of the situation, a full root cause analysis is performed, the system remediated to prevent any future issues, and reports generated and sent to all appropriate stakeholders.

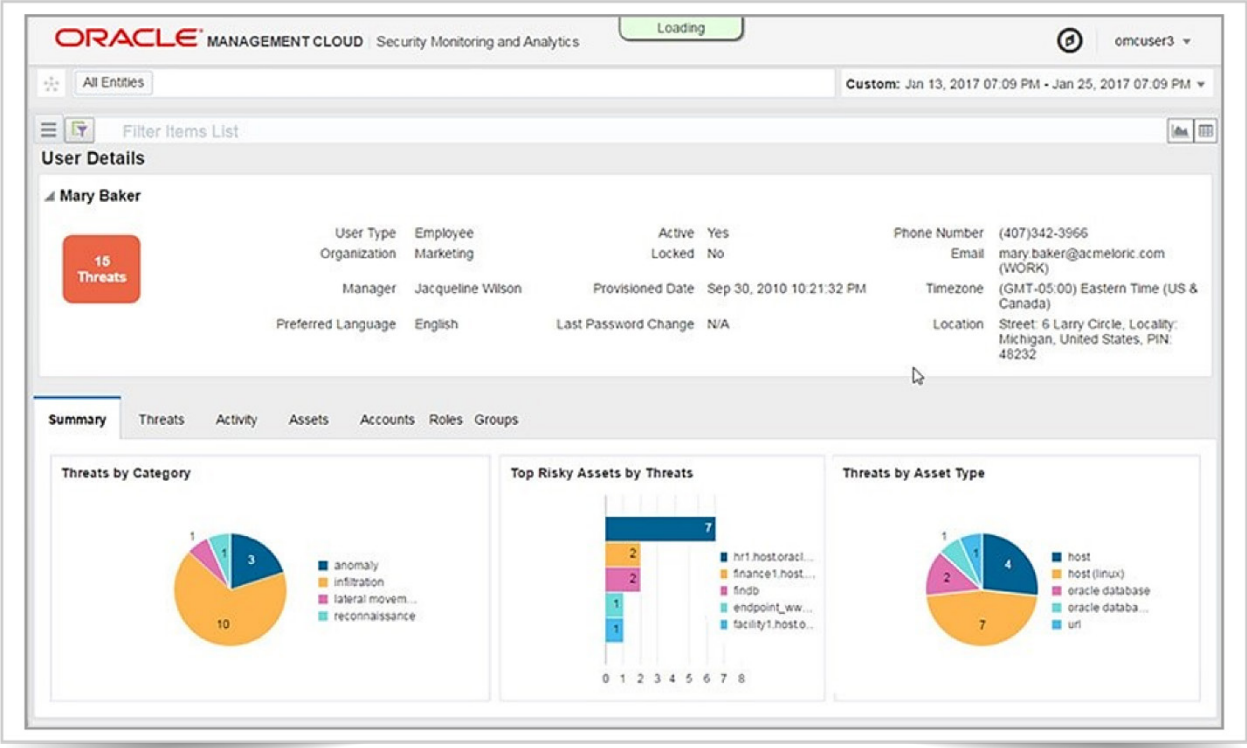


Oracle Security Monitoring and Analytics (SMA) Cloud Service

Oracle SMA Cloud Service enables rapid detection, investigation, and remediation of the broadest range of security threats across on-premises and cloud IT assets. Security Monitoring and Analytics provides integrated security information and event management (SIEM) and UEBA capabilities built on machine learning, user session awareness, and up-to-date threat intelligence context. With secure provisioning, simplified monitoring, and automated incident response, this service offers the single point of control needed to identify usage anomalies or system misuse. A sample dashboard screenshot of SMA Cloud Service is shown in Figure 3.10.1-23.

- Universal Threat Visibility: Collect and analyze security relevant data from multiple feeds and protect against known and unknown threats

- Advanced Threat Analytics and Visualization: Detects SQL Query anomalies across multiple behavioral attributes
- Attack Chain Visualization: Provides insight into an attack's origin, techniques and targets
- Single UI that can detect a threat from start to finish across team CNSI's hosting platform
- Auto-Remediation and Awareness to Configuration Changes



MTPSM-3-379

Figure 3.10.1-23. SMA Cloud Service Dashboard. SMA provides integrated SIEM and UEBA capabilities built on machine learning, user session awareness, and up-to-date threat intelligence context.

Oracle Log Analytics Cloud Service

Team CNSI uses Oracle Log Analytics cloud service to monitor, aggregate, index, and analyze all log data from multiple sources. This cloud service includes features that helps to detect usage anomalies and system misuse. A sample dashboard screenshot of Log Analytics Cloud Service is shown in Figure 3.10.1-24.

- Consolidates audit data from databases, operating systems, applications, firewalls, and directories
- Audit data is then stored into a central reporting repository for compliance reporting and alerting
- Enables users to search, explore, and correlate this data to troubleshoot problems faster and derive operational insight
- Smart clustering of log events based on common signatures helps identify patterns and outliers quickly and thus is used to identify and track usage anomalies

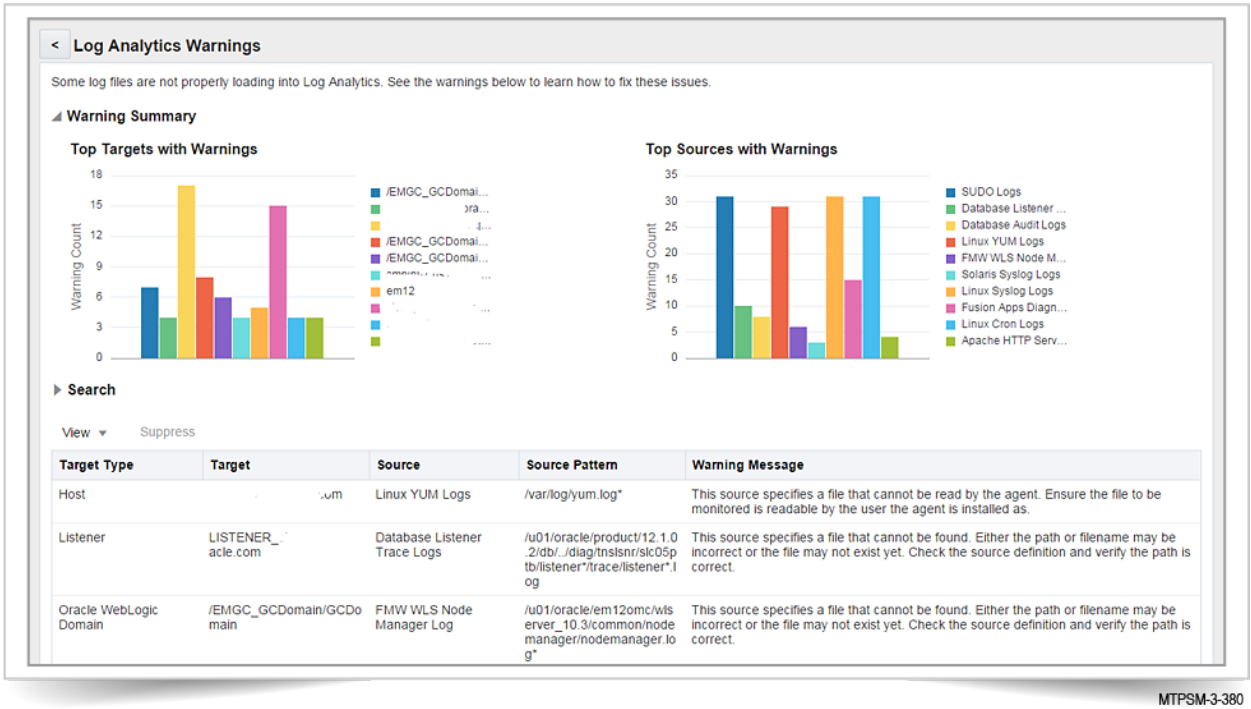


Figure 3.10.1-24. Oracle Log Analytics Cloud Service Dashboard. Oracle Log Analytics Cloud Service is used to monitor, aggregate, index, and analyze all log data from multiple sources to detect system anomalies.

Oracle Connection Manager (OCM)

Access to the Oracle databases by Team CNSI personnel is monitored and audited using OCM. Oracle Connection Manager is a multipurpose networking solution that offers increased scalability, multiprotocol connectivity and secure network access control. OCM includes the following features:

- Connection multiplexing
- Access control
- Source routing
- Multiprotocol Support
- Firewall Proxy Support

All client and application access to the databases must flow through the OCM. By using multiplexed network connections, OCM acts as a connection concentrator to “funnel” multiple client database sessions across a single network connection. Data download limits are enforced via OCM to prevent mass download of information from the system. This prevents intruders from doing a wholesale data dump limiting exposure if there is an account that has been compromised. Any requests out of the proper norms automatically triggers alerts to operations staff. Access to data for download is bound by RBAC rules to prevent access to information the person is not authorized to access. All data access is logged, and unusual activity generates alerts.

SEC07

The Contractor’s solution shall automatically maintain an audit trail of users, including database administrators, who pass through or view a record, regardless of whether data is changed.

Team CNSI's evoBrix PMIS solution includes a robust and comprehensive auditing solution that is used to record both data changes and data access. This solution includes Oracle database auditing, Oracle Log Analytics Cloud Service and OCM's audit framework and it is applicable for all users including administrators.

Oracle Database Auditing

Team CNSI uses Oracle database auditing to generate audit records for all users who are accessing the database. The audit records are stored in a syslog audit trail. Since the DBA cannot modify a syslog audit trail, audit records stored using this method is more secure than audit records stored using an operating system audit trail.

Oracle Log Analytics Cloud Service

Team CNSI uses Oracle Log Analytics cloud service to consolidates audit data from databases (syslog audit trail), operating systems, applications, firewalls, and directories into a central reporting repository for compliance reporting and alerting. This service allows for full reporting on additions, modifications, deletions, and access to data within the system.

Oracle Connection Manager (OCM)

Access to the Oracle databases by Team CNSI personnel is monitored and audited using OCM. All client and application access to the databases must flow through the OCM and the audit trail is recorded within the audit framework of OCM.

Application Audit Framework

Team CNSI's evoBrix PMIS solution has a comprehensive data model that supports record level history/ versioning and audit capability. evoBrix captures every change in the system and maintains the history, providing the information for a specific period. It also captures audit information, such as what changes have been made, who made the changes, and when. Based on Team CNSI's extensive experience in implementing and supporting operations for multiple States, we have refined an approach to support an audit trail of all pertinent events, giving due consideration to storage space and performance constraints. Changes, additions, or deletions to data (including operational and security data) and the associated errors or exceptions, if any, are tagged with information that includes the originating source (such as a specific inbound interface from a designated source, a business operations user making a change in the system, etc.), the date/time along with information about the user who initiated the change. Any errors captured as part of the data updates received from an external interface through the ESB is sent as a back feed to the designated source through an outgoing interface. The source system then verifies and performs necessary actions on the data. The corrected data is received in MT PSM in the next interface run.

Team CNSI's evoBrix PMIS solution for MT PSM maintains a complete audit trail of changes made to any data stored in the system. This includes both reference and transactional data. Audit trail entries include the following data elements that are also available for reporting purposes:

- Effective date: The date evoBrix PMIS began using the updated information
- From date: The beginning date of the effective date span
- To date: The end date of the effective date span
- Date Modified: The date the change was applied to the system
- Modified By: User ID of the person or system acting on the change
- Short Description: The short description of the reference code
- Long Description: The long description of the reference code

- Operational Flag: A flag that shows whether the system is actively using the information (Active) or has been "soft-deleted" and is retained only for historical purposes (Inactive)
- Remark: A free-form text entry field that allows the user to provide a narrative statement concerning the action taken

SEC08

The Contractor's solution shall have security audit trail reporting capabilities (e.g. security, level, locale, IP address, user ID, before and after changes).

Team CNSI's evoBrix PMIS solution includes a robust and comprehensive auditing solution covering database, network, and application layers. On the database and network layers, the audit solution comprises Oracle database auditing (fine grained auditing), Oracle Log Analytics Cloud Service, and OCM's audit framework. Additional details of these tools and their capabilities are explained in the SEC07 requirement. On the application layer, the solution offers a configurable Security Framework that maintains a complete audit trail of accesses and changes made to any data stored in the system.

Utilizing these audit solutions, Team CNSI is able to:

- Log every auditable event in application, database, and network layers
- Report on every auditable event
- Protect all logs from unauthorized modification or deletion
- Protect all logs from unauthorized viewing
- Provide users the ability to generate reports based on ranges of dates
- Be configured to ensure compliance with related Federal and State audit requirements

Application Tier Audit

Team CNSI's application security solution is built on a RBAC model, which is based on the Principle of Least Privilege and is augmented by a configurable Application Security Framework.

Role Based Access Control (RBAC)

The RBAC model allows easy, granular control for access to information. The RBAC controls are designed to NIST control standards for authentication and accounting solutions. Users only see the information to which they are authorized to have access; if a user is not authorized to view a set of information, the information is automatically restricted from view. User access to information is easily controlled by the assignment or removal of specific roles to the person. The RBAC model reduces the cost of identity security management and lowers the risk of accidental release of sensitive data. The RBAC model is proven, tested, and currently operational in Michigan, Utah, Illinois, and Washington projects that are managed by Team CNSI. There are four levels of users in our solution, each with a different security role, and all levels of user access are audited and monitored by the Application Security Framework.

1. View only User
2. Regular User
3. Super User
4. Administrator User

Application Security Framework

On the application layer, the solution offers a configurable Security Framework that provides a secure environment for information management and protects against unwanted loss or disclosure of data. Team CNSI's Application Security Framework maintains extensive user audit logging for the audit trail in support of HIPAA Security and Privacy to track changes made to any data stored in PMIS. Authorized users can access audit trail information using the web portal to keep track of who initiated the change, what changed, when the change was requested, who approved/denied the change, and when was it was approved/denied. The solution provides the ability to reverse or back out changes made in error while still retaining the associated audit trail.

The audit record records the following important elements of the current user's session:

- User ID
- Domain Name
- Audit Date
- Application Server ID
- Session ID
- IP Address
- Remarks

Database Tier Audit

Database auditing is built upon Fine-Grained Auditing (FGA) which enables a user to monitor data access based on content. The audit record records the following important elements of the current user's session:

- Operating system username
- User ID
- Client Host machine name and IP Address
- User's Terminal name
- Date and time of the creation of the audit trail entry
- Owner of the object
- Object name
- SQL Text of the query
- Data elements of the query (before and after changes)
- SQL statement type (Select or DML)

This auditing solution not only meets the audit trail requirements of the State but also provides extensive reporting capabilities using the data elements defined in the audit record.

- Data visualization using Charts and Controls
- Custom Out-of-the-box widgets
- Custom dashboards
- Log Search capability
- Anomaly detection using outliers

SEC09

The Contractor's solution shall ensure the audit trail that cannot be modified.

Team CNSI's audit solution generates audit records using Oracle Database Auditing. Audit polices are defined in the databases across multiple users covering different SQL types (SELECTs, DDLs, DMLs) and the audit records generated from this database auditing is stored either as an operating system audit trail or syslog audit trail.

Syslog Audit Trail

One potential security vulnerability for storing audit records in an operating system audit trail is that a privileged user, such as a DBA, can modify or delete audit records. To minimize this risk, Team CNSI stores the audit records in a syslog audit trail. Syslog is a standard protocol on Unix- and Linux-based systems for logging information from different components of a network. Thus, a privileged user does not have permissions to access the file system where these messages are logged. For this reason, audit records stored using a syslog audit trail are more secure than audit records stored using an operating system audit trail.

Oracle Log Analytics Cloud Service

Team CNSI uses Oracle Log Analytics cloud service to consolidates audit data from databases (syslog audit trail), operating systems, applications, firewalls, and directories into a central reporting repository for compliance reporting and alerting. Based on the separation of duties principle, only Team CNSI's security architect has administrative access to this cloud service. All other administrators including database administrators and system administrators have read-only access to generate audit reports.

SEC10

The Contractor's solution shall contain information determined by the Department and must meet Health Information Technology for Economic and Clinical Health Act (HITECH) auditing standards.

Team CNSI's evoBrix PMIS solution is hosted on FedRAMP and HIPAA compliant data centers in Oracle Government Cloud. Additionally, Team CNSI's evoBrix PMIS solution is HIPAA compliant, including all requirements and standards of the Health Information Technology for Economic and Clinical Health Act (HITECH) act. HITECH audit standards are comprehensive and involve multiple audit standards. Team CNSI's evoBrix PMIS solution is compliant with all these HITECH audit standards, and the compliance factors for these standards are explained in detail in Figure 3.10.1-25.

Audit Standard	Compliance Factor	Proposal Section
Identify the capabilities of applications and systems to understand what is auditable; disparate systems may require modified audit plans.	Team CNSI's evoBrix PMIS has robust and multi-tier audit system with a centralized repository to store and preserve the audit data	SEC07
Create and place warning banners on network and application sign-on screens to notify computer users that activities are being monitored and audited to help enforce workforce awareness.	All access to Team CNSI's evoBrix PMIS includes appropriate security warning banners including banners for application access as well as for backend system access	SEC62
Involve application and system owners, when appropriate, to determine what user activities should trigger an entry in the audit trails.	Team CNSI's evoBrix PMIS includes an audit trail of users, who pass through or view a record, regardless of whether data is changed. It also tracks and detects usage anomalies, system misuse, intrusions and hacking incidents	SEC06

Audit Standard	Compliance Factor	Proposal Section
Determine how random audits will be conducted as well as the frequency of those audits.	Team CNSI's evoBrix PMIS includes periodic risk based assessments based on NIST SP 800-53 rev4 standards and periodic penetration testing.	SEC55
Develop a standard set of process and documents for incident reporting	Team CNSI's Monitoring System is backed up by a comprehensive Incident Management Plan which includes the processes and procedures to report both successful and unsuccessful incidents, plan strategies and perform mitigation activities	SEC45
Determine what audit tools will be used for automatic monitoring and reporting	Team CNSI's evoBrix PMIS solution includes a robust and comprehensive auditing solution that is used to record both data changes and data access.	SEC07
Determine what to Audit	Team CNSI's evoBrix PMIS mandatorily audits access to all PHI and PII data elements which includes the following 18 HIPAA identifiers. ■ Name ■ Address (all geographic subdivisions smaller than state, including street address, city county, and zip code) ■ All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89) ■ Telephone numbers ■ Fax number ■ Email address ■ Social Security Number ■ Medical record number ■ Health plan beneficiary number ■ Account number ■ Certificate or license number ■ Any vehicle or other device serial number ■ Web URL ■ Internet Protocol (IP) Address ■ Finger or voice print ■ Photographic image ■ Any other characteristic that could uniquely identify the individual	SEC07
Implementing Audit Tools	Team CNSI's evoBrix PMIS solution includes an extensive and reliable auditing solution that is used to record both data changes and data access. This solution includes Oracle database auditing, Oracle Log Analytics Cloud Service and OCM's audit framework and it is applicable for all users including administrators.	SEC07 SEC06
Protecting and Retaining Audit Logs	Team CNSI's Audit system includes the following features: ■ Stores audit logs and records on a server separate from the system that generates the audit trail ■ Restrict access to audit logs to prevent tampering or altering of audit data ■ Retain audit trails based on a schedule determined collaboratively with operational, technical and risk management staff	SEC07

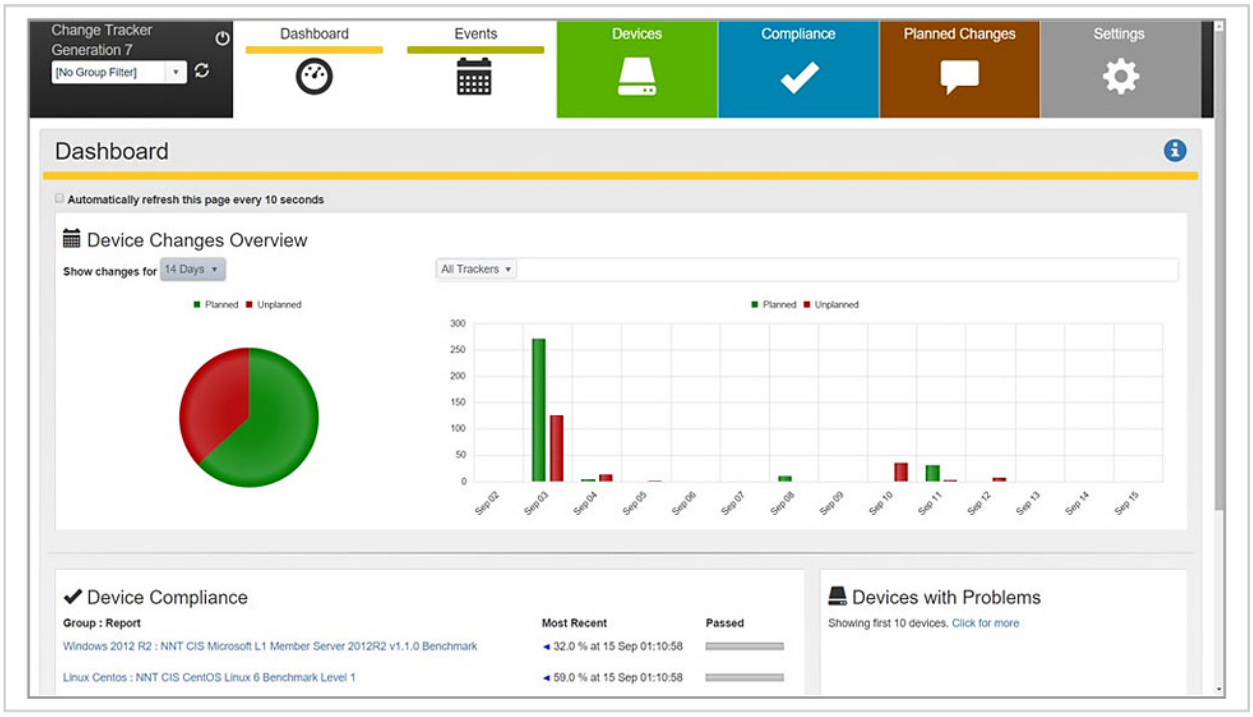
Figure 3.10.1-25. Compliance with HITECH Audit Standards. Team CNSI's evoBrix PMIS solution is compliant with HITECH audit standards based on these compliance factors.

SEC11

The Contractor shall perform risk assessments per the Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach NIST SP 800-53 Rev 4. Risk assessments shall be completed on an annual basis and when additions or changes to

functionality impact the security framework, architecture or when a new vulnerability exists.

Team CNSI's evoBrix PMIS undergoes risk assessment covering National Institute of Standards and Technology (NIST) SP 800-53 Rev 4 standards using New Net Technologies (NNT) Change Tracker product. Change Tracker's built-in NIST 800-53 report assesses the configured state of our system for compliance with the key NIST Security Controls. The result is a simple percentage score with clear remediation guidance, wherever non-compliance is highlighted. Thereafter Change Tracker provides real-time monitoring of core configuration settings covering installed software, running processes, services and startup states, registry keys, user accounts, audit and security policy, open network ports, and the overall integrity of the filesystem. Figure 3.10.1-26 provides a sample dashboard of NNT Change Tracker's dashboard.



MTPSM-3-425

Figure 3.10.1-26. NNT Change Tracker Dashboard. A sample dashboard of NNT Change Tracker's product that is used for performing risk assessments based on NIST 800-53 rev4 standards.

This full security risk assessment is based on the following standards:

- NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations standards
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems

This full security risk assessment covering NIST SP 800-53 Rev 4 is conducted in the following situations:

- Annual basis

- Whenever new or modified functionality impacts the security framework or architecture
- Whenever a new vulnerability exists

The results are reported using a plan of action and milestones (POA&M) format and all security gaps are remediated within appropriate timeframes. Systems security is maintained per the system security plan with regular system audits. Team CNSI's evoBrix PMIS solution is monitored and protected by different PaaS services within the security suite of the Oracle Cloud. These PaaS services help to identify usage anomalies and system misuse. The solution suite includes Oracle SMA Cloud Service, Oracle Log Analytics Cloud Service and OCM. All vulnerabilities are remediated and then the systems rescanned to ensure proper closure of vulnerabilities. Additional security scans are performed periodically on all systems, and whenever changes are made on the systems that could impact the security framework.

SEC12

The Contractor's solution shall manage role-based permissions and provide a National Institute of Standards and Technology (NIST) compliant identification, authentication and accounting solution.

Team CNSI's application security model is built on a RBAC model, which allows easy, granular control for access to information. The RBAC controls are designed to NIST control standards for authentication and accounting solutions. Users only see the information to which they are authorized to have access; if a user is not authorized to view a set of information, the information is automatically restricted from view. User access to information is easily controlled by the assignment or removal of specific roles to the person. The RBAC model reduces the cost of identity security management and lowers the risk of accidental release of sensitive data. The RBAC model is proven, tested, and currently operational in Michigan, Utah, Illinois, and Washington projects that are managed by Team CNSI.

The use of the RBAC model in the system ensures full confidentiality of PHI and PII information. Users of the system can only access a limited set of data based on their authorization in the system. The system facilitates easy removal of people from the list of those who are authorized to view information. The RBAC model ensures that the user can only alter or modify data that they are authorized to access and change.

All access to the data is tracked within the system. All transactions are monitored and recorded using application-level auditing and database auditing using Oracle Database Auditing. This allows for a full audit trail of who accessed what information, and who modified what information. The audit trail gives the State and Team CNSI a solid set of tools to respond to any inquiries and assertions that there are issues with records. The evoBrix PMIS tracks all changes using Oracle Database Audit and records all identity data. Every change to a record and all views of data in the system are recorded; the name of the person accessing the system and the date and time that they performed the actions are recorded.

SEC13

The Contractor's solution shall have multiple layers of external and internal security that provide administrative, physical, and technical mechanisms to protect sensitive or confidential information used in performing the responsibilities and duties defined for the module scope of work.

Team CNSI has implemented a robust security framework for ensuring Confidentiality, Integrity, and Availability. This is known as the CIA Triad and this provides multiple layers of external and internal security to protect sensitive and confidential information. This triad includes various administrative,

physical and technical mechanisms that are required to protect the sensitive information. A combination of encryption solutions, multi-tiered network with layered security, intrusion detection and prevention systems upholds the Confidentiality area of the Triad while multi-factor authentication, auditing, access management and log management supports the Integrity area of the Triad. High Availability architecture, multi-site design, robust system monitoring and alerting framework forms the Availability area of the Triad. Figure 3.10.1-27 provides an overview of the CIA Triad which enforces that Confidentiality, Integrity and Availability is the forefront for Team CNSI's system security design

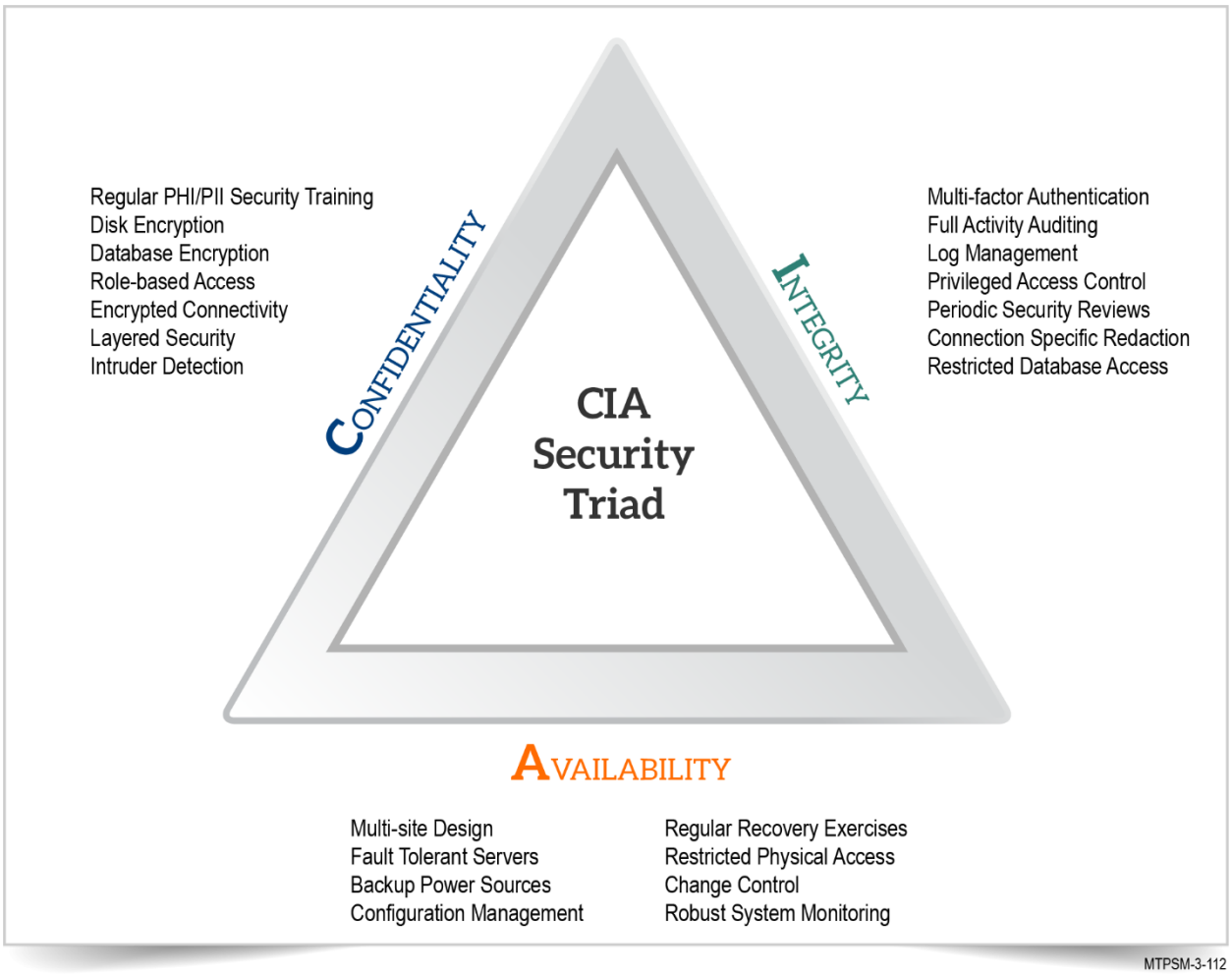


Figure 3.10.1-27. The CIA Security Triad. Confidentiality, Integrity, and Availability are the forefront of Team CNSI's system security design.

Data protection is the primary goal of the Team CNSI system security design. The primary defense is the tiered design of the system. All data is guarded behind multiple layers of security. The user accesses the evoBrix PMIS only after authenticating to the MT PSM system. The user then accesses the front-end web server in the DMZ. The firewall only allows access to the web ports of the server. The web server is allowed access through the firewall to the presentation server. The presentation servers in the presentation layer are allowed access to the application servers through the firewall between those two partitions. The application servers are allowed through the next firewall to the database servers. Thus, the most sensitive data is housed deep in the system behind multiple network firewalls to protect against network penetration. All Oracle databases are additionally protected by Oracle firewalls designed specifically for database protection. The Oracle databases are also protected by use of the OCM. Connectivity to the

databases is limited to the OCM and the application servers only. All client and application access to the databases must flow through the OCM or through the system of the web server/presentation server/application server chain.

SEC14

The Contractor's solution shall not include any code of unknown origin.

Team CNSI's MT PSM solution will not include any code of unknown origin. The evoBrix PMIS is managed and monitored using a robust configuration management system. All changes to the system at both operating system and application levels are monitored by the configuration management system. This prevents unauthorized applications or software code from being installed or loaded on the system. Configuration management also ensures that any changes to configuration or setup files are authorized changes.

Figure 3.10.1-28 lists the types of CIs that exist on the project. The list of CMDB tools and their respective CIs are specified in Figure 3.10.1-29.

Type of CI	Description
Source Code	Project source code
Status Records	Records in Jira or SharePoint providing a snapshot of the CI status
Hardware	Servers and routers that help implement the project activities

Figure 3.10.1-28. Types of CIs. Various types of CIs tracked in Team CNSI's evoBrix PMIS.

Figure 3.10.1-29 lists the applicable CMDB for each of the CIs in the system.

Name	Type of CI	Repository	Configuration Control Trigger
Java, JSP, XML, JS, PL/SQL, SQL, CSS, HTML, Images	Source code	Subversion	Initiation of the project
Source Code Defects/Enhancement Requests	Status Records	Jira	Submission to State
Servers, Routers, Switches	Document	iTOP/Wiki	Initiation of the Project

Figure 3.10.1-29. Items Under Configuration Management. Lists each type of CI, repository where it is stored and the phase that the CI is placed under configuration control.

In addition to a robust configuration management system, Team CNSI employs best practices for code management. Rather than relying on disparate source code libraries, we house a centralized code repository to maintain all solution dependent libraries. All open source libraries utilized by our evoBrix PMIS solution must be Free and Open-Source Software (FOSS) compliant. The goal of the FOSS compliance process is to ensure that all software (proprietary, third-party, or FOSS) gets reviewed and certified for license compliance. FOSS compliance audits are executed and tracked via the following process:

1. Scan the source code using Rogue Wave
2. Identify and resolve any discovered issues
3. Perform license review
4. Perform architectural review
5. Approve or Deny software component compliance

Once it passes the FOSS compliance audit, these libraries are uploaded into the centralized code repository and are available for use in the evoBrix PMIS solution. This well-defined process provides better control over source code and prevents the use of unauthorized applications or software code from being a part of the solution.

SEC15

The Contractor shall provide an independent third party to perform penetration testing within six (6) months prior to implementation. Penetration testing must also be performed by an independent third party on an annual basis and when additions or changes to functionality impact the security framework, architecture or when a new vulnerability exists. Penetration Test Report results shall be supplied to the Department and any major or critical vulnerabilities mitigated.

Team CNSI's evoBrix PMIS solution will be hosted in Oracle Government Cloud. In the Oracle Government Cloud, penetration testing is performed by a third-party audit firm periodically and it covers the following test services

- External Penetration Testing – Web application penetration testing
- Internal Penetration Testing – Black Box testing
- Network security scanning
- Network and Application vulnerability tests

Penetration Testing will be conducted in the following time periods and the resultant test reports will be submitted to DPHHS. If there are any major or critical vulnerabilities, a mitigation plan will also be provided by Team CNSI to DPHHS.

- Within 6 months prior to implementation
- Annual basis
- Whenever new functionality impacting the security framework gets added or modified

SEC16

The Contractor shall provide the primary and disaster recovery facility(s) which will ensure security, performance and disaster recovery requirements outlined in the module scope of work.

The Team CNSI evoBrix PMIS solution is hosted in Oracle's FedRAMP Government Cloud. The primary data center is in Chicago, IL, and the Disaster Recovery (DR) Data Center is in Ashburn, VA. The sites are geographically separated to protect from environmental hazards. The remote site is a warm failover site with all data actively replicated from the primary site to the remote site. In the event of the loss of the primary site the system is reconfigured to bring up the evoBrix PMIS on the remote site.

The secondary site is fully equipped and meets all the same security standards and performance requirements as the primary site. The secondary site has all the same backups and redundant systems as the primary site. This is to ensure that system operations run smoothly in the event of a disaster and that there are no security or performance issues when running DR site becomes operational. Additional details about the primary and secondary site and its architecture are explained in detail in the ENV02 requirement.

The disaster recovery procedures are tested on an annual basis to ensure full protection. Based upon our annual testing, the secondary site becomes fully operational within four hours. Team CNSI's DR solution comprises Oracle Data Guard and Rsync solutions.

- Oracle Data Guard is used to replicate changes in the production database to the DR site. If a disaster should occur and the production database server is not functioning, the DR site replica is activated. The transfer of changes from production to the DR site is done asynchronously to ensure no performance degradation on the production servers.
- Rsync is used to replicate non-database-related files. Much like the replication service provided by Oracle Data Guard, CNSI has established online, near real-time file replication using rsync and demonstrated this approach as a superior solution in our Washington and Michigan MMIS solutions. Rsync is a standard tool available in UNIX environments. CNSI has established this replication feature that keeps non-database data backed up more frequently than is typically possible using only traditional backup methods.

Team CNSI determines the critical and non-critical business functions for the disaster recovery purpose and documents them in the DR Plan. This plan defines procedures and processes to recover the system from a disaster at the State's primary data center site. A disaster, for purposes of this document, is defined as an event or occurrence which directly or indirectly impacts the processing capabilities of the system, causing a loss of critical service, exceeding defined limits, such that a decision is made to restore operations at a pre-determined alternate facility. This process is documented thoroughly and separately. To ensure any potential DR event is successful, Team CNSI provides a Disaster Recovery Test Plan that is executed annually. In other Team CNSI Medicaid solutions that have been operational since 2010, we successfully passed annual DR testing requirements using this model.

SEC17

The Contractor shall maintain policies and procedures for security clearance and staffing controls for allowing access to confidential information and/or to restricted areas within the Contractor's solution.

Team CNSI's proposed solution includes access controls that provides the system the ability to control, restrict, monitor, and protect resource availability, integrity and confidentiality. These access controls are designed and implemented based on the following principles:

- Principle of Least Privilege: If nothing has been specifically configured for an individual or the groups one belongs to, the user should not be able to access that resource (Default no access)
- Separation of Duties: Separating any conflicting areas of responsibility so as to reduce opportunities for unauthorized or unintentional modification or misuse of organizational assets and/or information.
- Need to know basis: It is based on the concept that individuals should be given access only to the information that they absolutely require in order to perform their job duties

In Team CNSI's proposed system, the policies and procedures for security clearance and staffing controls are classified into 3 categories

- Physical Access Controls
- Technical Access Controls
- Administrative Access Controls

Physical Access Controls

These physical access controls focus on supplying the right degree of access control by implementing various physical mechanisms that are described below

- Network Segmentation and Network Firewalls: Team CNSI's multi-layered security architecture ensures security and protection by placing the most sensitive portions of the system behind multiple security layers with a tiered architecture. This tiered approach includes network segmentation and firewalls, and it creates the most secure environment, putting up multiple defenses that secure information from attackers
- Data Backups: Team CNSI has developed and implemented a Contingency Plan for the evoBrix PMIS solution. Team CNSI tests the Contingency Plan every 12 months including the backup media testing. If testing reveals that the Contingency Plan is ineffective in the event of an emergency or other occurrence, Team CNSI revises the plan accordingly. The Contingency Plan addresses:
    - Backups – the strategy and procedures for creating and maintaining system and data backups
    - Disaster Recovery – procedures to restore any lost data or functionality in the event of a system outage or other emergency
    - Emergency Mode Operations – procedures to enable continuation of critical business processes and maintain the integrity of ePHI while the information system that normally provides the information is unavailable
- Perimeter Security: Team CNSI's system is hosted in Oracle Government Cloud. These cloud data centers include the following perimeter security mechanisms:
    - Physical access requires authorization and is monitored.
    - All employees and visitors must visibly wear official identification while onsite.
    - Visitors must sign a visitor's register and be escorted and/or observed while onsite.
    - Possession of keys/access cards and the ability to access the locations is monitored. Staff leaving Oracle employment must return keys/cards.
    - Closed Circuit TV (CCTV) monitoring.
    - Entrances are protected by physical barriers designed to prevent unauthorized entry by vehicles.
    - Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management.
    - Mantrap doors.
    - Motion detectors and alarms.

Technical Access Controls

Technical access controls are products or tools that restricts access to Cloud IT assets. They protect the integrity and availability of resources by limiting the number of subjects that can access them and protect the confidentiality of resources by preventing disclosure to unauthorized subjects.

- Encryption and protocols: Team CNSI employs a defense-in-depth approach to securing our solution by implementing multiple layers of network, system, and database encryption technologies to ensure all classified and potentially sensitive data is encrypted at rest and in transit. These controls are used to protect data when it is at rest and when it passes throughout the network. They preserve the confidentiality and integrity of data and enforce specific paths for communication to take place.
- Auditing: Team CNSI's evoBrix PMIS solution includes a robust and comprehensive auditing solution that is used to record both data changes and data access. This solution includes Oracle

database auditing, Oracle Log Analytics Cloud Service and OCM's audit framework and it is applicable for all users including administrators.

- Usage anomalies: Team CNSI's evoBrix PMIS solution is monitored and protected by various PaaS services within the security suite of the Oracle Cloud. These PaaS services help to identify usage anomalies and system misuse. The solution suite includes Oracle SMA Cloud Service, Oracle Log Analytics Cloud Service, and OCM. These tools enable rapid detection, investigation, and remediation of the broadest range of security threats across Team CNSI's cloud IT assets.
- Network Architecture: This control defines the logical and physical layout of the network, and also the access control mechanisms between different network segments. A combination of ACLs, routers, and firewalls help to enforce this access control.

Administrative Access Controls

Administrative access controls encompass procedures and policies that are aimed at enforcing process oriented access controls. This includes defining a security policy and procedure, security-awareness training and testing process.

- Policy and Procedures: Team CNSI's evoBrix PMIS includes a well-defined and proven security policy. This policy clearly states a high-level plan that states management's intent pertaining to how security should be practiced within our organization, what actions are acceptable, and what level of risk the company is willing to accept.
- Security-awareness training: All Team CNSI employees, contractors, and subcontractors undergo annual training on all privacy and security policies and also comply with the Business Associate Agreement, as required by the contract, CMS and federal and state requirements.
- Testing: This control states that all security controls, mechanisms, and procedures are tested on a periodic basis to ensure that they properly support the security policy, goals, and objectives set for them.

SEC18

The Contractor shall maintain adequate technical support/staffing to provide 24x7x365 coverage.

During Solution, Configuration, and Implementation (SCI) and operations phase, Team CNSI proactively monitors all infrastructure components as well as defined performance standards to ensure that we meet contract SLAs and performance metrics. Team CNSI's SLA governance processes establish and document all performance measurement criteria, along with the processes and procedures for monitoring, reporting on, and correcting any deficiencies.

Team CNSI's evoBrix PMIS solution includes a comprehensive and complete system monitoring and reporting framework. This framework ensures that the high-availability components are working properly across the system. OEM, HealthBeat, BMS, and DCIM provide monitoring and reporting capabilities covering all layers of hardware and software components. Figure 3.10.1-30 provides a classification of monitoring tools and their respective infrastructure modules

Monitoring Tool	Infrastructure Modules
Oracle Enterprise Manager	Databases and Database Servers SOA Suite Application Servers

Monitoring Tool	Infrastructure Modules
HealthBeat	Application Interfaces/Web Services Servers
Building Management System	Data Center Power and Cooling
Data Center Infrastructure Management	Infrastructure

Figure 3.10.1-30. Monitoring and System Performance Reporting Tools. This classification of monitoring tools and their associated infrastructure modules forms the backbone of the monitoring framework.

Notification alerts and emails from these reporting components are sent to the NOC Team, which is staffed 24x7x365. The NOC Team does the initial triage and then informs/notifies the appropriate operations teams for further action. They also maintain contact information for each level of support. Team CNSI's operations team are divided into four tiers:

- NOC/Help Desk Team
- Operations Support Team
- Application Services Team
- Infrastructure/Back-end Team

Once NOC Team does the initial triage of the notification alerts or email or ticket, they inform/call the appropriate operations team for further action. Each team is governed by an SLA for triaging these tickets or notification alerts. Figure 3.10.1-31 shows the response time for tickets triaged by each team.

Tier	Team CNSI Area(s)	Details	Availability	Response
1	NOC/Help Desk	■ Ticket triage ■ Monitor system performance and operations processes ■ General, application processing, access requests, and technical inquiries	■ 24x7x365	■ 30 minutes
2	Operations Support	■ Manages and supports all operational activities to ensure systems and processes are running effectively to maintain SLA compliance and responding to requests/issues accordingly ■ Tracking, facilitating, and coordinating tickets and operations processes ■ Operations processes include access requests, Incident Management, Event Management, Release Management, Change Requests, and SLAs	■ On Call (24x7x365)	■ 1 hour
3	Application Services	■ Triage, prioritize, and support tickets, incidents, and requests ■ Follows the DevOps model and collaborates closely with their business counterparts	■ On Call (24x7x365)	■ 1 hour
4	Infrastructure/ Back-End	■ Plan, monitor, maintain, and provide incident response for the infrastructure	■ On Call (24x7x365)	■ 1 hour

Figure 3.10.1-31. Team CNSI's System Support Model. Team CNSI establishes systematic processes to provide event/incident management support based on ITILv3.

SEC19

The Contractor's data encryption solution shall meet Federal Information Processing Standard (FIPS) 140-2 and at a minimum use AES 128 encryption.

Team CNSI evoBrix PMIS supports protection of confidentiality of all PHI delivered over the internet or other known open networks via encryption using AES and an open protocol TLS, SSL, IPsec, XML encryptions, or S/MIME or their successors. The system employs a defense-in-depth approach to securing our solution by implementing multiple layers of network, system, and database encryption technologies to ensure all classified and potentially sensitive data is encrypted at rest and in transit. We have extensive experience with these encryption technologies, through our implementations in our Michigan, Illinois, Utah, and Washington MMIS solutions. Figure 3.10.1-32 provides an overview of all the encryption solutions that are used in Team CNSI's evoBrix PMIS, thus meeting the Federal Information Processing Standard (FIPS) 140-2 standard.

Tier	Component	Encryption Method	Encryption Algorithm
Database Tier	Data Files	Oracle Transparent Database Encryption	AES-256
Database Tier	Encryption Keys	Oracle Key Vault	PKCS#12 file
Database Tier	Backups	Oracle RMAN Encryption	AES-256
Storage Tier	Oracle Data Pump Exports	Oracle Data Pump Encryption	AES-256
Storage Tier	Flat Files (at rest)	Linux eCryptfs	AES-256
Storage Tier	Flat Files (in transit)	Titan SFTP	SHA-1
Network Tier	Data Traffic	Oracle Network Encryption	AES-256
Network Tier	Data Integrity	Oracle Data Integrity	SHA-1
Application Tier	Network Traffic	SSL Encryption	256 bit SSL
Physical Transmission	Disks/Disk Partition	IDRIX VeraCrypt	AES-256

Figure 3.10.1-32. Data Encryption Solutions. An overview of Data Encryption solutions that are used in Team CNSI's evoBrix PMIS.

Database Tier

At the database layer, Team CNSI leverages advanced Oracle security tools, which ensures strong encryption of databases containing sensitive information such as PII and PHI.

- Oracle TDE: Team CNSI uses TDE to encrypt sensitive data at rest. Data is encrypted at the tablespace level using AES-256 algorithm. The encryption keys are stored in a wallet and the wallet is also secured, stored and backed up using Oracle Key Vault
- Oracle Key Vault: Team CNSI uses Oracle Key Vault to ensure protection of encryption keys. Oracle Key Vault is used to centrally authorize, secure, and manage all encryption keys. Oracle Key Vault is a FIPS 140-2 Level 3 compliant key management system, offering a strong and scalable solution.
- Oracle Backup Encryption: Team CNSI uses Oracle RMAN and Local TDE master encryption key to encrypt all database backups including full backups, incremental backups and archive log backups. This ensures that backups, which are usually stored in offsite locations, are secured.

Storage Tier

- Oracle Data Pump Encryption: Team CNSI uses Oracle Data Pump product for taking exports of database schemas and tables. The dump files that are generated by Oracle Data Pump are encrypted using Oracle Data Pump Encryption and the encryption algorithm is AES-256.
- Flat File Encryption at Rest: Team CNSI uses eCryptfs utility within Oracle Linux to encrypt a file system. This utility is used to encrypt individual files and directories using AES-256 algorithm.
- Flat File Transfer Encryption: Team CNSI uses Titan Secure FTP to ensure encryption of the file in transit.

Network Tier

- Oracle Database Network Encryption: Team CNSI uses AES-256 based network encryption to encrypt data in transit, thus ensuring that data is secure, as it travels across the network.
- Oracle Data Integrity: Team CNSI uses Secure Hash Algorithm 1 (SHA-1) based Data Integrity protection to safeguard data against Data modification attacks and replay attacks.
    - Data modification attack: An unauthorized party intercepting data in transit, altering it, and retransmitting it is a data modification attack
    - Replay Attack: Repetitively retransmitting an entire set of valid data

Application Tier

At the application layer, all user sessions to and from the application are encrypted with 256bit SSL. This approach provides end-to-end network security, reducing the system's exposure to potentially malicious internet traffic and mitigating the possibility of internet-based attempt to defeat critical safeguards that could expose sensitive personal, health, or financial information.

Physical Transmission

Team CNSI's evoBrix PMIS solution does not normally require physical transmission of data using disks or disk partitions. However, when a need arises, then Team CNSI uses IDRIX VeraCrypt, which is an open source disk encryption utility. This utility is used to perform on-the-fly encryption of disks and disk volumes using AES-256 algorithms.

SEC20

The Contractor shall ensure that all data, regardless of its location, is encrypted at rest.

The Team CNSI evoBrix PMIS solution for MT PSM protects confidentiality by encrypting all data at rest, thus ensuring that the system is compliant with FIPS 140-2 standard. All data, across different tiers, is encrypted at rest and this is the basis for our security architecture.

Oracle Transparent Database Encryption (TDE)

Team CNSI uses TDE to encrypt data at rest within the data files. Data is encrypted at the tablespace level using AES-256 algorithm. The encryption keys are stored in a wallet and the wallet is also secured and backed up using Oracle Key Vault.

Oracle Key Vault

Centralized key management is another element within Team CNSI's security layer to reduce exposure of sensitive data and ensure reliability and security of the solution. To ensure protection of encryption keys, we leverage Oracle Key Vault to centrally authorize, secure, and manage all encryption keys. Oracle Key Vault is a FIPS 140-2 Level 3 compliant key management system, offering a strong and scalable solution.

Oracle Backup Encryption

Team CNSI uses Oracle RMAN and Local TDE master encryption key to encrypt all database backups including full backups, incremental backups and archive log backups. This ensures that backups, which are usually stored in offsite locations, are also secured.

Oracle Data Pump Encryption

Team CNSI uses Oracle Data Pump product for taking exports of database schemas and tables. The dump files that are generated by Oracle Data Pump are encrypted using Oracle Data Pump Encryption and the encryption algorithm is AES-256

Flat File Encryption at Rest

Team CNSI uses eCryptfs utility within Oracle Linux to encrypt a file system. This utility is used to encrypt individual files and directories using AES-256 algorithm.

Physical Transmission

Team CNSI's evoBrix PMIS solution does not normally require physical transmission of data using disks or disk partitions. However, when a need arises, then Team CNSI uses IDRIX VeraCrypt, which is an open source disk encryption utility. This utility is used to perform on-the-fly encryption of disks and disk volumes using AES-256 algorithms.

SEC21

The Contractor's transmission security shall use TLS 1.2, SHA 2 with a minimum of a 2048 bit key.

The Team CNSI evoBrix PMIS solution for MT PSM encrypts all data in transit. Our security architecture and design is based on a defense-in-depth approach and encrypting the data in transit is another key feature of the system.

- All connections to the MT PSM system use SSL technology for fully encrypted connection. SSL connections use TLS 1.2, SHA 2 with a minimum of a 2048-bit key.
- All file transfer connections use secure file transfer protocols for encrypted transfer. Team CNSI uses Titan Secure FTP to ensure encryption of the file in transit and a 256bit AES encryption is used to encrypt the files.
- Administration and operational staff use encrypted VPN connectivity to access all the servers.
- All database data transferred on the network uses the Oracle network encryption and Oracle Data integrity products to protect the data in flight.

SEC22

The Contractor will provide a completed Security Audit Report with results to the Department by the 30th (thirtieth) of September each year. The Security Audit Report must include either an electronic data processing (EDP) systems audit using SSAE 16 at a minimum level service organization control (SOC) 2 Type II or a NIST 800-53 rev 4 assessment at a "moderate" system risk control level.

The Contractor shall provide a mitigation plan for all reported deficiencies. Major and critical deficiencies must be corrected within forty (40) calendar days of the report submission to the Department.

Team CNSI's evoBrix PMIS undergoes risk assessment covering NIST SP 800-53 Rev 4 standards using New Net Technologies (NNT) Change Tracker product. Change Tracker's built-in NIST 800-53 report assesses the configured state of our system for compliance with the key NIST Security Controls. The result is a simple percentage score with clear remediation guidance, wherever non-compliance is

highlighted. Thereafter Change Tracker provides real-time monitoring of core configuration settings covering installed software, running processes, services and startup states, registry keys, user accounts, audit and security policy, open network ports, and the overall integrity of the filesystem

The outcome of this security risk assessment is a Security Audit Report. This report will be submitted to DPHHS within 30th (thirtieth) of September each year. The evaluation of the security systems uses the System Security Plan (SSP) as guidance for the audit. Each security control describes what the security control covers and how to evaluate it. The assessment method section of each security control specifies what systems need to be evaluated, what tests need to be accomplished, and what personnel to interview as part of the assessment in the audit. The results are reported using a plan of action and milestones (POA&M) format and all major and critical security gaps are remediated within forty (40) calendar days of the submission of audit report.

Additionally, Team CNSI's evoBrix PMIS Solution is hosted in Oracle Government Cloud, which has the following certifications in place:

- SSAE 16 SOC 1 Type II
- SSAE 16 SOC 2 Type II
- HIPAA/HITECH
- Federal Risk and Authorization Management Program (FedRAMP)

Team CNSI's evoBrix PMIS solution includes security and privacy controls that are compliant with the most current version of the CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E) and NIST standards. Team CNSI's evoBrix PMIS solution adheres to the following security standards

- Federal Information Security Management Act (FISMA)
- Internal Revenue System (IRS) Publication 1075
- Patient Protection and Affordable Care Act (PPACA) or (ACA)
- NIST Special Publication 800-66 Revision 1
- NIST Special Publications 800-53 and 800-53A
- NIST Special Publication 800-47
- NIST Special Publication 800-88 Revision 1
- NIST Special Publication 800-111

SEC23

The Contractor's solution shall provide security features that support increasing the complexity of the authentication and authorization as the sensitivity of the data or functionality increases.

Team CNSI has contributed significantly to agency and system security plans in the states of Washington, Michigan and Utah, as well as CMS, the U.S. Census Bureau, and the DOD. In all these implementations, Team CNSI has extensive experience in handling and securing highly sensitive data including PHI and PII data. Our approach to developing security controls and procedures for the DPHHS MMIS solution is to tightly integrate these strategies and best practices we have developed, with the existing DPHHS security framework and extend or strengthen it wherever necessary.

Team CNSI's evoBrix PMIS solution will integrate with the Montana State's existing IAM infrastructure to provide a seamless IAM experience for internal and external users. Our solution will employ Oracle Access Manager to provide integration with the DPHHS system integration platform. It will consume identities provided by the DPHHS identity provider. The identity federation will use SAML 2.0.

Also, Team CNSI's evoBrix PMIS solution uses tiered system architecture to layer systems placement to give optimal protection to the most sensitive systems deep inside multiple layers of protection. The evoBrix PMIS uses RBAC policies, so that access is based on people's roles in the system. Direct server access is protected with privileged account management systems to restrict and record all direct access to backend systems. Data which is stored and transmitted in different tiers are encrypted and secured. Data present in Development and System Test environments are de-identified. All these measures are aimed at protecting and securing the data, which is highly sensitive, within evoBrix PMIS solution. If the sensitivity of the data or functionality increases, then Team CNSI's solution will provide additional security features to support complex authentication and authorization mechanisms.

SEC24

All Contractor's module components shall adhere to any applicable the Department system security practices, configurations & procedures.

Team CNSI has reviewed State of Montana's security and privacy control requirements and our proposed evoBrix PMIS does comply with these security processes.

The Team CNSI evoBrix PMIS, hosted in Oracle Government Cloud, includes security and privacy controls that are compliant with FedRAMP, HIPAA, HITECH, FISMA, and NIST standards. Detailed information about these security and compliance standards are provided in SEC22 requirement.

If DPHHS identifies any additional security practices and configurations during project performance, Team CNSI will adhere to the same by going through Enterprise Architecture (EA) review process and Change Control Board (CCB) process explained below.

- EA Review is a governance process that incorporates MITA standards to accommodate future programs and initiatives.
- CCB represents the interests of project management by ensuring that a structured process is used to decommission or procure new hardware, software and licenses. Detailed information about the CCB process is described in SEC72 requirement.

SEC25

The Contractor's solution shall provide the ability to grant authorization through role-based security (create, delete, modify and view) access to user interfaces, reports, data elements/field level, and menu items.

The Team CNSI evoBrix PMIS uses RBAC to ensure that information access is restricted to only appropriate access based on a user's roles. The RBAC system restricts access to only data the user is authorized to access, view, or modify, and allows easy, granular control for access to information. Users only see the information to which they are authorized to have access; if a user is not authorized to view the information, then it is automatically restricted from view. User access to information is easily controlled by the assignment or removal of specific roles to the person. The RBAC model reduces the cost of identity security management and lowers the risk of accidental release of sensitive data. The RBAC model is proven, tested, and currently operational in multiple states managed by Team CNSI.

The use of the RBAC model in the evoBrix PMIS ensures full confidentiality of PHI and PII. Users of the system can only access a limited set of data based on authorization in the system. The evoBrix PMIS facilitates easy removal of people from the list of authorized people to view information.

SEC26

The Contractor's solution shall allow access and role changes to be made in real-time with appropriate authorizations.

Team CNSI has a documented process and policy for User Life Cycle Management. These policies and processes are followed to manage users from creation to termination. Team CNSI's operations team has a centralized group to manage user access. Policies are created for user access requests. These requests are validated and a formal approval process is followed before any users are created and granted access. One of the most critical processes that is followed is user termination. Our operations team is integrated with Human Resources to ensure access is revoked upon employee termination.

Team CNSI's user management framework, incorporating elements of our audit and security policies:

- Enforce a limit of (configurable) consecutive invalid access attempts by a user. The System protects against further, possibly malicious, user authentication attempts using an appropriate mechanism (i.e., locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm).
- Allow users access based on their roles irrespective of their geographical location.
- Enforce minimum password requirements compliant with State-provided security policies.
- Allow a user to change his or her password at any time.
- Have mandatory security questions for the user to answer for username and password validation in case of any user requested changes.

The initial configuration and ongoing management of end-users and system administrator access to specific security module of evoBrix applications is a critical security activity. Each security level and account follows our evoBrix RBAC model. RBAC enforces access control based on domains, profiles to domains, roles, profiles to roles, user accounts, pages, and pages to specific roles. Security levels are designed and implemented to control access by end-users, system administrators, software developers, and testers performing functional testing, as well as the User Acceptance Testing (UAT) and the production environments. The RBAC enforces the most restrictive set of rights/privileges or accesses needed by users/groups or processes acting on behalf of users for the performance of specified tasks. Figure 3.10.1-33 provides an overview of different compliance factors that are built into the Team CNSI's evoBrix solution to enforces the below required security controls.

Security Control	Compliance Factors
Requires a unique sign-on (ID and password)	Each system administration account/password is unique Each end user account/password is unique
Supports a user security profile that controls user access rights to data categories and system functions	Team CNSI evoBrix PMIS solution use RBAC policies defined in our applications to control access to system functions.
Permits supervisors or other designated officials to set and modify user security access profile	Team CNSI requires verification from the State and/or designated stakeholders before account creation is initiated. Upon verification, Team CNSI systems provide ability for authorized individuals to modify user security access profiles through screens.
Alerts appropriate staff authorities of potential violations of privacy safeguards, such as inappropriate access to confidential information	The evoBrix PMIS solution notifies the systems team via email of potential risks and violations detected by our automated systems tools.

Figure 3.10.1-33. Standard Access Controls Configuration. Team CNSI collaborates with the State to ensure RBAC policies align with existing DPHHS policies.

SEC27

The Contractor's solution, in order to protect the database from SQL injection attacks, shall access the database from the application through a standard database abstraction layer.

Data protection is the primary goal of Team CNSI's evoBrix PMIS. Protecting the database from SQL injection attacks is critical to achieving this goal. Team CNSI employs different mechanisms and tools to protect the system from SQL Injection attacks, as explained in Figure 3.10.1-34.

Solution	Solution Description
Database Abstraction Layer	The evoBrix PMIS application is built in such a way that the application's presentation layer does not directly access the database and only business service layer perform database activity. There is a database abstraction framework which is built on top of JDBC. This framework uses Java classes and provides full SQL abstraction by using prepared statements with bind variables. In this method, the developer must first define all the SQL code, and then pass in each parameter to the query later. This coding style allows the database to distinguish between code and data, regardless of what user input is supplied. Prepared statements ensure that an attacker is not able to change the intent of a query, even if SQL commands are inserted by an attacker.
Data Sanitization	The evoBrix PMIS application uses strong encryption logic to encrypt all form action URL that is posted as a request to application, any request that's fails in the decryption process is returned as an invalid/bad request which prevents intrusions'. PMIS application also intercepts each request through interceptors to validate all input data that's being passed on to the application server during this validation it checks for any special characters (SQL injection) and returns as invalid request when found.
Multi-tiered network architecture	All data is guarded behind multiple layers of security. The user accesses the evoBrix PMIS only after authenticating to the MT PSM system. The user then accesses the front-end web server in the DMZ. The firewall only allows access to the web ports of the server. The web server is allowed access through the firewall to the presentation server. The presentation servers in the presentation layer are allowed access to the application servers through the firewall between those two partitions. The application servers are allowed through the next firewall to the database servers. Thus, the most sensitive data is housed deep in the system behind multiple network firewalls to protect against network penetration.
Principle of Least Privilege	The evoBrix PMIS solution code uses non-system accounts (also called as application service accounts) that have rights that are restricted to only the access needed for the application to run properly. These application service accounts follow the RBAC model that is built in the evoBrix PMIS solution which is based on the principle of least privilege. Every web application accessing the database has its own application service account. Every user accessing the database, through tools like TOAD or SQL Developer, has his/her own named user account. These application service account and named user accounts are different from the system or administrative accounts.
Continuous monitoring	Team CNSI's evoBrix PMIS solution is monitored and protected by various PaaS services within the security suite of the Oracle Cloud. These PaaS services help to identify usage anomalies and system misuse including user behavioral analysis. The solution suite includes Oracle Security Monitoring and Analytics (SMA) Cloud Service, Oracle Log Analytics Cloud Service and Oracle Connection Manager (OCM). These tools enable rapid detection, investigation, and remediation of the broadest range of security threats, including SQL injection attacks, across Team CNSI's cloud IT assets

Figure 3.10.1-34. Protection Mechanisms Against SQL Injection Attacks. Team CNSI's system includes various mechanisms and tools to protect the system from SQL Injection attacks.

SEC28

The Contractor's solution shall be easy-to-use and provide a user interface that allows authorized users to edit, create, and implement role-based and group-based security at the data element/field level for authorized users based upon individual characteristics or functional security groups.

Team CNSI's evoBrix PMIS solution has a RBAC security framework inbuilt with the solution. This framework comes bundled with a user interface that allows authorized users to manage role-based and group-based security at the data element/field level. The evoBrix Security Framework is implemented

through the conceptual network of user accounts, domains, profiles, roles, pages, and page controls. Each user within the evoBrix PMIS solution is associated with a unique user account. User domains map to departments within an organization. Users are required to select a domain when they are registering to access the system. Profiles control user access to the evoBrix PMIS screens and associated functionality. Each profile may be associated with one or more roles. A role is granted access to specific pages and page controls within those pages.

Access is defined at four levels:

- No Access: A role does not have any access to a given page and therefore cannot access it.
- View Only Access: A role is granted view only access to a page.
- Full Access: A role is granted full access to a page, including the ability to modify data elements or invoke actions.
- Controlled Access: A role has limited access to a page and can only view or update specific elements within the page. Security is defined at the level of page (data) elements or controls. Privileges for each page element are defined as No Access, View Only, and Full Access.

SEC30

The Contractor must limit access to its off-site facilities; including storage facilities. The Department has the right to perform physical security audits of the Contractor's off-site and on-site facilities at the Department's discretion.

Team CNSI's private cloud is hosted in Oracle's FedRAMP Government Cloud. Access to Team CNSI's cloud infrastructure is tightly controlled and it is strictly limited to Oracle support personnel only. All storage holding PHI information is tightly controlled, monitored, and tracked.

Since these data centers are operated by a third-party, Team CNSI will provide FedRAMP certification and audit information, when requested. This is consistent with the state's Q&A response to this RFP.

SEC31

The Contractor shall establish security and privacy standards and standard operating procedures. These standards include HIPAA, Federal Information Security Management Act (FISMA), Privacy Act, Federal Tax Information (FTI), and other Federal and State laws, regulations, and policies. The Contractor shall also establish business and technical protocols to ensure that the transmission and storage of information remains secure.

Team CNSI's FedRAMP and HIPAA Data Centers perform annual audits to comply and achieve certification with Statements on Standards for Attestation Engagements/Service Organization Control (SSAE/SOC) and HIPAA standards. The following certifications are in place to provide for the confidentiality, integrity, and availability of the information systems:

- SSAE 16 SOC 1 Type II
- SSAE 16 SOC 2 Type II
- HIPAA/HITECH
- Federal Risk and Authorization Management Program (FedRAMP)

Additionally, Team CNSI's evoBrix PMIS solution includes security and privacy controls that are compliant with the most current version of FISMA and NIST standards. Team CNSI's evoBrix PMIS solution adheres to the following security standards:

- Federal Information Security Management Act (FISMA)
- Internal Revenue System (IRS) Publication 1075 (FTI)
- Privacy Act of 1974
- Patient Protection and Affordable Care Act (PPACA) or (ACA)
- NIST Special Publication 800-66 Revision 1
- NIST Special Publications 800-53 and 800-53A
- NIST Special Publication 800-47
- NIST Special Publication 800-88 Revision 1
- NIST Special Publication 800-111

Team CNSI's evoBrix PMIS solution comprises various standard operating procedures that form an integral part of the solution. These standard operating procedures, apart from conforming to various security and privacy standards, also establish business and technical protocols to ensure secure transmission and storage of information. These standard operating procedures are proven, tested, and currently operational in Michigan, Utah, Illinois, and Washington projects that are managed by Team CNSI. They are explained in detail in the sections below.

Role Based Access Control (RBAC)

Team CNSI's application security solution is built on a Role Based Access Control (RBAC) model which is based on the Principle of Least Privilege. This RBAC model is augmented by a configurable Application Security Framework. The RBAC model allows easy, granular control for access to information. The RBAC controls are designed to NIST control standards for authentication and accounting solutions. Users only see the information to which they are authorized to have access; if a user is not authorized to view a set of information, the information is automatically restricted from view.

Application Security Framework

On the application layer, the solution offers a configurable Security Framework that provides a secure environment for information management and protects against unwanted loss or disclosure of data. Team CNSI's Application Security Framework maintains extensive user audit logging for the audit trail in support of HIPAA Security and Privacy to track changes made to any data stored in PMIS. Team CNSI's evoBrix PMIS solution has a comprehensive data model that supports record level history/versioning and audit capability. evoBrix captures every change in the system and maintains the history, providing the information for a specific period. It also captures audit information, such as what changes have been made, who made the changes, and when. Changes, additions, or deletions to data (including operational and security data) and the associated errors or exceptions, if any, are tagged with information that includes the originating source (such as a specific inbound interface from a designated source, a business operations user making a change in the system, etc.), the date/time, and information about the user who initiated the change. Any errors captured as part of the data updates received from an external interface through the ESB are sent as a back feed to the designated source through an outgoing interface. The source system then verifies and performs necessary actions on the data. The corrected data is received in MT PSM in the next interface run.

Operations Management Portal (OMP)

Operations Management Portal (OMP) is a centralized tool used by Team CNSI's Operations Support team to track and process user access requests. The OMP platform is fully integrated based on ITIL standards. All Team CNSI personnel (including administrators) must access the system (servers, databases, and application) using their own named user accounts only. Access to Application Service accounts or the Administrative accounts ("root," "dba") is restricted.

Team CNSI personnel must create tickets in OMP and follow the User Access Request process to request new named user accounts. This is applicable for both creating new named users as well as for modifying or dropping existing named users.

Data De-identification

Team CNSI ensures that data in all development and system test environments for MT PSM only house scrambled, masked, de-identified data to support the solution configuration and development activities. As part of our experience implementing and supporting multiple Medicaid systems for the States of Michigan, Washington, Illinois, and Utah, Team CNSI leverages a custom data de-identification solution, dataSecureD, to safeguard both the PHI and PII information in the data. dataSecureD provides a comprehensive data de-identification solution that ensures compliance with the Data Privacy and Protection mandates, most notably, the HIPAA Privacy Rule. With this solution, sensitive PHI and PII data can be replaced with de-sensitized but realistic values, allowing production data to be safely and meaningfully used for development, testing, and/or shared with external partners for business needs.

Audit

Team CNSI's evoBrix PMIS solution includes a robust and comprehensive auditing solution that is used to record both data changes and data access. This solution includes Oracle database auditing, Oracle Log Analytics Cloud Service, and OCM's audit framework, and it is applicable for all users including administrators. For additional details on the auditing solutions, please refer to the SEC07 requirement.

Oracle Database Auditing

Team CNSI uses Oracle database auditing to generate audit records for all users who are accessing the database. The audit records are stored in a syslog audit trail. Since the DBA cannot modify a syslog audit trail, audit records stored using this method are more secure than audit records stored using an operating system audit trail.

Oracle Log Analytics Cloud Service

Team CNSI uses Oracle Log Analytics cloud service to consolidates audit data from databases (syslog audit trail), operating systems, applications, firewalls, and directories into a central reporting repository for compliance reporting and alerting. This service allows for full reporting on additions, modifications, deletions, and access to data within the system.

Oracle Connection Manager (OCM)

Access to the Oracle databases by Team CNSI personnel is monitored and audited using OCM. All client and application access to the databases must flow through the OCM, and the audit trail is recorded within the audit framework of OCM.

Encryption

Team CNSI's evoBrix PMIS Solution also ensures that transmission and storage of information remains secure. Figure 3.10.1-35 provides an overview of all the encryption solutions that are used in Team CNSI's evoBrix PMIS to ensure storage and transmission of data is secure.

Tier	Component	Encryption Method	Encryption Algorithm
Database Tier	Data files	Oracle Transparent Database Encryption	AES-256
Database Tier	Encryption Keys	Oracle Key Vault	PKCS#12 file
Database Tier	Backups	Oracle RMAN Encryption	AES-256
Storage Tier	Oracle Data Pump Exports	Oracle Data Pump Encryption	AES-256
Storage Tier	Flat Files (at rest)	Linux eCryptfs	AES-256
Storage Tier	Flat Files (in transit)	Titan SFTP	SHA-1
Network Tier	Data Traffic	Oracle Network Encryption	AES-256
Network Tier	Data Integrity	Oracle Data Integrity	SHA-1
Application Tier	Network Traffic	SSL Encryption	256 bit SSL
Physical Transmission	Disks/Disk Partition	IDRIX VeraCrypt	AES-256

Figure 3.10.1-35. Storage and Transmission Encryption Solutions. An overview of Storage and Transmission Encryption solutions that are used in Team CNSI's evoBrix PMIS.

SEC38

The Contractor's solution shall employ malicious code protection mechanisms at IT systems entry and exit points, at workstations, servers, and mobile computing devices on the network to detect and eradicate malicious code.

Team CNSI has established a comprehensive information security policy. Team CNSI employs different mechanisms at various tiers to detect and eradicate malicious code. At the application tier, Team CNSI leverages IBM Security AppScan product for scanning security vulnerabilities in the application code. At the data center hosting layer, Team CNSI's hosting platform employs IDS, IPS, Anti-virus software and network firewalls to monitor and protect and IT systems entry and exit points. All Team CNSI supplied equipment including Client Desktops/Laptops, Mobile devices are also scanned using different protection mechanisms. Detailed information on all these mechanisms and products is discussed below.

IBM Security AppScan

Team CNSI's evoBrix PMIS solution leverages IBM Security AppScan tool to scan application code before deploying them to web and mobile applications. This greatly enhances web application security and mobile application security thereby improving application security program management and strengthening regulatory compliance. By scanning our web and mobile applications prior to deployment, AppScan enables us to identify security vulnerabilities and generate reports and fix recommendations. This tool minimizes web application attacks and expensive data breaches by automating testing of application security vulnerabilities.

Hosting Platform

Team CNSI's hosting platform, Oracle Government Cloud, includes the following solutions to secure the access/entry points.

- Intrusion Detection System (IDS)

IDS monitors the network and systems for malicious activity and security violations. Any detected activity or violation is collected centrally using Oracle Cloud's Log Analytics Service, which is a SIEM system, and reports are generated from this service.

- Intrusion Prevention System (IPS)

Intrusions that are detected by IDS are reported to the IPS. The IPS attempts to block or stop the intrusion as well as reporting the incidents. This includes both Network-based intrusions and Host-based intrusions

- Anti-virus software

An important component within the Hosting Platform Security is the anti-virus software. This feature provides comprehensive antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, URL blocking/filtering, and content filtering services. It includes protection from known and advanced threats, including protection against targeted and persistent malware attacks

- Network Segmentation and Network Firewall

Team CNSI's multi-layered security architecture ensures security and protection by placing the most sensitive portions of the system behind multiple security layers with a tiered architecture. This tiered approach includes network segmentation and firewalls, and it creates the most secure environment, putting up multiple defenses that secure information from attackers. Additional information about Team CNSI's multi-layered security approach is explained in SEC04 requirement.

Team CNSI-supplied equipment

All Team CNSI-supplied equipment is configured for encrypted disk and password-protected access at the hardware layer. This includes all workstations, laptops, and mobile devices. Team CNSI uses the following protection mechanisms for detecting and eradicating malicious code at all IT systems entry and exit points:

- Workstations/Laptops
    - Custom, hardened OS image deployed to all Team CNSI laptops and desktops.
    - Whole disk encryption applied to all Team CNSI laptops.
    - Active Directory authentication and Group Policy enforcement of security configuration standards.
    - Cisco Advanced Malware Protection (AMP) for Endpoints: Commercial virus/malware protection installed on all clients and centrally managed by the CNSI Help Desk.
    - Windows Server Update Services: Centrally managed OS and application patch management.
    - OpenDNS with Umbrella roaming client: DNS protection along with anti-phishing and malware protection capabilities
    - Tennable Nessus Scanner: Scans and reports vulnerabilities and provides patching solutions. It also provides asset grouping and tagging features.
- Mobile Devices:
    - Custom security configuration profiles installed on all Team CNSI mobile devices.
    - Whole device encryption, strong password, and device locking policies centrally managed.
    - Remote-wipe capability enabled and centrally managed on all Team CNSI mobile devices.

SEC39

The Contractor's solution shall use foundational technical standards such as X.509 Certificate format and Public Key Cryptography Standard (PKCS).

The Team CNSI's evoBrix PMIS uses current state of the art encryption and certificate systems to protect all data both at rest and in flight on networks. All connections to the DPHHS PSM system use SSL technology for fully encrypted connection. SSL connections use TLS 1.2, SHA 2 with a minimum of a 2048-bit key. Our solution uses X.509 certificates signed by Verisign, a third-party Certificate authority. These certificates conform to the widely accepted X.509 pubic key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

Team CNSI uses Oracle TDE to encrypt both data at rest and database backups. The encryption keys are stored in an Oracle Wallet, a PKCS#12 standards-based key storage file. These encryption keys are stored in Public Key Cryptography Standard (PKCS#12) format.

Team CNSI uses Oracle Key Vault to ensure protection of encryption keys. Oracle Key Vault is used to centrally authorize, secure, and manage all encryption keys. Oracle Key Vault is a FIPS 140-2 Level 3 compliant key management system, offering a strong and scalable solution.

SEC41

The Contractor shall collaborate with the Systems Integration Services Contractor to integrate the Contractor's solution into the State's integration platform for single sign-on and federated identity management.

Team CNSI's evoBrix PMIS solution will integrate with the State's existing SSO and federated identity management platform to provide a seamless IAM experience for internal and external users across the MPATH system. This solution will provide the ability to identify users in different contexts (such as time, day of week, location of access, or type of access method), allowing State policies and user preferences to be applied consistently across the system. Our solution will employ Oracle Access Manager to provide integration with the DPHHS system integration platform. It will consume identities provided by the DPHHS identity provider. The identity federation will use SAML 2.0. Detailed information about this integration is explained in SEC01 requirement.

SEC42

The Contractor shall have an overall data security process that supports data security auditing.

Because of our experience and the maturity of our security practice, Team CNSI is accustomed to playing a key role in helping State and Federal agencies build a robust and comprehensive data security process that supports data security auditing. We have contributed significantly to agency and system security plans in the states of Michigan, Washington, Illinois and Utah, as well as CMS, the U.S. Census Bureau, and the DOD. This data security audit includes auditing multiple systems and processes within Team CNSI's evoBrix PMIS and these systems and processes are described below.

Encryption

Team CNSI employs a multi-layer encryption solution covering network, system, and database tiers. This ensures that all classified and potentially sensitive data is encrypted at rest and in transit. We have extensive experience with these encryption technologies, through our implementations in our Michigan, Illinois, Utah, and Washington MMIS solutions. Figure 3.10.1-36 provides an overview of all the encryption solutions that are used in Team CNSI's evoBrix PMIS.

Tier	Component	Encryption Method	Encryption Algorithm
Database Tier	Data files	Oracle Transparent Database Encryption	AES-256
Database Tier	Encryption Keys	Oracle Key Vault	PKCS#12 file
Database Tier	Backups	Oracle RMAN Encryption	AES-256
Storage Tier	Oracle Data Pump Exports	Oracle Data Pump Encryption	AES-256
Storage Tier	Flat Files (at rest)	Linux eCryptfs	AES-256
Storage Tier	Flat Files (in transit)	Titan SFTP	SHA-1
Network Tier	Data Traffic	Oracle Network Encryption	AES-256
Network Tier	Data Integrity	Oracle Data Integrity	SHA-1
Application Tier	Network Traffic	SSL Encryption	256 bit SSL
Physical Transmission	Disks/Disk Partition	IDRIX VeraCrypt	AES-256

Figure 3.10.1-36. Data Encryption Solutions. An overview of Data Encryption solutions that are used in Team CNSI's evoBrix PMIS.

Database Tier

At the database layer, Team CNSI leverages advanced Oracle security tools, which ensures strong encryption of databases containing sensitive information such as PII and PHI.

- Oracle TDE: Team CNSI uses TDE to encrypt sensitive data at rest. Data is encrypted at the tablespace level using the AES-256 algorithm. The encryption keys are stored in a wallet and the wallet is also secured, stored, and backed up using Oracle Key Vault.
- Oracle Key Vault: Team CNSI uses Oracle Key Vault to ensure protection of encryption keys. Oracle Key Vault is used to centrally authorize, secure, and manage all encryption keys. Oracle Key Vault is a FIPS 140-2 Level 3 compliant key management system, offering a strong and scalable solution.
- Oracle Backup Encryption: Team CNSI uses Oracle RMAN and Local TDE master encryption key to encrypt all database backups including full backups, incremental backups, and archive log backups. This ensures that backups, which are usually stored in offsite locations, are secured.

Storage Tier

- Oracle Data Pump Encryption: Team CNSI uses Oracle Data Pump for taking exports of database schemas and tables. The dump files that are generated by Oracle Data Pump are encrypted using Oracle Data Pump Encryption and the encryption algorithm is AES-256.
- Flat File Encryption at Rest: Team CNSI uses eCryptfs utility within Oracle Linux to encrypt a file system. This utility is used to encrypt individual files and directories using AES-256 algorithm.
- Flat File Transfer Encryption: Team CNSI uses Titan Secure FTP to ensure encryption of files in transit.

Network Tier

- Oracle Database Network Encryption: Team CNSI uses AES-256 based network encryption to encrypt data in transit, thus ensuring that data is secure as it travels across the network

- Oracle Data Integrity: Team CNSI uses Secure Hash Algorithm 1 (SHA-1) based Data Integrity protection to safeguard data against data modification attacks and replay attacks
    - Data modification attack: An unauthorized party intercepting data in transit, altering it, and retransmitting it is a data modification attack
    - Replay Attack: Repetitively retransmitting an entire set of valid data

Application Tier

At the application layer, all user sessions to and from the application are encrypted with 256bit SSL. This approach provides end-to-end network security, reducing the system's exposure to potentially malicious internet traffic and mitigating the possibility of internet-based attempt to defeat critical safeguards that could expose sensitive personal, health, or financial information.

Physical Transmission

Team CNSI's evoBrix PMIS solution does not normally require physical transmission of data using disks or disk partitions. However, when a need arises, Team CNSI uses IDRIX VeraCrypt, which is an open source disk encryption utility. This utility is used to perform on-the-fly encryption of disks and disk volumes using AES-256 algorithms.

Audit Systems and Behavioral Audit

Team CNSI's evoBrix PMIS solution is monitored and audited by multiple solutions and PaaS services within the security suite of the Oracle Cloud. These solutions help to audit all user accesses and identify usage anomalies and system misuse. These solutions enable rapid detection, investigation, and remediation of the broadest range of security threats across Team CNSI's cloud IT assets. Detailed information about these cloud services and tools is provided in SEC06. The audit suite includes the following security solutions:

- Oracle Database Auditing
- Oracle SMA Cloud Service – Behavioral Audit
- Oracle Log Analytics Cloud Service
- Oracle Connection Manager (OCM)
- Application Audit Framework

Application Security Audit

Team CNSI's application security solution is built on an RBAC model, which is based on the Principle of Least Privilege and is augmented by a configurable Application Security Framework.

Role Based Access Control (RBAC)

The RBAC model allows easy, granular control for access to information. The RBAC controls are designed to NIST control standards for authentication and accounting solutions. Users only see the information to which they are authorized to have access; if a user is not authorized to view a set of information, the information is automatically restricted from view. User access to information is easily controlled by the assignment or removal of specific roles to the person. The RBAC model reduces the cost of identity security management and lowers the risk of accidental release of sensitive data. The RBAC model is proven, tested, and currently operational in Michigan, Utah, Illinois, and Washington projects that are managed by Team CNSI.

Application Security Framework

Team CNSI's Application Security Framework maintains extensive user audit logging for the audit trail in support of HIPAA Security and Privacy to track changes made to any data stored in PMIS. Authorized users can access audit trail information using the web portal to keep track of who initiated the change, what changed, when the change was requested, who approved/denied the change, and when was it was approved/denied. The solution provides the ability to reverse or back out changes made in error while still retaining the associated audit trail.

Network Vulnerabilities and Controls

Team CNSI's approach to auditing network vulnerabilities addresses the areas of Interception, Availability, and Access/entry points. Team CNSI implements multiple tools and solutions to audit this area. Figure 3.10.1-37 provides an overview of all the network vulnerabilities areas and the audit security solutions that are implemented in Team CNSI's evoBrix PMIS.

Network Vulnerability Area	Scope	Audit Security Solutions
Interception	Data that is being transmitted over the network is vulnerable to being intercepted by an unintended third party who could put the data to harmful use.	■ Oracle network encryption using AES-256 algorithm to encrypt data in transit between databases and application tier ■ All user sessions to and from the application are encrypted with 256bit SSL ■ Oracle Data Integrity using SHA-1 to protect data integrity
Availability	Lost connectivity in networks could cause business interruption.	■ Team CNSI's hosting platform in Oracle Government Cloud has redundant paths between different tiers and an access point ■ Automatic routing to switch the traffic to the available path without loss of data or time
Access/entry points	Networks are vulnerable to unwanted access. A weak point in the network can make that information available to intruders. It can also provide an entry point for viruses and Trojan horses.	■ Team CNSI's hosting platform includes the following solutions to secure the access/entry points: • Intrusion Detection System (IDS) • Intrusion Prevention System (IPS) • Anti-virus software • Network segmentation and network firewall • Auditing systems (Oracle SMA Service, Oracle Log Analytics • Service and OCM) ■ All Team CNSI-supplied equipment is configured for encrypted disk and password-protected access at the hardware layer. This includes all workstations, laptops, and mobile devices.

Figure 3.10.1-37. Audit Security Solutions for Network Vulnerabilities. An overview of Audit Security solutions that are used in Team CNSI's evoBrix PMIS to address network vulnerabilities.

SEC44

The Contractor must be compliant with the security processes outlined in the "Security and Privacy Controls Requirements" document that has been included in the Procurement Library.

Team CNSI has developed expert knowledge of all applicable industry and Federal standards, models, and practices related to security of state Medicaid systems, and the most recent standards outlined by FedRAMP, HIPAA, HITECH, FISMA, and NIST standards. We reviewed State of Montana's security and privacy control requirements and our proposed evoBrix PMIS does comply with these security processes.

Team CNSI's evoBrix PMIS undergoes risk assessment covering NIST SP 800-53 Rev 4 standards using New Net Technologies (NNT) Change Tracker product. Change Tracker's built-in NIST 800-53 report assesses the configured state of our system for compliance with the key NIST Security Controls. The result is a simple percentage score with clear remediation guidance, wherever non-compliance is highlighted. Thereafter Change Tracker provides real-time monitoring of core configuration settings covering installed software, running processes, services and startup states, registry keys, user accounts, audit and security policy, open network ports and the overall integrity of the filesystem. The outcome of this security risk assessment is a Security Audit Report. This report will be submitted to DPHHS by September 30th each year. The evaluation of the security systems uses the SSP as guidance for the audit.

SEC45

The Contractor shall monitor system activity and prevent and detect intrusion, hacking, unusual activity, or system compromise. The Contractor shall immediately report any incidents of such, regardless of the outcome to the state, activate a Department approved communication strategy, perform mitigation activities, and provide continuous status updates to the Department until the issues are resolved to the Department's satisfaction. Only authorized contractor personnel may override system security alerts and edits.

Team CNSI's evoBrix PMIS solution has a robust and extensive monitoring system in place to protect the integrity of the system. Team CNSI's Monitoring system is built with multiple PaaS services and tools that helps to identify usage anomalies and system misuse as well as detect intrusion and hacking. Team CNSI's Monitoring System is backed up by a comprehensive Incident Management Plan which includes the processes and procedures to report both successful and unsuccessful incidents, plan strategies and perform mitigation activities along with regular status updates to DPHHS. Upon resolution of the incident, a full root cause analysis (RCA) is performed and the RCA report is submitted to DPHHS. Team CNSI's policy is that only authorized personnel may override system security alerts and edits.

Monitoring System

The Monitoring System comprises of Oracle SMA Cloud Service, Oracle Log Analytics Cloud Service, OCM, IDS, and IPS. Detailed information about these solutions are explained in SEC06 requirement.

Oracle Security Monitoring and Analytics (SMA) Cloud Service

Oracle SMA Cloud Service enables rapid detection, investigation and remediation of the broadest range of security threats across on-premises and cloud IT assets. Security Monitoring and Analytics provides integrated SIEM and UEBA capabilities built on machine learning, user session awareness, and up-to-date threat intelligence context.

Oracle Log Analytics Cloud Service

Team CNSI's monitoring system uses Oracle Log Analytics cloud service to monitor, aggregate, index, and analyze all log data from multiple sources. This cloud service includes features that helps to detect usage anomalies and system misuse.

- Consolidates audit data from databases, operating systems, applications, firewalls, and directories
- Audit data is then stored into a central reporting repository for compliance reporting and alerting
- Enables users to search, explore, and correlate this data to troubleshoot problems faster and derive operational insight

- Smart clustering of log events based on common signatures helps identify patterns and outliers quickly and thus is used to identify and track usage anomalies

Oracle Connection Manager (OCM)

Team CNSI personnel accesses databases using named users and this type of access is monitored and audited using OCM. All client and application access to the databases must flow through the OCM. Data download limits are enforced via OCM to prevent mass download of information from the system. This prevents intruders from doing a wholesale data dump limiting exposure if there is an account that has been compromised. Any requests out of the proper norms automatically trigger alerts to operations staff. Access to data for download is bound by RBAC rules to prevent access to information the person is not authorized to access. All data access is logged, and unusual activity generates alerts.

Intrusion Detection System (IDS)

Team CNSI's monitoring system uses Oracle Government Cloud's IDS to monitor the network and systems for malicious activity and security violations. Any detected activity or violation is collected centrally using Oracle Cloud's Log Analytics Service, which is a SIEM system, and reports are generated from this service.

Intrusion Prevention System (IPS)

Team CNSI's monitoring system uses Oracle Government Cloud's IPS to block or stop the intrusions that were reported by the IDS. The IPS attempts to block or stop the intrusion, as well reporting the incidents. This includes both Network-based intrusions and Host-based intrusions

Incident Management

Team CNSI operational teams use OTRS to log Incident Management items so they can be tracked and triaged to resolution and finally closure. All intrusion and hacking incidents, no matter whether they are successful or unsuccessful, are reported to our 24x7 NOC Help Desk and operations team through the tools and cloud services that were described in the Monitoring System section. When an incident occurs:

- Team CNSI Help Desk is notified of the incident through the tools and cloud services that were described in the Monitoring System section.
- Team CNSI's operations management is notified and will notify the State of the incident and status based on information known, regardless of outcome.
- Team CNSI will activate a DPHHS approved communication strategy as needed.
- The Help Desk opens an incident ticket using OTRS.
    - The ticket describes the event and the module or operational area affected by the issue
    - The Help Desk assigns the Priority Level (i.e., Urgent, High, Normal, or Low) and enters pertinent information
    - Help Desk notifies the appropriate response team
    - Help Desk notifies account management of the issue and the assigned response team
- Team CNSI assembles the appropriate personnel to conduct an analysis of the issue and define an action plan to resolve the issue depending upon the severity level of the issue.
- Once the appropriate course of action is determined, Team CNSI opens a Jira ticket for internal tracking purposes.
- Team CNSI assigns the appropriate personnel to conduct its own detailed internal review and obtain the appropriate approvals to commence the resolution. In this meeting, a discussion of the issue,

solution, and a review of the scripts, if any, is conducted. Scripts should meet the same standards set by Team CNSI internally to ensure continuity and reduce the chance of negative effects to the system.
- Team CNSI submits the mitigation plan to CCB for emergency approval. Once approved, the mitigation plan and activities are implemented.
- Team CNSI Operations Management provides continuous status updates to DPHHS throughout the incident until the resolution is completed.

After the incident is resolved, Team CNSI creates an Incident Report, an example of which is shown in Figure 3.10.1-38. An Incident Report compiles the following information:

- What triggered the incident
- What services are affected by the incident
- A complete timeline of events
- All actions taken to resolve the issue
- Lessons that were learned and ideas for prevention in the future
- List of each person involved at any time throughout the incident
- Summary of each communication
- Attachments, including actual emails and records of phone calls and meetings, with a summary of what was discussed

The completed Incident Report is then distributed to Team CNSI's management. After review, Team CNSI management distributes the Incident Report to the appropriate DPHHS personnel. If more than one problem occurs in the same area, Team CNSI conducts a root-cause analysis to develop a thorough understanding of the issue and its causes. The Incident Reports for those problems are used as part of the tracking and understanding of the problems. A plan is derived from the analysis for either corrective or preventative actions that reduces the risk of another occurrence to an acceptable level. The corrective or preventative actions is documented, implemented, and shared with DPHHS. Follow up reviews of the actions are conducted to make sure they are properly alleviating the issue and determine whether there is a more efficient way of correcting or preventing the problem.

CNSI

Production Incident Report

Incident Headline:	
Incident Date/Time:	
Report Author:	
Team(s)/Individual(s) Involved:	
Date Report Prepared:	
Ticket Number(s):	

Incident Details

Description:

Detailed description of the incident.

Scope and Impact of the Incident:

Who or what was impacted by the incident. List both short term and long term Impacts.

Incident Resolution Timeline

Communications:

List all communications relating to the incident (emails, phone calls etc.). Include individuals involved & timelines.

Solution: Steps Taken to Resolution and Next Steps:

Detailed descriptions of steps taken to resolve the incident including timelines.

Root Cause:

Detailed description on what caused the incident to occur.

Incident Prevention Plan

Lessons Learned and Recommendations:

Describe lessons learned as a result the incident and provide detailed recommendations on how to prevent this incident from reoccurring in the future.

Action Plan:

Describe the Action Plan to implement the Recommendations including Owners and expected completion dates for the Actions.

Step	Task	Owner	Planned Date
1	Example: Install new certificate when there is a change or time to renew the LN SSL certificate.	PCS and MI Deployment team	NA

Incident Report Template.docx CNSI Page | 1

MTPSM-3-159

Figure 3.10.1-38. Sample Production Incident Report. Team CNSI focuses on root cause analysis to address incidences during production.

SEC46

The Contractor shall provide and operate solutions that terminate access immediately and/or generate alerts for conditions that violate security rules, unauthorized attempts to access data and system functions, and system activity based on security parameters.

Team CNSI's evoBrix PMIS solution is monitored and protected by different PaaS services within the security suite of the Oracle Cloud. These PaaS services help to identify usage anomalies and system misuse. The solution suite includes Oracle SMA Cloud Service, Oracle Log Analytics Cloud Service and OCM. These tools enable rapid detection, investigation, and remediation of the broadest range of security threats across Team CNSI's cloud IT assets.

If a breach or system misuse is detected, these security tools record and attempt to shut down the breach. Alerts are generated to the operations staff, who contact all appropriate Team CNSI staff. Upon resolution of the situation, a full root cause analysis is performed, the system remediated to prevent any future issues, and reports generated and sent to all appropriate stakeholders. Detailed information about these services and tools is explained in SEC06 requirement.

Additionally, Team CNSI has established a comprehensive information security policy. Team CNSI employs different mechanisms at various tiers to detect and eradicate malicious code. At the application tier, Team CNSI leverages IBM Security AppScan product for scanning security vulnerabilities in the application code. At the data center hosting layer, Team CNSI's hosting platform employs IDS, IPS, anti-virus software, and network firewalls to monitor and protect and IT systems entry and exit points. All Team CNSI supplied equipment including Workstations/Laptops and mobile devices are also scanned using different protection mechanisms. Detailed information on all these mechanisms and products is discussed in the SEC38 requirement.

SEC47

The Contractor's solution shall ensure that only authorized users have access to systems and data, by requiring the following:

- Unique authentication credentials identifiable to each user of the system, not allowing for the re-use of credentials;
- Authenticates the receiving entity prior to a system initiated session, such as transmitting responses to case inquiries;
- Maintenance of key user information as part of a user profile including user ID, name, employer/state agency,
- Identity verification information, and an indicator of employee versus contractor;
- Multi-factor user authentication and the ability to restrict or permit a user's access to system functions, features, and processes based on the user's assigned roles based on business need and user security profile and a unique user ID and password and including a read-only access level;
- Column and row-level security access, data classification schemes, and/or the designation of data at multiple levels (e.g., case, individual) as restricted or sensitive (e.g., substance abuse treatment data) with the ability to define and implement exclusion controls on a per-user or user-group basis within a multi-level organizational structure, (e.g., external agencies and Appeals units).
- A method for authentication of all internal and external users and systems and the ability to deny access to all invalid users and systems;

- Encrypted passwords in storage and in transmission;
- The capability to automatically suspend users who have not accessed the systems within a time period specified by the Department;
- The termination of authorized sessions after a time period of no activity specified by the Department, with a warning message displayed prior to the session timeout;
- Enforce a sufficient level of authentication and identification against fraudulent transmission, imitative communications, and deceptive communications by validating the transmission, message, station or individual; and
- A method for designated security administrators to set and modify user security access profile

evoBrix PMIS will integrate with the MT PSM identity management system to make use of the single sign-on and authorization systems for users. Each user will be individually authenticated prior to accessing the system. Figure 3.10.1-39 provides a complete list of access standards and the equivalent compliance features that are built into the evoBrix PMIS solution.

Access Standards	Compliance Features	Proposal Section
Unique authentication credentials identifiable to each user of the system, not allowing for the re-use of credentials.	■ The evoBrix web portal leveraging the DPHHS IAM security framework for integration allows the solution to offer a secure SSO experience. ■ All Team CNSI personnel have named user access to the system and no shared accounts are created.	■ SEC01 ■ SEC48
Authenticates the receiving entity prior to a system initiated session, such as transmitting responses to case inquiries.	■ Team CNSI's evoBrix PMIS solution will integrate with the DPHHS's HUB system for system initiated access. ■ A handshake is established first with the exchange of certificates between the PMIS and other state agencies. ■ This establishes a 256bit SSL encrypted tunnel.	■ SEC01
Maintenance of key user information as part of a user profile including user ID, name, and employer/state agency.	■ Team CNSI's Operations Support team uses Operations Management Portal (OMP) to track and process user access requests. ■ As a part of this user access process, key user information is captured and recorded.	■ SEC48
Identity verification information, and an indicator of employee versus contractor.	■ Team CNSI's OMP product tracks and records this information.	■ SEC48
Multi-factor user authentication and the ability to restrict or permit a user's access to system functions, features, and processes based on the user's assigned roles based on business need and user security profile and a unique user ID and password and including a read-only access level.	■ Team CNSI's application security model is built on RBAC policies, which allows easy, granular control for access to information. The RBAC controls are designed to NIST control standards for authentication and accounting solutions.	■ SEC12 ■ SEC01
Column and row-level security access, data classification schemes, and/or the designation of data at multiple levels (e.g., case, individual) as restricted or sensitive (e.g., substance abuse treatment data) with the ability to define and implement exclusion controls on a per-user or user-group basis within a multi-level organizational structure, (e.g., external agencies and Appeals units).	■ Team CNSI employs a defense-in-depth approach to securing our solution by implementing multiple layers of network, system, and database encryption technologies to ensure all classified and potentially sensitive data is encrypted at rest and in transit.	■ SEC02
A method for authentication of all internal and external users and systems and the ability to deny access to all invalid users and systems.	■ Team CNSI's system includes authentication mechanisms for user-initiated access, system initiated access and backend system access.	■ SEC02

Access Standards	Compliance Features	Proposal Section
Encrypted passwords in storage and in transmission.	■ Team CNSI employs a defense-in-depth approach to securing our solution by implementing multiple layers of network, system, and database encryption technologies to ensure all classified and potentially sensitive data is encrypted at rest and in transit.	■ SEC02
The capability to automatically suspend users who have not accessed the systems within a time period specified by the Department.	■ Team CNSI's password policy is based on a CIS v2.1.0 password guidelines. Users get automatically suspended if they don't change their password every 60 days. ■ Additionally, all user account access is reviewed on a quarterly basis by Operations Support team and inactive users are dropped.	■ SEC66
The termination of authorized sessions after a time period of no activity specified by the Department, with a warning message displayed prior to the session timeout.	■ Team CNSI's user access policy is based on a CIS v2.1.0 benchmarks. All authorized sessions are timed out after 30 minutes of inactivity.	■ SEC66
Enforce a sufficient level of authentication and identification against fraudulent transmission, imitative communications, and deceptive communications by validating the transmission, message, station or individual; and a method for designated security administrators to set and modify user security access profile.	■ Team CNSI's solution is monitored and protected by different PaaS services to identify usage anomalies and system misuse. The solution suite includes Oracle Security Monitoring and Analytics (SMA) Cloud Service, Oracle Log Analytics Cloud Service and Oracle Connection Manager (OCM). These tools enable rapid detection, investigation, and remediation of the broadest range of security threats across Team CNSI's cloud IT assets.	■ SEC06

Figure 3.10.1-39. Compliance to Access Standards. List of access standards and the equivalent compliance features that are built into the evoBrix PMIS solution.

SEC48

The Contractor shall provide to the Department, upon request, a listing of all users having access to the Contractor's module components and/or data with details regarding the access granted to each user.

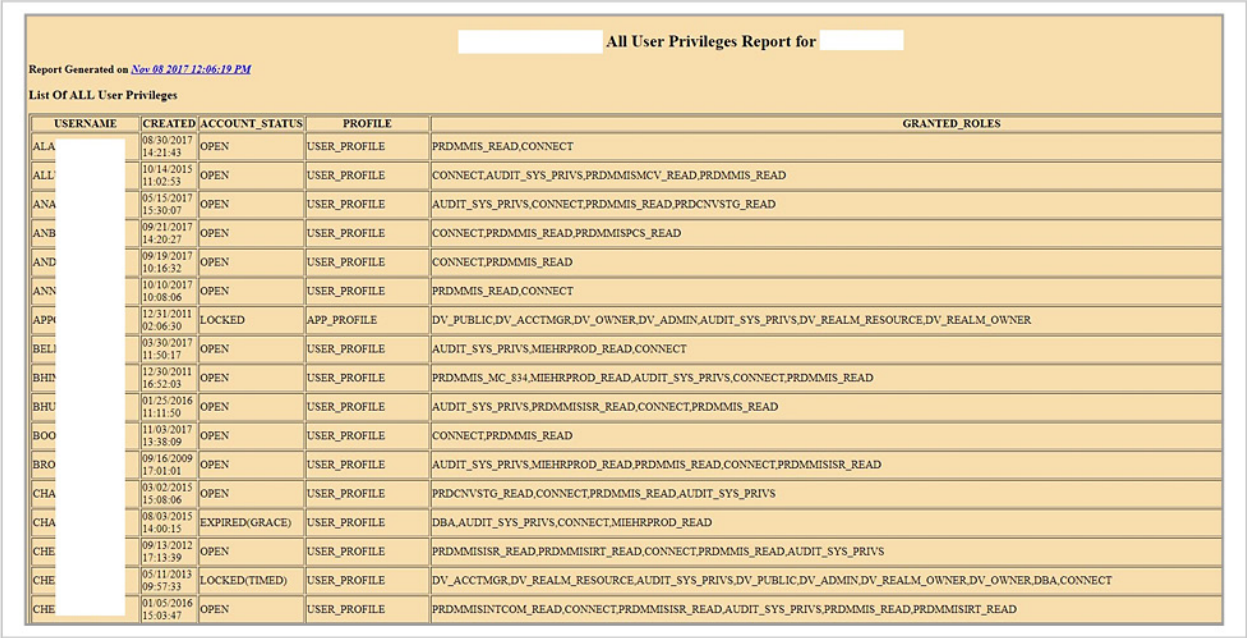
Operations Management Portal (OMP) is a centralized tool used by Team CNSI's Operations Support team to track and process user access requests. The OMP platform is fully integrated based on ITIL standards. All Team CNSI personnel (including administrators) must access the system (servers, databases, and application) using their own named user accounts only. Access to Application Service accounts or the Administrative accounts ("root," "dba") is restricted.

Team CNSI personnel must create tickets in OMP and follow the User Access Request process to request for new named user accounts. This is applicable for both creating new named users as well as for modifying or dropping existing named users. The User Access Request process for creating a new named user is as follows:

1. Team CNSI personnel logs into OMP and creates a ticket for Named User Access.
2. This OMP ticket contains details about the user such as User's First Name, User's Last Name, User's Email ID, User's Phone Number, User's Manager Name and Contact Details along with the level of access (READ, WRITE) required for each database or application schema.
3. The OMP ticket goes through the approval process workflow. The user's manager reviews the ticket and approves it. This is the first level of approval.
4. The ticket is then approved by the Project Manager, which is the second level of approval.
5. Finally, the ticket is approved by the Operations Manager, which is the third level of approval.

6. All the three levels of approval are based on the Principle of Least Privilege (i.e., only the least privilege that is required to perform the duties) is assigned to the named user. If unnecessary privileges are requested in the ticket, then the ticket is denied and the user must create a new ticket/request with minimal privileges and then start from Step 1.
7. Once the ticket is approved, it is then submitted to the respective Admin team.
8. The Admin team then creates the named user. Based on the level of access requested in the ticket, the Admin team will assign appropriate Roles and Profiles to the named user.

A sample "User Access Report" is shown in Figure 3.10.1-40. This report provides a list of all users along with current account status, the date in which the account was created, and the profile and roles that were assigned to each named user.



All User Privileges Report for

Report Generated on Nov 08 2017 12:06:19 PM

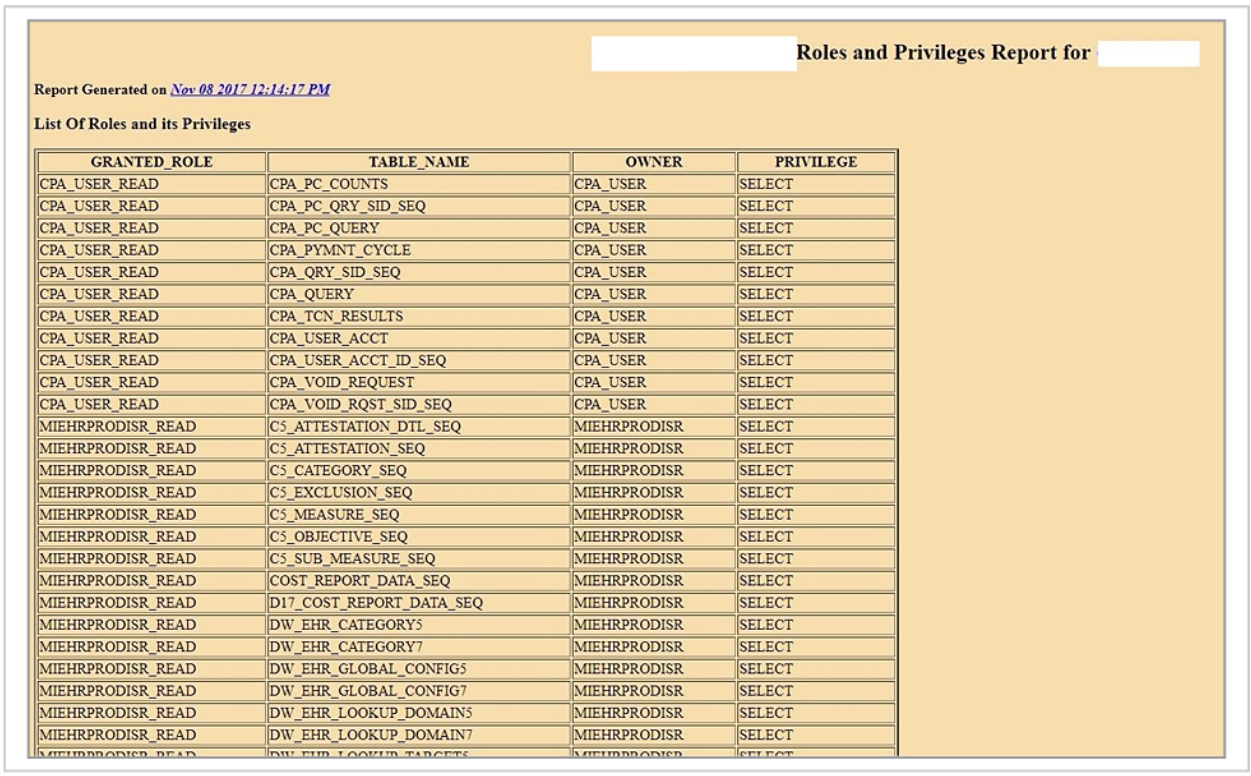
List Of ALL User Privileges

USERNAME	CREATED	ACCOUNT_STATUS	PROFILE	GRANTED_ROLES
ALA	08/30/2017 14:21:43	OPEN	USER_PROFILE	PRDMMIS_READ,CONNECT
ALL	10/14/2015 11:02:53	OPEN	USER_PROFILE	CONNECT,AUDIT_SYS_PRIVS,PRDMMISMCV_READ,PRDMMIS_READ
ANA	05/15/2017 15:30:07	OPEN	USER_PROFILE	AUDIT_SYS_PRIVS,CONNECT,PRDMMIS_READ,PRDCNVSTG_READ
ANB	09/21/2017 14:20:27	OPEN	USER_PROFILE	CONNECT,PRDMMIS_READ,PRDMMISPCS_READ
AND	09/19/2017 10:16:32	OPEN	USER_PROFILE	CONNECT,PRDMMIS_READ
ANN	10/10/2017 10:08:06	OPEN	USER_PROFILE	PRDMMIS_READ,CONNECT
APP	12/31/2011 02:06:30	LOCKED	APP_PROFILE	DV_PUBLIC,DV_ACCTMGR,DV_OWNER,DV_ADMIN,AUDIT_SYS_PRIVS,DV_REALM_RESOURCE,DV_REALM_OWNER
BEL	03/30/2017 11:50:17	OPEN	USER_PROFILE	AUDIT_SYS_PRIVS,MIEHRPROD_READ,CONNECT
BHI	12/30/2011 16:52:03	OPEN	USER_PROFILE	PRDMMIS_MC_834,MIEHRPROD_READ,AUDIT_SYS_PRIVS,CONNECT,PRDMMIS_READ
BHU	01/25/2016 11:11:50	OPEN	USER_PROFILE	AUDIT_SYS_PRIVS,PRDMMISISR_READ,CONNECT,PRDMMIS_READ
BOO	11/03/2017 13:38:09	OPEN	USER_PROFILE	CONNECT,PRDMMIS_READ
BRO	09/16/2009 17:01:01	OPEN	USER_PROFILE	AUDIT_SYS_PRIVS,MIEHRPROD_READ,PRDMMIS_READ,CONNECT,PRDMMISISR_READ
CHA	03/02/2015 15:08:06	OPEN	USER_PROFILE	PRDCNVSTG_READ,CONNECT,PRDMMIS_READ,AUDIT_SYS_PRIVS
CHA	08/03/2015 14:00:15	EXPIRED(GRACE)	USER_PROFILE	DBA,AUDIT_SYS_PRIVS,CONNECT,MIEHRPROD_READ
CHE	09/13/2012 17:13:39	OPEN	USER_PROFILE	PRDMMISISR_READ,PRDMMISIRT_READ,CONNECT,PRDMMIS_READ,AUDIT_SYS_PRIVS
CHE	05/11/2013 09:57:33	LOCKED(TIMED)	USER_PROFILE	DV_ACCTMGR,DV_REALM_RESOURCE,AUDIT_SYS_PRIVS,DV_PUBLIC,DV_ADMIN,DV_REALM_OWNER,DV_OWNER,DBA,CONNECT
CHE	01/05/2016 15:03:47	OPEN	USER_PROFILE	PRDMMISINTCOM_READ,CONNECT,PRDMMISISR_READ,AUDIT_SYS_PRIVS,PRDMMIS_READ,PRDMMISIRT_READ

MTPSM-3-365

Figure 3.10.1-40. User Access Report. This report contains the list of users who are currently active in the system along with the profiles and roles that are assigned to them, and this forms the basis for User Access review process.

A sample "Roles and Privileges Report" is shown in Figure 3.10.1-41. This report provides a list of all roles created along with the object names on which it has access and the type of privileges (SELECT, INSERT, UPDATE, DELETE) it has on these objects.



Roles and Privileges Report for

Report Generated on Nov 08 2017 12:14:17 PM

List Of Roles and its Privileges

GRANTED_ROLE	TABLE_NAME	OWNER	PRIVILEGE
CPA_USER_READ	CPA_PC_COUNTS	CPA_USER	SELECT
CPA_USER_READ	CPA_PC_QRY_SID_SEQ	CPA_USER	SELECT
CPA_USER_READ	CPA_PC_QUERY	CPA_USER	SELECT
CPA_USER_READ	CPA_PYMNT_CYCLE	CPA_USER	SELECT
CPA_USER_READ	CPA_QRY_SID_SEQ	CPA_USER	SELECT
CPA_USER_READ	CPA_QUERY	CPA_USER	SELECT
CPA_USER_READ	CPA_TCN_RESULTS	CPA_USER	SELECT
CPA_USER_READ	CPA_USER_ACCT	CPA_USER	SELECT
CPA_USER_READ	CPA_USER_ACCT_ID_SEQ	CPA_USER	SELECT
CPA_USER_READ	CPA_VOID_REQUEST	CPA_USER	SELECT
CPA_USER_READ	CPA_VOID_RQST_SID_SEQ	CPA_USER	SELECT
MIEHRPRODISR_READ	C5_ATTESTATION_DTL_SEQ	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	C5_ATTESTATION_SEQ	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	C5_CATEGORY_SEQ	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	C5_EXCLUSION_SEQ	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	C5_MEASURE_SEQ	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	C5_OBJECTIVE_SEQ	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	C5_SUB_MEASURE_SEQ	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	COST_REPORT_DATA_SEQ	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	D17_COST_REPORT_DATA_SEQ	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	DW_EHR_CATEGORY5	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	DW_EHR_CATEGORY7	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	DW_EHR_GLOBAL_CONFIG5	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	DW_EHR_GLOBAL_CONFIG7	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	DW_EHR_LOOKUP_DOMAIN5	MIEHRPRODISR	SELECT
MIEHRPRODISR_READ	DW_EHR_LOOKUP_DOMAIN7	MIEHRPRODISR	SELECT

MTPSM-3-461

Figure 3.10.1-41. Roles and Privilege Report. This report contains the list of roles present in the system along with the list of objects and type of privileges.

Team CNSI's evoBrix PMIS solution contains multiple profiles and roles. A profile is a named set of resource limits and password parameters that restrict database usage and instance resources for a given user. A list of the profiles and a brief description of each is provided in Figure 3.10.1-42.

Profile Name	Profile Description
USER_PROFILE	This profile is assigned to Named Users only
APP_PROFILE	This profile is assigned to Application Schemas and Service Accounts
SYS_PROFILE	This profile is assigned to Admin Schemas within Oracle Database

Figure 3.10.1-42. evoBrix PMIS' Profiles. evoBrix PMIS features multiple profiles which define the user's level of resource limits.

SEC49

The Contractor shall provide and operate solutions for security incident reporting and mitigation mechanisms. The Contractor shall preserve and report specified audit data when security violations are detected and mitigated.

Team CNSI's evoBrix PMIS solution includes a comprehensive security framework for reporting and mitigating security incidents. The system is monitored and protected by different PaaS services within the security suite of the Oracle Cloud. These PaaS services help to identify usage anomalies and system misuse, report security incidents and mitigate the same.

The solution suite includes Oracle SMA Cloud Service, Oracle Log Analytics Cloud Service, and OCM. These tools enable rapid detection, investigation, reporting, and mitigation of the broadest range of security threats across Team CNSI's cloud IT assets. Once these security violations are detected and mitigated, the necessary audit data is preserved and archived using Oracle Archive Storage Classic Cloud Service.

Detailed information about these cloud services and tools is provided in response to requirement SEC06. Figure 3.10.1-43 provides an overview of these solutions that are used for security incident reporting and mitigation along, with their features.

Tier	Solution	Features
All Tiers	Oracle SMA Cloud Service	■ Threat Detection ■ Predictive Analytics ■ Automated Incident Response ■ Simplified Monitoring and Reporting
All Tiers	Oracle Log Analytics Cloud Service	■ Topology-Aware Exploration ■ Efficient Machine Learning ■ Smart Clustering ■ Insightful and Custom Dashboards ■ Light Touch Aggregation
Database Tier	Oracle Connection Manager	■ Connection Multiplexing ■ Access Control ■ Source Routing ■ Firewall Proxy Support ■ Multiprotocol Support

Figure 3.10.1-43. Security Incident Reporting and Mitigation Solutions. An overview of solutions that are used for security incident reporting and mitigation along with their relevant features.

SEC50

The Contractor shall comply with NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices where required by CMS to protect confidential information stored on end user devices.

Team CNSI has established a comprehensive information security policy that helps to protect confidential information stored on end user devices. This information security policy enforces encryption of all confidential data that is stored in Team CNSI's evoBrix PMIS in Oracle Government Cloud. It also enforces encryption on all Team CNSI-supplied equipment, thus enabling the solution to be compliant with NIST Special Publication 800-111: Guide to Storage Encryption Technologies.

Encryption

Team CNSI employs a defense-in-depth approach to securing our solution by implementing multiple layers of network, system, and database encryption technologies to ensure all classified and potentially sensitive data is encrypted at rest and in transit. Figure 3.10.1-44 provides an overview of all the encryption solutions that are used in Team CNSI's evoBrix PMIS.

Tier	Component	Encryption Method	Encryption Algorithm
Database Tier	Data Files	Oracle Transparent Database Encryption	AES-256
Database Tier	Encryption Keys	Oracle Key Vault	PKCS#12 file

Tier	Component	Encryption Method	Encryption Algorithm
Database Tier	Backups	Oracle RMAN Encryption	AES-256
Storage Tier	Oracle Data Pump Exports	Oracle Data Pump Encryption	AES-256
Storage Tier	Flat Files (at rest)	Linux eCryptfs	AES-256
Storage Tier	Flat Files (in transit)	Titan SFTP	SHA-1
Network Tier	Data Traffic	Oracle Network Encryption	AES-256
Network Tier	Data Integrity	Oracle Data Integrity	SHA-1
Application Tier	Network Traffic	SSL Encryption	256 bit SSL
Physical Transmission	Disks/Disk Partition	IDRIX VeraCrypt	AES-256

Figure 3.10.1-44. Data Encryption Solutions. An overview of Data Encryption solutions that are used in Team CNSI's evoBrix PMIS.

Team CNSI-supplied Equipment

All Team CNSI-supplied equipment is configured for encrypted disk and password-protected access at the hardware layer. This includes all workstations, laptops, and mobile devices. Additional details about various protection mechanisms used at all IT systems entry and exit points are explained in detail in SEC38.

SEC51

The Contractor shall comply with NIST Federal Information Processing Standards (FIPS) Publication 180-4: Secure Hash Standards as required by CMS for use of secure hash algorithms.

Team CNSI's evoBrix PMIS solution understands the importance of maintaining data integrity during transit. All connections to the DPHHS PSM system use SSL technology for fully encrypted connection and these SSL connections use TLS 1.2, SHA 2 with a minimum of a 2048-bit key.

Additionally, our solution uses Oracle Data Integrity solution to protect against data modification attacks and replay attacks and the algorithm used here is Secure Hash Algorithm-1 (SHA-1).

- Data modification attack: An unauthorized party intercepting data in transit, altering it, and retransmitting it is a data modification attack. For example, intercepting a $100 bank deposit, changing the amount to $10,000, and retransmitting the higher amount is a data modification attack.
- Replay Attack: Repetitively retransmitting an entire set of valid data is a replay attack, such as intercepting a $100 bank withdrawal and retransmitting it ten times, thereby receiving $1,000.

This ensures that Team CNSI's evoBrix PMIS solution complies with NIST Federal Information Processing Standards (FIPS) Publication 180-4: Secure Hash Standards.

SEC52

The Contractor shall comply with NIST Federal Information Processing Standards (FIPS) Publication 186-4: Digital Signature Standard as required by CMS for use of secure algorithms in digital signatures.

Team CNSI's evoBrix PMIS solution will integrate with the Montana State's IAM infrastructure to provide a seamless IAM experience for internal and external users across the MPATH system. This

integration, along with secure communication uses SSL 3.0/TLS 1.2, ensures message integrity, non-repudiation, and user authentication. The system requires trading partners to digitally sign their application for enrollment in to the system. By using SSL 3.0/TLS 1.2 secure communication, the system is compliant with NIST Federal Information Processing Standards (FIPS) Publication 186-4: Digital Signature Standard.

SEC53

The Contractor shall comply with the Harmonized Security and Privacy Framework - Exchange Reference Architecture Supplement Version 1.0 and as required by CMS

Team CNSI's evoBrix PMIS solution incorporates a Risk-based Security and Privacy framework. Through our implementations in Michigan MMIS projects, our solution has undergone risk assessments based on MARS-E Document Suite standards, thus making it complaint with the Harmonized Security and Privacy Framework - Exchange Reference Architecture Supplement Version 1.0.

Team CNSI's evoBrix PMIS solution is compliant with the following security and privacy controls that are related to Harmonized Security and Privacy Framework. Figure 3.10.1-45 provides an overview of these controls and a short description on how our solution is compliant with these security and privacy controls.

Control Name	Key Compliance Factors	Proposal Location/ Security Requirement #
Security Controls	■ Compliance with security controls that commensurate with the sensitivity and encryption of the data stored and exchanged.	SEC02
Identify, Credential and Access Management	■ Identify Proofing ■ Authorization	SEC01
Secure Infrastructure and Managed Services Computing	■ Data Encryption Solutions ■ Data protection/audit Methods ■ Infrastructure Monitoring Framework	SEC02 SEC07 SEC18
Data Encryption	■ Data Encryption at Rest ■ Data Encryption in Transit	SEC02
Audit Trails	■ Data protection/audit Methods	SEC07
Continuity of Operations and Disaster Recovery	■ Disaster Recovery Process	SEC16
Compliance Oversight	■ Risk Assessment and Management ■ Penetration Testing ■ Protection against Vulnerabilities ■ Continuous Monitoring and Reporting	SEC55 SEC15 SEC38 SEC18
Privacy	■ Accessibility ■ Data Integrity ■ Accountability	SEC64 SEC61 SEC06
Systems and Data Classification	■ FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems ■ FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems	SEC11 SEC53

Figure 3.10.1-45. Harmonized Security and Privacy Framework. Key compliance factors of Team CNSI's evoBrix PMIS solution with respect to the security and privacy controls of Harmonized Security and Privacy Framework.

SEC54

The Contractor shall comply with the OASIS Web Services Security - Simple Object Access Protocol (SOAP) Message Security Version 1.1 Specifications as required by CMS to build secure web services to implement message content integrity and confidentiality.

Team CNSI's evoBrix PMIS solution supports data trading in real-time through evoBrix Oracle Service Bus (OSB) web services. The evoBrix architecture uses an enterprise class service bus (Oracle Fusion SOA) as the core orchestration tool of business processes across the different applications that support Medicaid operations. This solution provides an integration backbone that connects core applications and services without directly accessing the underlying systems. The evoBrix PMIS solution supports robust authorization, authentication, and validation features using OSB. The solution is capable of handling common industry standard service requests such as SOAP and REST. Also, various attributes of the service can be changed without impacting existing clients.

Team CNSI evoBrix PMIS solution complies with OASIS Web Services Security – Simple Object Access Protocol (SOAP) Message Security Version 1.1 Specifications by following the below standards:

- OSB uses WS-security, which is a specification published by OASIS for SOAP web service security. WS-security strengthens the integrity and confidentiality of the messages exchanged between the underlying systems via data encryption, username/password validation, security tokens, and signed messages.
- Team CNSI's evoBrix PMIS solution supports Oracle Web Service Manager (OWSM) via OSB for centralizing policy management and security of Web Services. As part of the OWSM functionality, team CNSI configures key store, create OWSM policy and attach the policy to OSB proxy service to ensure integrity and confidentiality of the message content to secure the web services.

SEC55

The Contractor shall respond to all risks identified through the periodic security risk assessments with a CMS Information Security Program Plan of Action and Milestones (POA&M) containing clarifying information, a proposed mitigation strategy if necessary, a timeline for implementation, and shall work with the Department to successfully execute the POA&Ms.

Team CNSI's evoBrix PMIS undergoes risk assessment covering NIST SP 800-53 Rev 4 standards using NNT's Change Tracker product. Change Tracker's built-in NIST 800-53 report assesses the configured state of our system for compliance with the key NIST Security Controls. The result is a simple percentage score with clear remediation guidance, wherever non-compliance is highlighted. Thereafter, Change Tracker provides real-time monitoring of core configuration settings covering installed software, running processes, services and startup states, registry keys, user accounts, audit and security policy, open network ports, and the overall integrity of the filesystem. This risk assessment covering NIST SP 800-53 Rev 4 is conducted in the following situations:

- Annual basis
- Whenever new or modified functionality impacts the security framework or architecture
- Whenever a new vulnerability exists

Additionally, Team CNSI's hosting platform undergoes penetration testing periodically through an independent third-party security firm. Penetration Testing will be conducted in the following time periods

and the resultant test reports will be submitted to DPHHS. If there are any major or critical vulnerabilities, a mitigation plan will also be provided by Team CNSI to DPHHS.

- Within 6 months prior to implementation
- Annual basis
- Whenever new functionality impacting the security framework gets added or modified

The results of the audits requiring remediation will be put in a Plan of Action and Milestones (POA&M) report, and will be used for the process of remediating any adjustments to the system that come up in the audit. The POA&M worksheet has two sections and the format is based on the NIST standards. The top section of the POA&M documents basic system information and tracks the headers described in the Figure 3.10.1-46.

Headers	Details
CSP	The Vendor Name
System Name	The Information System Name
Impact Level	Systems are categorized as Low, Moderate, or High based on a completed FIPS 199/800-60 evaluation.
POA&M Date	The date the POA&M was created

Figure 3.10.1-46. POA&M Template Header Information Description. Displays POA&M Template Header documents basic system information.

The bottom section of the POA&M Template is the corrective action plan used to track security weaknesses, and shown in Figure 3.10.1-47.

Column	Details
POA&M ID	Assign a unique identifier to each POA&M item
Controls	Specify the security control affected by the weakness identified during the security assessment process.
Weakness Description	Describe the weakness identified during the assessment process. Use the Weakness Description provided by the security assessor or the vulnerability scanner that discovered the weakness
Weakness Severity Level	The severity level is based on the risk the weakness poses to the agency's overall security and privacy posture. There are three levels of severity as defined by OMB: significant deficiency, reportable condition, and weakness.
Weakness Risk Level	Risk level is dependent on multiple factors, such as Federal Information Processing Standard (FIPS) 199 category, operating environment, compensating controls, nature of the vulnerability, and impact if a system is compromised
Asset Identifier	List the asset/platform on which the weakness was found. The Asset Identifier must be unique and consistent across all POA&M documents
Point of Contact	Identify the person/role that is responsible for resolving the weakness
Overall Remediation Plan	Provide a high-level summary of the actions required to remediate the plan. In cases where it is necessary to provide sensitive information to describe the remediation plan, italicize the sensitive information to identify it and include a note in the description stating that it is sensitive.
Original Detection Date	Provide the month, day, and year when the weakness was first detected.
Scheduled Completion Date	Assign a completion date to every weakness that includes the month, day, and year. The Scheduled Completion Date column must not change once it is recorded
Planned Milestones	Each weakness must have a milestone entered with it that identifies specific actions to correct the weakness with an associated completion date. Planned Milestone entries shall not change once they are recorded.
Supporting Documents	List any additional documents that are associated with the POA&M item.
Comments	Provide any additional comments that have not been provided in any of the other columns.

Figure 3.10.1-47. POA&M Template Column Information Description. Shows detailed column information containing corrective action plan to track and fix security weaknesses.

SEC56

The Contractor shall ensure all contractor and subcontractor personnel providing services under this contract are familiar with and comply with the Business Associate Agreement and the privacy and security policies included in the RFP.

All Team CNSI employees, contractors, and subcontractors undergo annual training on all privacy and security policies and also comply with the Business Associate Agreement, as required by the contract, CMS, and federal and state requirements.

SEC57

The Contractor shall provide logical segregation of the Contractor's solution, components, and network connections with other entities and prevent any unauthorized disclosure of the States' data.

The evoBrix PMIS is hosted in an Oracle Government Cloud that is logically separated from other entities to prevent any unauthorized disclosure of any of the State's data. This logical segregation applies to physical resources (CPU, networking, databases, application stack, database storage). Each tenant has their own separate database and application instances. The tenants are isolated from each other through firewalls which means that one tenant cannot see or access other tenant's IT cloud assets.

The confidentiality, integrity, and availability of Team CNSI's evoBrix PMIS solution is secured because of the following features that are an integral part of our solution:

- Data encryption at all tiers
- Full system auditing covering all components and tiers
- Transparency/Audit-ability of Administrative accounts
- Third-party risk assessments and penetration testing
- Virtual Private cloud

SEC58

The Contractor's solution code shall never run from a system level account with unlimited privileges such as "root" or "administrator".

The evoBrix PMIS solution code uses non-system accounts (also called as application service accounts) that have rights that are restricted to only the access needed for the application to run properly. These application service accounts follow the RBAC model that is built in the evoBrix PMIS solution, which is based on the principle of least privilege. Every web application accessing the database has its own application service account. Every user accessing the database, through tools like TOAD or SQL Developer, has their own named user account. These application service account and named user accounts are different from the system or administrative accounts.

No system accounts with unlimited privileges are used to run the application. If anyone tries to login with the system accounts, no matter whether it is successful or unsuccessful, our OCM audit tool detects the same and sends notification alerts and emails to the operations support team. This condition is treated as a non-compliance and necessary remedial actions are taken.

Additionally, all direct access to systems and databases by Team CNSI personnel (including administrators) happens through named user accounts. Each person in Team CNSI is assigned a named user and the naming convention is <last name><first letter of first name><sequence number>).

SEC59

The Contractor shall ensure the confidentiality, privacy, and security of all state data passing through the Contractor and subcontractor networks.

Team CNSI's security architecture emphasizes the importance of protecting and securing data that passes through contractor and subcontractor networks. We employ different mechanisms to ensure the confidentiality, privacy, and security of all state data passing through our networks and subcontractor network.

All connectivity to the evoBrix PMIS is made only via encrypted connections. All backend connections by operations staff are made through encrypted VPN connections. The VPN connections are configured to not allow split tunneling so that the VPN connection does not allow attackers entrance, even when the workstation is on public networks.

- At the application layer, all user sessions to and from the application are encrypted with 256bit SSL. All web sessions are made via HTTPS SSL connections. This approach provides end-to-end network security, reducing the system's exposure to potentially malicious internet traffic and mitigating the possibility of internet-based attempt to defeat critical safeguards that could expose sensitive personal, health, or financial information.
- At the database layer, Team CNSI uses AES-256 based network encryption to encrypt database traffic in transit, thus ensuring that data is secure as it travels across the network. This ensures that encrypted data flows from the evoBrix PMIS to contractor and subcontractor networks.
- Team CNSI uses Secure Hash Algorithm 1 (SHA-1) based Oracle Data Integrity protection to safeguard data against data modification attacks and replay attacks.
    - Data modification attack: An unauthorized party intercepting data in transit, altering it, and retransmitting it is a data modification attack
    - Replay Attack: Repetitively retransmitting an entire set of valid data
- All Team CNSI-supplied equipment is configured for encrypted disk and password-protected access at the hardware layer. This includes all workstations, laptops, and mobile devices. This will ensure that Team CNSI-supplied equipment does not have any vulnerabilities that can be hacked into. By ensuring protection to these end user devices, we safeguard the data that is flowing through CNSI networks and subcontractor networks.
    - Workstations/Laptops
        - Custom, hardened OS image deployed to all Team CNSI laptops and desktops
        - Whole disk encryption applied to all Team CNSI laptops
        - Active Directory authentication and Group Policy enforcement of security configuration standards
        - Commercial virus/malware protection installed on all clients and centrally managed by the CNSI Help Desk
        - Centrally managed OS and patch management using Windows Server Update Services

- Mobile Devices:
  - Custom security configuration profiles installed on all Team CNSI mobile devices
  - Whole device encryption, strong password, and device locking policies centrally managed
  - Remote-wipe capability enabled and centrally managed on all Team CNSI mobile devices

SEC60

The Contractor shall establish and implement emergency access procedures for the Department to obtain secure access to module data during an emergency. Emergency access procedures shall be subject to the Department's approval.

Team CNSI has developed expert knowledge of all applicable industry and Federal standards, models, and practices related to security of state Medicaid systems, and the most recent standards outlined by FedRAMP, HIPAA, HITECH, FISMA, and NIST standards. One of the important access control guideline within HIPAA is to develop emergency access procedures, so that we are compliant with Security Rule safeguard standards and Team CNSI's evoBrix PMIS solution adheres to these Security Rule safeguard standards.

Emergency access refers to loss of data and systems containing electronic protected health information due to an emergency. Emergencies may include, but are not limited to, fire, vandalism, terrorism, system failure, or natural disaster. Team CNSI understands that during such an emergency, delay in accessing vital information could result in danger to someone's health leading to "Access to Care" Issues. Team CNSI gives huge importance to avoid such "Access to Care" issues and so has developed and streamlined the following emergency access procedures.

Contingency Plan

Team CNSI has developed and implemented a Contingency Plan for evoBrix PMIS solution. Team CNSI tests the Contingency Plan every 12 months including the backup media testing. If testing reveals that the Contingency Plan will is ineffective in the event of an emergency or other occurrence, Team CNSI revises the plan accordingly. The Contingency Plan addresses:

- Backups – the strategy and procedures for creating and maintaining system and data backups
- Disaster Recovery – procedures to restore any lost data or functionality in the event of a system outage or other emergency
- Emergency Mode Operations – procedures to enable continuation of critical business processes and maintain the integrity of ePHI while the information system that normally provides the information is unavailable

Disaster Recovery Process

As per the HIPAA guidelines for emergency access procedures, Team CNSI understands that having a proven and robust disaster recovery solution is a very critical requirement. Team CNSI's disaster recovery solution includes a primary data center in Chicago, IL, and the DR Data Center is in Ashburn, VA. The sites are geographically separated to protect from environmental hazards. The remote site is a warm failover site with all data actively replicated from the primary site to the remote site. In the event of the loss of the primary site, the system is reconfigured to bring up the evoBrix PMIS on the remote site within four hours.

The following examples can lead to the declaration of a disaster:

- Extended power outage expected to exceed backup power capacity facility-wide
- Loss of a building or buildings due to fire, flood, earthquake, or a hazardous material (HAZMAT) incident
- Water or structural damage
- Regional or local damage or conditions from severe weather
- Incidents that causes the primary data center or telecommunication lines to be non-functional

The secondary site is fully equipped and meets all the same security standards as the primary site. The secondary site has all the same backups and redundant systems as the primary site. This is to ensure that system operations run smoothly in the event of a disaster and that there are no security or performance issues when running DR site becomes operational. Additional details about the primary and secondary site and its architecture is explained in detail in ENV02 requirement.

Off-site backups

Team CNSI's backup and recovery processing approach is reliable and robust and is based on adhering to the following principles:

- Data is stored in native and encrypted format in local and remote locations
- Data deduplication and replication
- Instant mount features for low Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Fully managed and fully monitored solution by dedicated operations team

CNSI's backup and recovery approach is based on using the following tools:

- Oracle Cloud Backup Service: All the systems are backed up using Oracle's Database Backup Service and Oracle Cloud Infrastructure Object and Archive Storage Classic Service. All data running in the environment is backed up in its native format and stored on off-device storage appliances.
    - Oracle Cloud Infrastructure Object Storage Classic – Storage for both structured and unstructured data including backups supported by enterprise-class data protection, resilience, and elastic scalability
    - Oracle Cloud Infrastructure Archive Storage Classic – Storage for infrequently accessed data with enterprise-grade security, resilience, and elastic scalability
- Oracle Recovery Manager (RMAN): This solution is used to configure and backup the Oracle databases to local and offsite locations. RMAN Backup includes Oracle RMAN Compression and Encryption features to ensure that backups, which are stored in offsite locations, are also secured.

Emergency Mode Operations

Team CNSI has established and documented operations procedures for emergency access processes for the department to obtain secure access to module data during an emergency. The emergency access procedures will be presented to DPHHS for approval.

SEC61

The Contractor's solution must protect data from improper alteration or destruction including authentication mechanisms and to corroborate that the data has not been altered or destroyed in an unauthorized manner.

Protecting the integrity of data is one of the foundational concepts in Team CNSI's evoBrix PMIS solution along with availability and confidentiality. Protecting data integrity not only implies protecting data from improper alteration or destruction but also means that the authorized user has access to the right information at the appropriate time. Inaccurate electronic protected health information could result in harm or even potential death of a patient. In addition, the risk of such information could adversely impair the business viability.

- All data access in Team CNSI's evoBrix PMIS solution is granted on a least access security model. This prevents people from deleting or altering data they are not authorized to delete or alter.
- All application access is controlled using RBAC policies within the evoBrix PMIS application to limit access.
- Direct access to systems and databases by Team CNSI's administrative personnel is restricted based on access controls and Team CNSI uses Centrify's privileged access management solution to control the privileged access.
- Access to underlying databases happens through Oracle Connection Manager which records and audit all user accesses. This solution also allows connections from trusted sources.
- Team CNSI uses Secure Hash Algorithm 1 (SHA-1) based Data Integrity protection to safeguard data against Data modification attacks and replay attacks in the database layer.
- Oracle Database Backups are validated on a weekly basis to ensure that backup data is not altered or destroyed during transit.

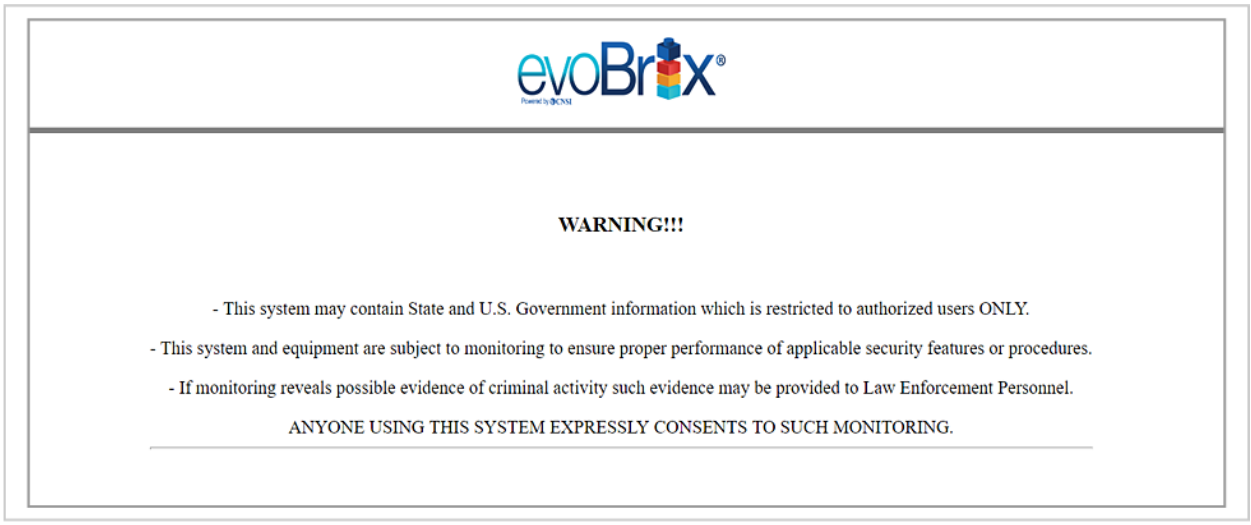
Additionally, all access to data is monitored, logged, and recorded to show who accesses data, and what they do. Access to Team CNSI's solution is monitored and protected by different PaaS services within the security suite of the Oracle Cloud. These PaaS services help to identify usage anomalies and system misuse. The solution suite includes Oracle SMA Cloud Service, Oracle Log Analytics Cloud Service, and OCM. These tools enable rapid detection, investigation, and remediation of the broadest range of security threats across Team CNSI's cloud IT assets. Detailed information about these solutions are explained in SEC06 requirement.

If a breach or system misuse is detected, these security tools records and attempts to shut down the breach and make sure that data is not altered or destroyed in an unauthorized manner. Alerts are generated to the operations staff, who contacts all appropriate Team CNSI staff. Upon resolution of the situation, a full root cause analysis is performed, the system remediated to prevent any future issues, and reports generated and sent to all appropriate stakeholders.

SEC62

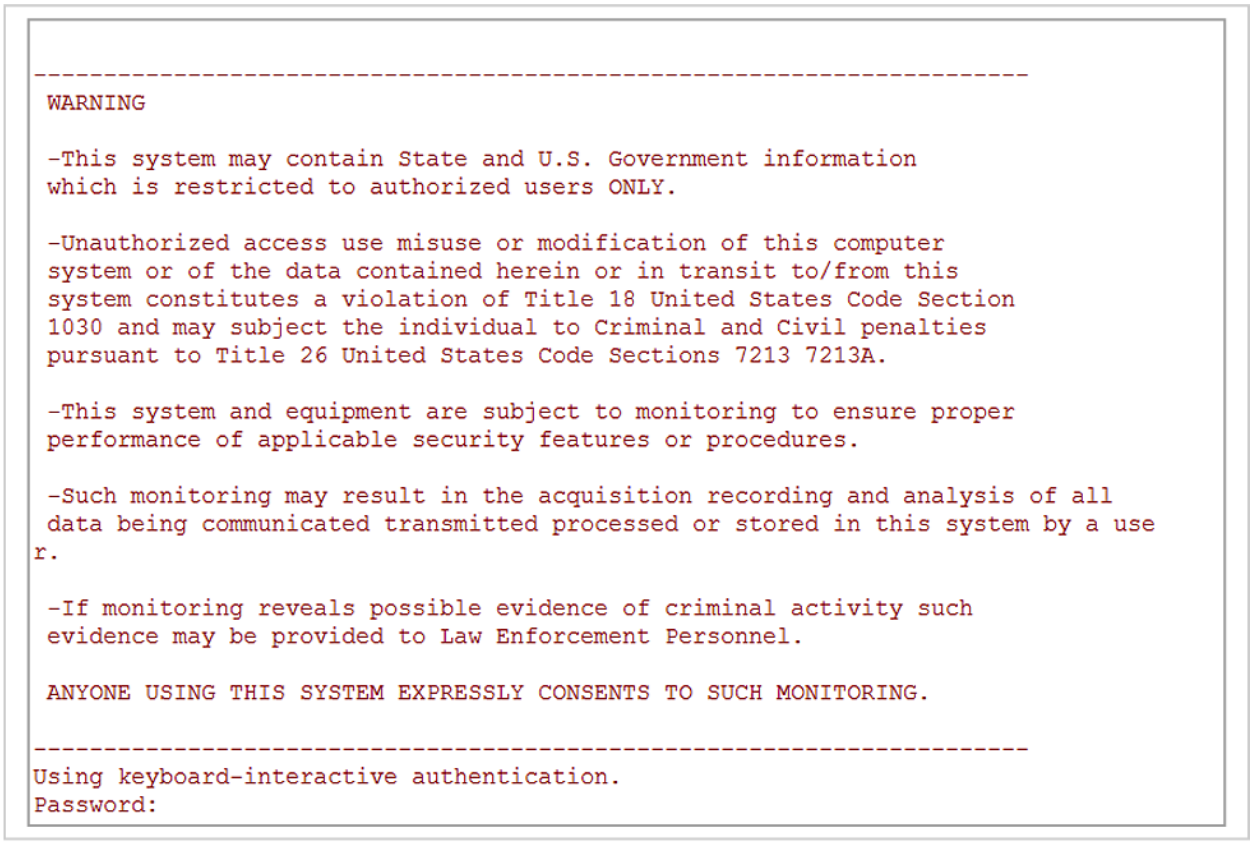
The Contractor's solution shall display a security warning banner prior to allowing entry into the system. The solution shall have security warning banners and headers and footers that adhere to Federal, state, and other applicable standards that are prominently displayed introductory screens.

All access to the evoBrix PMIS includes appropriate security warning banners. The application usage banner message is described in Figure 3.10.1-48. Additionally, Login screens for access to backend systems by systems administrators also displays appropriate security warning banners that is prominently displayed on login and the banner message is displayed in Figure 3.10.1-49.



MTPSM-3-352

Figure 3.10.1-48. Application Usage Banner Message. A security warning banner when logging into Team CNSI's evoBrix PMIS Application.



MTPSM-3-351

Figure 3.10.1-49. Backend System Access Banner Message. A security warning banner when accessing backend systems in Team CNSI's evoBrix PMIS solution.

SEC63

The Contractor shall utilize cloud-based technology wherever advantageous to maximize the efficient and effective utilization of technology.

Team CNSI's proposed solution is built on Oracle Government Cloud Platform that is both FedRAMP and HIPAA compliant. Team CNSI's hosting platform includes hardware and software components that are built using either PaaS, IaaS, or SaaS services and it offers the following features.

Lower Cost While Increasing Automation

Oracle PaaS services includes the highest level of automation which reduces labor costs plus eliminates the cost related to human error. In addition, the IaaS services leverages the best-in-class Oracle virtualization technologies to logically partition physical servers, leading to a lower total cost of ownership.

Increase Business Agility

By leveraging massive economies of scale and unique deployment options, Oracle Cloud Platform assists Team CNSI to quickly setup and kickstart the system setup. In addition, it allows infrastructure components, that are of the same type, to be added or removed quickly. The cloud platform also supports cloud bursting and it is cost effective. It permits additional capacity usage at a metered rate, when the demand for computing capacity spikes. Any additional capacity used is charged on an hourly basis and billed monthly in arrears ("Pay as You Go" model).

IT Efficiency and Reduced Complexity

The Oracle Cloud Platform offers Cloud IT operations as a managed service. This includes patching and maintaining the IaaS and PaaS instances, cloud bursting and gaining operational efficiencies through constantly evolving, best-in-class computing hardware.

Ensure Business Continuity and Security

The Oracle Cloud Platform minimizes system downtime by incorporating high availability architecture at all tiers and ensures rapid data recovery for all types of disaster scenarios. Data protection is achieved by utilizing modern security techniques and multi-layered security, at state-of-the-art data centers. This security architecture also includes advanced data encryption during transmission or storage to protect against security breaches.

A detailed list of all the proposed services and solutions are included in "Attachment L - Technology Metrics." The classification of Infrastructure components and their equivalent Cloud Services are specified in Figure 3.10.1-50.

Infrastructure Components	Cloud Service Type	Cloud Service
Database	PaaS	Oracle Database Cloud Service (DBCS)
Virtual Machines (VM)	IaaS	Oracle Compute Classic Cloud Service
Application Server	PaaS	Oracle Java Cloud Service (JCS)
Integration Platform	PaaS	Oracle Service Oriented Architecture Cloud Service (SOA CS)
Storage	PaaS	Oracle Cloud Block Storage

Infrastructure Components	Cloud Service Type	Cloud Service
Backup Storage	PaaS	Oracle Cloud Object Storage
Backup Service	PaaS	Oracle Cloud Backup Service
Provider Screening	SaaS	Lexis Nexis Screening
Provider Fee Collection	SaaS	First Data Fee Collection Service

Figure 3.10.1-50. Infrastructure components and its equivalent Cloud Services. This classification maps how each infrastructure component is subscribed as IaaS, PaaS, or SaaS services.

SEC64

The Contractor shall ensure user account access is reviewed on a quarterly basis at a minimum. User accounts should be appropriately disabled as roles and responsibilities change.

Operations Management Portal (OMP) is a centralized tool used by Team CNSI's Operations Support team to track and process user access requests. The OMP platform is fully integrated based on ITIL standards. All Team CNSI personnel (including administrators) must access the system (servers, databases, and application) using their own named user accounts only. Access to Application Service accounts or the Administrative accounts ("root," "dba") is restricted.

Team CNSI personnel must create tickets in OMP and follow the User Access Request process to request for new named user accounts. This is applicable for both creating new named users as well as for modifying or dropping existing named users.

All user account access is reviewed on a quarterly basis by Operations Support team. A sample "User Access Report", as shown in Figure 3.10.1-51, is generated for this review process and the steps of this review process is explained below. This report provides a list of all users along with this current account status, the date in which the account was created as well as the profile and roles that was assigned to each named user.

All User Privileges Report for

Report Generated on *Nov 08 2017 12:06:19 PM*

List Of ALL User Privileges

USERNAME	CREATED	ACCOUNT_STATUS	PROFILE	GRANTED_ROLES
ALA	08/30/2017 14:21:43	OPEN	USER_PROFILE	PRDMMIS_READ,CONNECT
ALL	10/14/2015 11:02:53	OPEN	USER_PROFILE	CONNECT,AUDIT_SYS_PRIVS,PRDMMISMCV_READ,PRDMMIS_READ
ANA	05/15/2017 15:30:07	OPEN	USER_PROFILE	AUDIT_SYS_PRIVS,CONNECT,PRDMMIS_READ,PRDCNVSTG_READ
ANB	09/21/2017 14:20:27	OPEN	USER_PROFILE	CONNECT,PRDMMIS_READ,PRDMMISPCS_READ
AND	09/19/2017 10:16:32	OPEN	USER_PROFILE	CONNECT,PRDMMIS_READ
ANN	10/10/2017 10:08:06	OPEN	USER_PROFILE	PRDMMIS_READ,CONNECT
APP	12/31/2011 02:06:30	LOCKED	APP_PROFILE	DV_PUBLIC,DV_ACCTMGR,DV_OWNER,DV_ADMIN,AUDIT_SYS_PRIVS,DV_REALM_RESOURCE,DV_REALM_OWNER
BEL	03/30/2017 11:50:17	OPEN	USER_PROFILE	AUDIT_SYS_PRIVS,MIEHRPROD_READ,CONNECT
BHI	12/30/2011 16:52:03	OPEN	USER_PROFILE	PRDMMIS_MC_834,MIEHRPROD_READ,AUDIT_SYS_PRIVS,CONNECT,PRDMMIS_READ
BHU	01/25/2016 11:11:50	OPEN	USER_PROFILE	AUDIT_SYS_PRIVS,PRDMMISISR_READ,CONNECT,PRDMMIS_READ
BOO	11/03/2017 13:38:09	OPEN	USER_PROFILE	CONNECT,PRDMMIS_READ
BRO	09/16/2009 17:01:01	OPEN	USER_PROFILE	AUDIT_SYS_PRIVS,MIEHRPROD_READ,PRDMMIS_READ,CONNECT,PRDMMISISR_READ
CHA	03/02/2015 15:08:06	OPEN	USER_PROFILE	PRDCNVSTG_READ,CONNECT,PRDMMIS_READ,AUDIT_SYS_PRIVS
CHA	08/03/2015 14:00:15	EXPIRED(GRACE)	USER_PROFILE	DBA,AUDIT_SYS_PRIVS,CONNECT,MIEHRPROD_READ
CHE	09/13/2012 17:13:39	OPEN	USER_PROFILE	PRDMMISISR_READ,PRDMMISIRT_READ,CONNECT,PRDMMIS_READ,AUDIT_SYS_PRIVS
CHE	05/11/2013 09:57:33	LOCKED(TIMED)	USER_PROFILE	DV_ACCTMGR,DV_REALM_RESOURCE,AUDIT_SYS_PRIVS,DV_PUBLIC,DV_ADMIN,DV_REALM_OWNER,DV_OWNER,DBA,CONNECT
CHE	01/05/2016 15:03:47	OPEN	USER_PROFILE	PRDMMISINTCOM_READ,CONNECT,PRDMMISISR_READ,AUDIT_SYS_PRIVS,PRDMMIS_READ,PRDMMISIRT_READ

MTPSM-3-365

Figure 3.10.1-51. User Access Report. This report contains the list of users who are currently active in the system along with the profiles and roles that are assigned to them, and this forms the basis for User Access review process.

User Access Review Process

1. An automated report called "User Access Report" is scheduled every quarter
2. The outcome of this tool is a HTML report containing the list of all Named Users, date in which their named user was created, the current account status and the expiry date
3. Figure 64-1 describes a sample "User Access Report"
4. This report gets delivered to the Operations Support Team, every quarter
5. Operations Support Team reviews the user list
6. During this review process, Operations Support Team raises tickets in OMP, if any of the below conditions are true
   a. If a user left the company or the user is no longer working on the current project
   b. A user's role or responsibilities changed
7. These tickets are assigned to the appropriate administrative teams and necessary action is taken

SEC66

The Contractor's solution shall meet the minimum password requirements below:

1. Must not contain the user's account name or parts of the user's full name that exceed two consecutive characters
2. Minimum password length: 8 characters
3. Contain characters from 3 of the following 4 categories
   a. English uppercase characters (A through Z)
   b. English lowercase characters (a through z)
   c. Base 10 digits (0 through 9)
   d. Non-alphabetic characters (for example, !, $, #, %) (these will not work when logging into ReRite from Toshiba printers ... not on the key pad)
4. History: Cannot reuse a password for 24 password changes, user cannot reset password again for 24 hours
5. Expiration time frame: 60 day
6. Lockouts for failed attempts – account locks after 3 failed attempts, will unlock after 15 minutes

Team CNSI's password policy is based on a combination of password guidelines from both Center for Internet Security (CIS) Benchmarks v2.1.0 and NIST Special Publication 800-63B. Figure 3.10.1-52 provides a complete listing of password guidelines that form an integral part of Team CNSI's password policy. These guidelines surpass the minimum password requirements set by DPHHS.

Password Parameter	Description	Value
Failed Login Attempts	This is the number of failed login attempts before locking the user account.	3 times
Password Lock Time	This is the number of days that must pass after an account is locked before it is unlocked.	1 day
Password Life Time	This is how long an existing password is valid.	60 days
Password Reuse Time	Specifies the number of days before which a password cannot be reused.	30 days

Password Parameter	Description	Value
Password Reuse Max	Specifies the number of password changes required before the current password can be reused.	30 times
Password Reset Time	Specifies the number of hours before which a password cannot be reset.	24 hours
Password Minimum Length	Minimum password length	8 characters
Password Complexity	Contain characters from 3 of the following 4 categories a. English uppercase characters (A through Z) b. English lowercase characters (a through z) c. Base 10 digits (0 through 9) d. Non-alphabetic characters (for example, !, $, #, %) Does not contain the user's account name Does not contain parts of the user's full name that exceed two consecutive characters	

Figure 3.10.1-52. Password Guidelines. A complete listing of password guidelines within Team CNSI's password policy.

SEC67

The Contractor's solution shall track disclosures of ePHI; provide authorized users access to and reports on the disclosures.

Team CNSI has developed expert knowledge of all applicable industry and Federal standards, models, and practices related to security of state Medicaid systems, and the most recent standards outlined by FedRAMP, HIPAA, HITECH, FISMA, and NIST standards.

Team CNSI's evoBrix PMIS solution tracks disclosures of ePHI at application, database, and network tiers using multiple solutions, and these solutions are described below at each tier. It also provides authorized users access to and reports on the disclosures using these solutions.

Application Tier

Disclosure Tracking

At the application tier, Team CNSI's Application Security Framework maintains extensive user audit logging for the audit trail in support of HIPAA Security and Privacy to track changes made to any data stored in PMIS, including ePHI data. The audit record records the following important elements of the current user's session:

- User ID
- Domain Name
- Audit Date
- Application Server ID
- Session ID
- IP Address
- Remarks

Access Control

Team CNSI's application security model is built on a RBAC model, which allows easy, granular control for access to information. The RBAC controls are designed to NIST control standards for authentication and accounting solutions. Users only see the information to which they are authorized to have access; if a user is not authorized to view a set of information, the information is automatically restricted from view. User access to information is easily controlled by the assignment or removal of specific roles to the person. The RBAC model reduces the cost of identity security management and lowers the risk of accidental release of sensitive data.

Disclosure Reports

Users, authorized by the RBAC model, can access audit trail information using the web portal to keep track of who initiated the change, what changed, when the change was requested, who approved/denied the change, and when was it was approved/denied.

Database and Network Tier

Disclosure Tracking

At the database tier, Team CNSI's evoBrix PMIS solution includes a robust and comprehensive auditing solution that is used to record both data changes and data access. This solution includes Oracle database auditing (fine grained auditing) and OCM's audit framework, and it is used to audit all users including administrators.

Team CNSI employs Oracle database auditing (fine grained auditing) to record both data changes and data access at the database tier. Oracle database auditing stores the audit records in a syslog audit trail. Syslog is a standard protocol on Unix- and Linux-based systems for logging information from different components of a network. Thus, a privileged user does not have permissions to access the file system where these messages are logged. For this reason, audit records stored using a syslog audit trail are more secure than audit records stored using an operating system audit trail. The audit record records the following important elements of the current user's session:

- Operating system username
- User ID
- Client Host machine name and IP Address
- User's Terminal name
- Date and time of the creation of the audit trail entry
- Owner of the object
- Object name
- SQL Text of the query
- Data elements of the query (before and after changes)
- SQL statement type (Select or DML)

At the network tier, access to the databases by Team CNSI personnel and applications is monitored and audited using Oracle Connection Manager (OCM). All client and application access to the databases must flow through the OCM and the audit trail is recorded within the audit framework of OCM. Data download limits are enforced via OCM to prevent mass download of information from the system. This prevents intruders from doing a wholesale data dump, limiting exposure if there is an account that has been compromised. Any requests out of the proper norms automatically trigger alerts to operations staff.

Access to data for download is bound by RBAC rules to prevent access to information the person is not authorized to access. All data access is logged, and unusual activity generates alerts.

Access Control

At the database and network tier, Team CNSI's evoBrix PMIS solution employs Operations Management Portal's (OMP) User Access Request process for access control. OMP is a centralized tool used by Team CNSI's Operations Support team to track and process user access requests. The OMP platform is fully integrated based on ITIL standards. All Team CNSI personnel (including administrators) must access the system (servers, databases, and application) using their own named user accounts only. Access to Application Service accounts or the Administrative accounts ("root," "dba") is restricted.

Team CNSI personnel must create tickets in OMP and follow the User Access Request process to request for new named user accounts. This is applicable for both creating new named users as well as for modifying or dropping existing named users. The User Access Request process for creating a new named user is as follows:

1. Team CNSI personnel logs into OMP and creates a ticket for Named User Access.
2. This OMP ticket contains details about the user such as User's First Name, User's Last Name, User's Email ID, User's Phone Number, User's Manager Name, and Contact Details along with the level of access (READ, WRITE) required for each database or application schema.
3. The OMP ticket goes through the approval process workflow. The user's manager reviews the ticket and approves it. This is the first level of approval.
4. The ticket is then approved by the Project Manager, which is the second level of approval.
5. Finally, the ticket is approved by the Operations Manager, which is the third level of approval.
6. All the three levels of approval are based on the Principle of Least Privilege (i.e., only the least privilege that is required to perform the duties is assigned to the named user). If unnecessary privileges are requested in the ticket, then the ticket is denied and the user muat create a new ticket/request with minimal privileges and then start from Step 1.
7. Once the ticket is approved, it is then submitted to the respective admin team.
8. The Admin team then creates the named user. Based on the level of access requested in the ticket, the Admin team will assign appropriate Roles and Profiles to the named user.

This process ensures that only authorized users get access to the system which includes ePHI data.

Disclosure Reports

Team CNSI uses Oracle Log Analytics cloud service to consolidates audit data from databases (syslog audit trail), operating systems, applications, firewalls, and directories into a central reporting repository for compliance reporting and alerting. This service allows for full reporting on additions, modifications, deletions, and access to data within the system.

The evoBrix PMIS solution is also compliant with the HITECH Act's Audit standards including processes that addresses the access, use, and disclosure of PHI and these standards are explained in detail in Figure 3.10.1-53.

Audit Standard	Compliance Factor	Proposal Section
Identify the capabilities of applications and systems to understand what is auditable; disparate systems may require modified audit plans.	Team CNSI's evoBrix PMIS has robust and multi-tier audit system with a centralized repository to store and preserve the audit data	SEC07

Audit Standard	Compliance Factor	Proposal Section
Create and place warning banners on network and application sign-on screens to notify computer users that activities are being monitored and audited to help enforce workforce awareness.	All access to Team CNSI's evoBrix PMIS includes appropriate security warning banners including banners for application access as well as for backend system access	SEC62
Involve application and system owners, when appropriate, to determine what user activities should trigger an entry in the audit trails.	Team CNSI's evoBrix PMIS includes an audit trail of users, who pass through or view a record, regardless of whether data is changed. It also tracks and detects usage anomalies, system misuse, intrusions and hacking incidents	SEC06
Determine how random audits will be conducted as well as the frequency of those audits.	Team CNSI's evoBrix PMIS includes periodic risk based assessments based on NIST SP 800-53 rev4 standards and periodic penetration testing.	SEC55
Develop a standard set of process and documents for incident reporting	Team CNSI's Monitoring System is backed up by a comprehensive Incident Management Plan which includes the processes and procedures to report both successful and unsuccessful incidents, plan strategies and perform mitigation activities	SEC45
Determine what audit tools will be used for automatic monitoring and reporting	Team CNSI's evoBrix PMIS solution includes a robust and comprehensive auditing solution that is used to record both data changes and data access.	SEC07
Determine what to Audit	Team CNSI's evoBrix PMIS mandatorily audits access to all PHI and PII data elements which includes the following 18 HIPAA identifiers. ■ Name ■ Address (all geographic subdivisions smaller than state, including street address, city county, and zip code) ■ All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89) ■ Telephone numbers ■ Fax number ■ Email address ■ Social Security Number ■ Medical record number ■ Health plan beneficiary number ■ Account number ■ Certificate or license number ■ Any vehicle or other device serial number ■ Web URL ■ Internet Protocol (IP) Address ■ Finger or voice print ■ Photographic image ■ Any other characteristic that could uniquely identify the individual	SEC07
Implementing Audit Tools	Team CNSI's evoBrix PMIS solution includes an extensive and reliable auditing solution that is used to record both data changes and data access. This solution includes Oracle database auditing, Oracle Log Analytics Cloud Service and OCM's audit framework and it is applicable for all users including administrators.	SEC07 SEC06
Protecting and Retaining Audit Logs	Team CNSI's Audit system includes the following features: ■ Stores audit logs and records on a server separate from the system that generates the audit trail ■ Restrict access to audit logs to prevent tampering or altering of audit data ■ Retain audit trails based on a schedule determined collaboratively with operational, technical and risk management staff	SEC07

Figure 3.10.1-53. Compliance with HITECH Audit Standards. Team CNSI's evoBrix PMIS solution is compliant with HITECH audit standards based on these compliance factors.

SEC68

The Contractor shall support the State in developing a Privacy Impact Analysis for each module or module component that includes the following information:

– Use of personally identifiable information (PII) or personal health information (PHI) and a description of the types of data that will be collected

– Sources of PII/PHI, populations, and transfer and disclosure mechanisms

– Legal environment (legal authorities and state privacy laws)

– Details about the entities with which the collected information will be shared

– Privacy and security standards for its business partners and other third parties and the agreements that bind these entities

– Incident handling procedures

– Privacy and/or security awareness programs and materials for its workforce

Team CNSI will assist the State in developing a Privacy Impact Analysis for every evoBrix PMIS module that includes the following information:

- Use of PII or PHI and a description of the types of data that will be collected
- Sources of PII/PHI, populations, and transfer and disclosure mechanisms
- Legal environment (legal authorities and state privacy laws)
- Details about the entities with which the collected information will be shared
- Privacy and security standards for its business partners and other third parties and the agreements that bind these entities
- Incident handling procedures
- Privacy and/or security awareness programs and materials for its workforce

SEC70

The Contractor shall provide the ability to de-identify and/or redact data for entities not authorized to receive PII or PHI and utilize de-identification algorithms to allow for re-identification of data if required.

Team CNSI leverages a custom data de-identification solution, dataSecureD, to de-identify both the PHI and PII information in the data. Team CNSI's solution has the capability to de-identify or redact the data when sending it to internal or external entities that are not authorized to receive PII or PHI data.

Team CNSI's dataSecureD solution employs a Metadata Discovery service that is responsible for screening and identifying the potential PHI and PII data elements from the MT PSM solution's data dictionary which are grouped into metadata clusters based on the type of data the PHI or PII entails. For example, the PHI / PII data elements related to names (such as first name, last name, middle name, organization name, etc.) are grouped under a NAMES master group, the data elements related to various types of identifiers (such as Social Security Number, Employer Identification Number, Tax Identification Number, etc.) are grouped under an IDENTIFIER master group, and so on. The solution does allow users to configure selective data elements that needs to be de-identified without requiring a lot of customization.

©2017 CNSI

The de-identification process is typically irreversible once the mapping data set, that is built to crosswalk the PHI/PII data elements to the non-PHI/non-PII values, is dropped. However, if there is a requirement to re-identify the de-identified data set, the dataSecureD solution has provision for customizing the de-identification process to not drop the mapping data set. To support the necessity for re-identifying the data, the mapping data set is archived and encrypted to a secured location that can then be used for data re-identification, as necessary.

Detailed information about Team CNSI's dataSecureD product and the de-identification solution is explained in SEC71 requirement.

SEC71

The Contractor shall provide a process for masking, sanitizing, scrambling, or de-sensitizing sensitive data (e.g., PII/PHI) when extracting data from the production environment for use in non-production environments.

Team CNSI ensures that data in all development and system test environments for MT PSM only house scrambled, masked, de-identified data to support the solution configuration and development activities. As part of our experience from implementing and supporting multiple Medicaid systems for the States of Michigan, Washington, Illinois, and Utah, Team CNSI leverages a custom data de-identification solution, dataSecureD, to safeguard both the PHI and PII information in the data. dataSecureD aims at providing a comprehensive data de-identification solution that ensures compliance with the Data Privacy and Protection mandates, most notably, the HIPAA Privacy Rule. With this solution, sensitive PHI and PII data can be replaced with de-sensitized, but realistic values, allowing production data to be safely and meaningfully used for development, testing, and/or shared with external partners for business needs. The dataSecureD solution comes with the features and benefits as illustrated in Figure 3.10.1-54 to support the masking/de-identification needs for MT PSM.

Features	Benefits
■ Pre-configured components and templates that reduces the upfront work required to define the de-identification rules and data relationships as it is purpose-built for Team CNSI's evoBrix PMIS solution. ■ Fast, reliable, and secure. Leverages a highly scalable framework for scrambling the data using in-database MapReduce principle. ■ Ensures both structural and data integrity which is key for ensuring the MT PSM solution functionality isn't disrupted due to the scrambling of the sensitive data. ■ Repeatable process for multiple runs with full restart capabilities. ■ Process is irreversible by default, but configurable should the need dictate, once the mapping dataset is dropped after the de-identification process. Data cannot be rolled back or back tracked to its original value.	■ Greatly reduces the risk of a privacy data breach because the MT PSM project staff would only have access to de-identified data in the non-Production environments such as Development and System Test. ■ Multi-factor de-identification scheme vastly randomizes the assignment of non-PHI/non-PII values from the mapping dictionary by first removing the existing PHI data values to create empty placeholders before overwriting the placeholders with the de-identified data. ■ Facilitates reasonably quick provisioning of realistic de-identified data for supporting the development and testing phases of SDLC. ■ Eases security configuration in vendor-hosted DB environments. ■ Greater productivity/ease of access to realistic, but anonymized/de-identified data, for higher work quality. The more you know your data, the better the outcome. ■ Drives key operational, analytical, and strategic initiatives.

Figure 3.10.1-54. Features and Benefits of Team CNSI's Data De-identification Solution. Team CNSI's dataSecureD solution has several readily available features that are easily configurable to benefit the data de-identification needs for MT PSM.

The dataSecureD solution is built to mask/scramble the following 18 identifiers. Under the HIPAA Privacy Rule, these "identifiers" can reasonably be used to identify an individual and hence needs to be masked/scrambled/de-identified.

1. Names
2. Geographic subdivisions smaller than a state
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, and date of death and all ages over 89 and all elements of dates (including year) indicative of such age (except that such ages and elements may be aggregated into a single category of age 90 or older)
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

SEC72

The Contractor shall review and identify monthly, any unneeded hardware, software, and licenses, present recommendations to the State for review and ensure that any unneeded hardware, software, and licenses have been decommissioned upon approval from the State.

Team CNSI employs a comprehensive capacity management process which adheres to the ITILv3 standards. Team CNSI has broad and deep experience in various state MMIS implementations and will leverage its success and lessons learned to ensure that the hardware and software infrastructure for the evoBrix PMIS solution fully addresses DPHHS identified requirements. We use real-time operational metrics from production implementations for capacity planning. The outcome of capacity planning helps to identify any unneeded hardware, software and licenses, that can be decommissioned through the Change Control Board (CCB) process, upon approval from the State. This enables Team CNSI to provide a low-risk, cost-effective infrastructure for managing and operating the evoBrix PMIS solution.

Team CNSI uses the following tools and methods to support ongoing resource capacity use during operations:

- HealthBeat constantly reports all areas including applications and OS resources and generates reports, which helps to monitor and plan the future resource needs
- OEM provides a single pane for managing and monitoring various components, such as databases, middleware, and servers

Team CNSI's Capacity Planning approach is divided into three dimensions:

- Component Capacity Planning
- Service Capacity Planning
- Business Capacity Planning

Component Capacity Planning

Team CNSI uses metrics, such as claim volumes, enrolled providers, and concurrent business operations staff, to size the recommended hardware and software components. This sizing also considers the amount of data that must be stored by the evoBrix PMIS solution, ensuring that the system is sized sufficiently to maintain and retain all data and imaged and electronic documents for the retention timeframes specified by DPHHS.

Team CNSI's Component Capacity Management looks at additional metrics such as:

- Number of users and transactions
- Type of transactions
- Data retention
- Database size
- Location of system compared to location of users
- Expected transaction performance, for both transactions and overall system uptime
- Duration parameters for maintenance windows
- Disaster recovery requirements

Service Capacity Planning

During operations, Team CNSI proactively monitors all hardware and software components. Team CNSI looks for trends that indicate capacity and performance issues that may occur in the future. In the event of a trend that indicates a risk, we take proactive steps to resolve capacity issues before the problem occurs. Our process for analysis is to:

- Identify monitoring touch points, frequency, and schedule
- Prioritize the monitoring metrics to identify the most relevant and applicable
- Collect metrics from various monitoring tools throughout the system
- Identify subsystems, processes, components, or system functionality that are not performing optimally
- Generate performance deficiency reports and distribute them to analysts for assessment

Business Capacity Planning

Team CNSI's business capacity solution addresses challenges related to the volumes of members, providers, and new programs anticipated for the future, as well as issues related to performance, maintenance, and availability.

The hardware platform for the evoBrix PMIS solution has been designed to allow future expansion without impacting operations. Servers used for the system are implemented in a load balanced/cluster configuration allowing for horizontal and vertical expansion. Team CNSI offers the options of adding more CPUs, memory, or input/output (I/O) boards to existing servers, or adding newer equipment and decommissioning the older servers to achieve higher levels of performance, if necessary.

Change Control Board (CCB) Process

Based on the inputs from the capacity planning reports, any unneeded hardware, software and licenses can be decommissioned by going through the Change Control Board (CCB) process. Direction is determined by consensus of all organizations represented at the CCB including, at a minimum, personnel from Team CNSI and DPHHS PMO. The CCB represents the interests of project management by ensuring that a structured process is used to decommission any unused hardware, software and licenses.

The Change Control Board performs the following:

- Reviews the current hardware, software and license assets monthly
- Requests that impact analysis of proposed hardware and software changes be performed including changes to operational and acquisition costs
- Makes recommendations to the State for final decisions on decommissioning excess hardware or licenses
- Starts decommission process for any unneeded hardware and software assets, and starts procurement process for any new hardware and software requests
- Reviews the hardware or software changes for both decommission and procurement processes
- Makes decisions and monitors progress of the hardware and software installation or deinstallation
- Communicates decisions made to affected groups and individuals

As a part of our technical processes, Team CNSI establishes two CCBs to manage review and approval of changes as follows:

- Tier 1 CCB – consisting of Team CNSI technical and business operations staff with a focus on reviewing and approving changes
- Tier 2 CCB – consisting of Team CNSI, DPHHS, and SI staff to review status of tickets and approve changes prior to production implementation

SEC73

The Contractor will provide the completed reports with the results of the service organization control (SOC) 1 Type II audit annually on date identified by the State. The Contractor shall provide a mitigation plan for all areas of non-compliance. Issues found to be non-compliant shall be corrected within forty (40) calendar days of the report submission to the Department.

Team CNSI's system is built on a multi-layered security approach that protects the backend client data from unauthorized access. Team CNSI's FedRAMP and HIPAA compliant Data Centers perform annual audits to comply and achieve certification with Statements on Standards for Attestation Engagements/Service Organization Control (SSAE/SOC), FedRAMP and HIPAA standards. All these certifications will remain in place for the duration of the contract and Team CNSI can provide DPHHS with the most recent version of compliance certificates and audit reports on an annual basis. The following certifications are in place to provide for the confidentiality, integrity, and availability of the information systems:

- SSAE 16 SOC 1 Type II
- SSAE 16 SOC 2 Type II
- HIPAA/HITECH
- Federal Risk and Authorization Management Program (FedRAMP)

Team CNSI will provide completed reports after each annual security audit of the system. If there are items found to be non-compliant, then there will be a POA&M report also released with remediation plans and the same will be presented to the CCB on an emergency basis. The system will be remediated within 40 calendar days of the release of the report and the necessary changes are updated in the CMDB.

3.10.1.3 Hosting and Environments

This section addresses hosting and environment requirements. The Department prefers cloud based hosting for the proposed solution. The Department expects the delivery of the solution/services to be seamless with the hosting solution providing the flexibility to integrate other solutions for security and regulatory purposes in the future, and be cost-effective and scalable. Also, the Contractor is expected to provide a hosting environment for all solution components that has a Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance, or has a documented NIST 800-53 rev 4 at a "moderate" system risk assessment designation. In addition, the Contractor is required to demonstrate that their hosting solution is Statement on Standards for Attestation Engagements (SSAE-16) SOC 1 Type 2 and SOC 2 Type 2 compliant.

In their response, the Offeror must describe their approach to solutions and services that meets State and federal regulations, security and performance requirements detailed in Attachment F, Requirements Matrix.

Team CNSI's private cloud will be hosted in the Oracle FedRAMP compliant Government Cloud. The primary data center will be in Chicago, IL, and the Disaster Recovery (DR) Data Center will be in Ashburn, VA. These data centers utilize a robust and redundant infrastructure architecture to provide maximum uptime for critical data, applications, and technologies. In addition, these data centers provide managed services that are anchored in world-class secure data center facilities with best-of-breed infrastructure and highly robust network architecture. All hardware components including servers, switches, storage appliances, backup storage appliances, and firewalls are hosted in HIPAA compliant and FedRAMP compliant data centers. Team CNSI's private cloud is elastic and scalable to allow for both short-term capacity spikes as well as long-term growth as needs evolve.

The Team CNSI Advantage

Team CNSI's private cloud solution enables high performance and high availability business operations with built in scalability for future growth.

- Hosted in Oracle's FedRAMP-compliant and HIPAA-compliant Government Cloud
- A multi-tier secure solution, compliant with federal standards and mandates
- Elastic and scalable to meet current and future needs
- A private cloud hosted on a industry-leading virtualization platform
- A robust set of managed services - IaaS, PaaS and SaaS services
- A full-scale Disaster Recovery Platform backed up by a well-tested and proven Disaster Recovery Process

MTPSM-3-187

ENV02

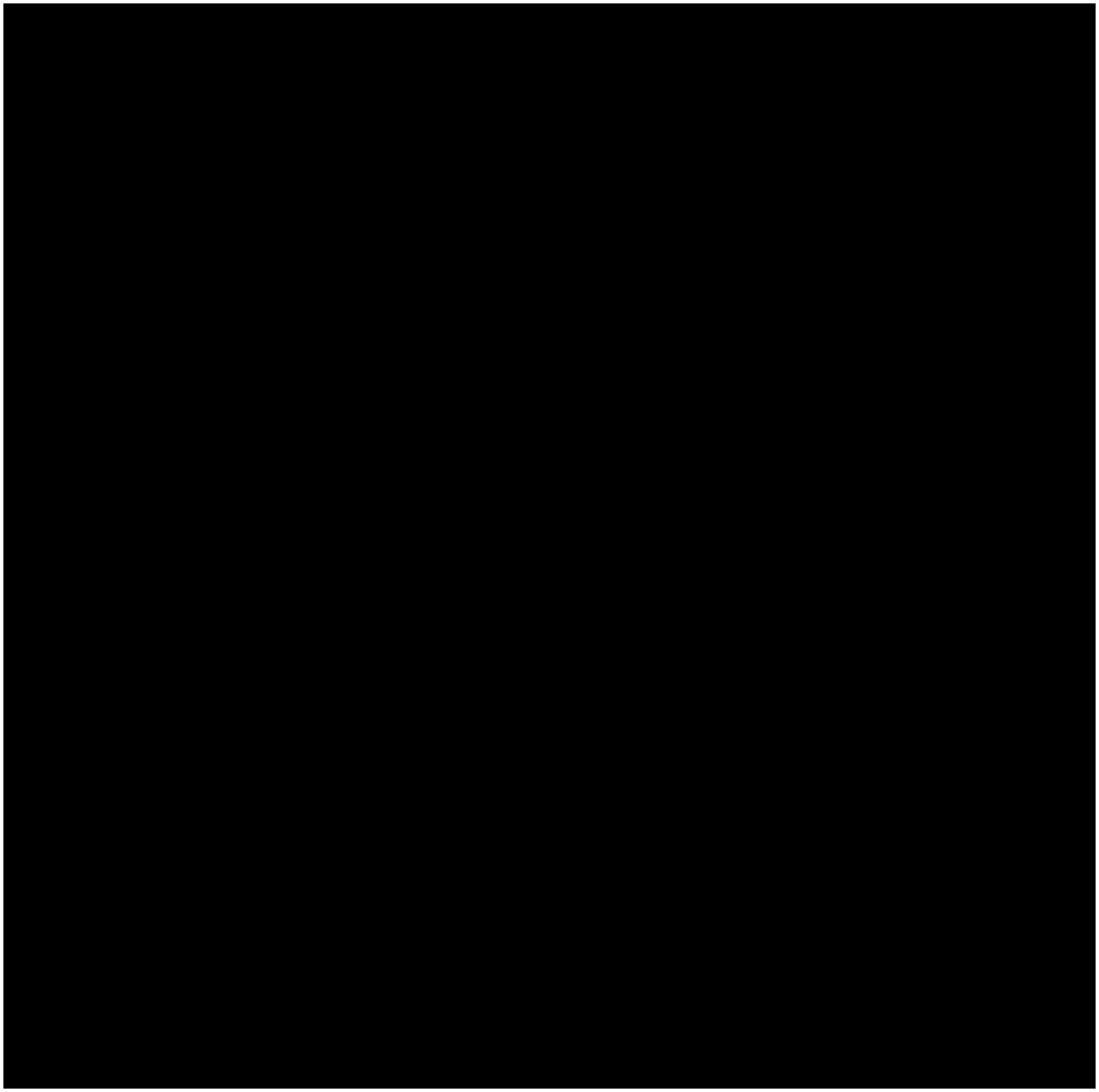
The Contractor shall provide hosting services that shall meet all state requirements.

Team CNSI's hosting solution meets all of the state requirements a outlined below and in the following requirement responses.

Hosting Platform Topology

An overview of the hosting platform topology starting from firewalls to Storage Area Network (SAN) is explained in Figure 3.10.1-55. The topology starts with the Firewall Pair (for high-availability) at the top.

These are connected to the Application Host VMs through the 10 GB switches. The Application Host VMs are then connected to the Database Hosts through the 10 GB switches, which in turn are connected to the Hybrid SAN via 40GB switches. An identical topology exists for the DR site as well, so that system operations run smoothly in the event of a disaster.



Managed Services and Key Features of Hosting Platform

Team CNSI's evoBrix PMIS solution includes managed services at the data center level covering security services, data services, network services, and infrastructure services. Figure 3.10.1-56 provides an overview of Oracle Cloud's hosting solution, types of managed services, and certifications.

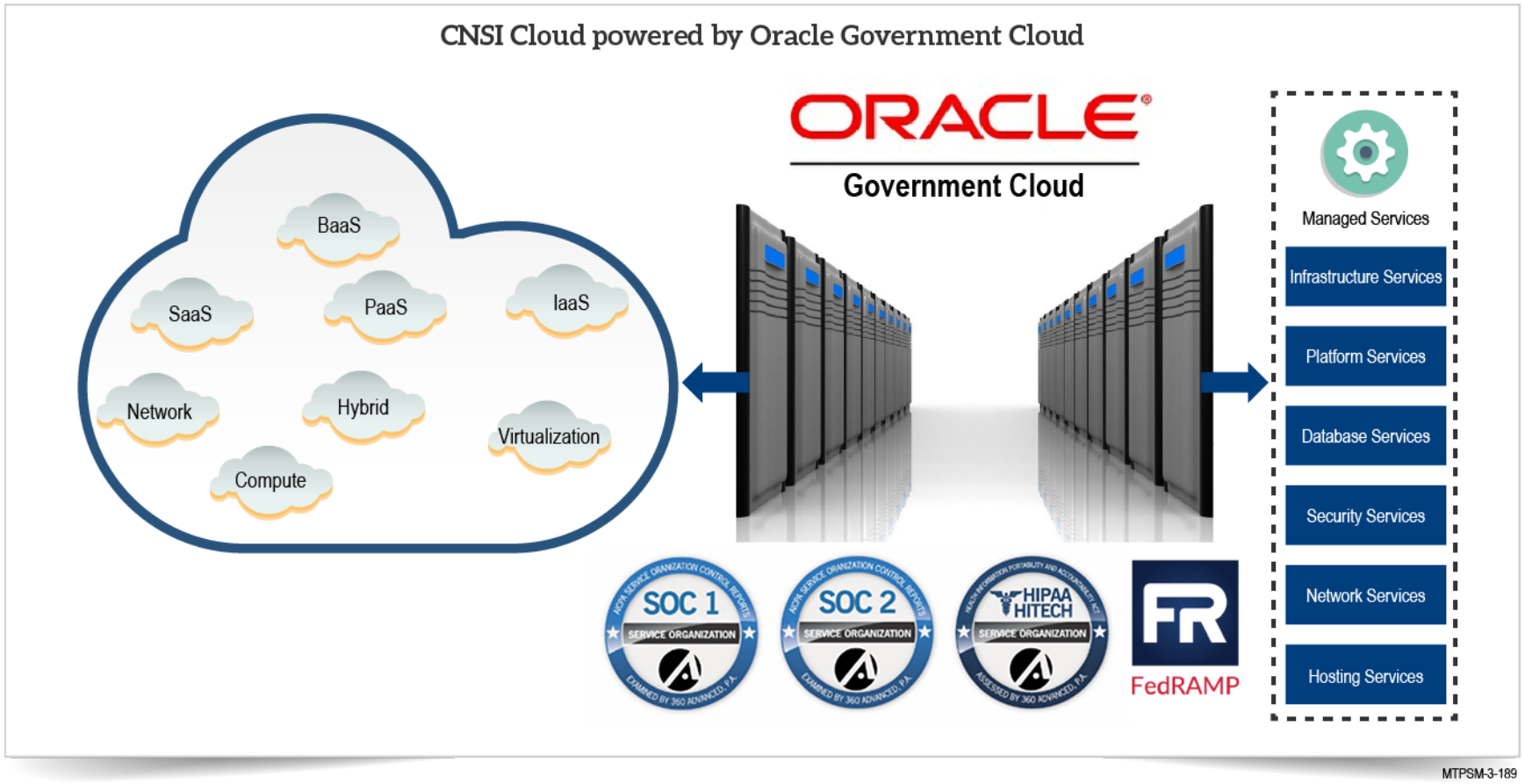


Figure 3.10.1-56. Hosting Solution Overview. Oracle Cloud's hosting solution, types of managed services, and certifications reflect the robust solution Team CNSI offers the State.

Team CNSI's hosting platform includes hardware and software components that are built using Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) services including multiple security and encryption solutions. Figure 3.10.1-57 provides an overview of the various PaaS, IaaS, encryption and security services that form the building blocks of Team CNSI's evoBrix PMIS solution. All hardware and software components that are required to support the proposed solution and services will have the necessary licensing agreements in place for the entire duration of the contract.



Team CNSI's hosting platform has several state-of-the-art features in the areas of fire control, security and communication services, power, and environment. An overview of the key features of Team CNSI's hosting platform solution is shown in Figure 3.10.1-58.

Key Features of Hosting Platform	
Service	**Summary**
Location	■ Chicago, IL and Ashburn, VA ■ Locations selected for low risk of natural disasters ■ Geographically diverse ■ Tier III Type Data Center Tier ■ HIPAA and FedRAMP compliant Oracle Government Cloud
Power	■ Complete N+1 power redundancy infrastructure ■ Cooling Redundancy = N+2 ■ Industry-leading environmental support systems ■ Generator-protected lighting/HVAC systems
Environmental	■ Complete N+2 infrastructure for heating and air conditioning ■ High-efficiency DSE Series Liebert CRAC Units
Fire Control	■ State-of-the-art fire suppression and detection systems ■ Sprinkler heads with failsafe triggers
Security Services	■ Secure access through biometric hand-geometry or card scanners ■ Manned security and monitoring via CCTV cameras ■ Defense-in-depth security ■ Oracle badged security experts safeguard your data ■ Strong Encryption standards ■ Secure Data Isolation ■ Advanced Application Security Options ■ Secured perimeter fencing ■ Restricted roof access
Compliant with SSAE 16 Requirements	■ Customer environments isolated through cabinets and/or cages ■ Stringent access controls and restrictions, including biometrics
Communication Services	■ Carrier-neutral – customer chooses any telco that has presence at the data center or is willing to invest in connectivity to the data center ■ High-speed, and low-latency connection between customer data center and Oracle Cloud services that unlocks the benefits of a true hybrid cloud setup and offers better security than exchanging your data over the Internet
Structured Wiring and LAN Communications	■ Multiple carriers and diverse points of entry ■ Dual links for network hubs ■ Diverse fiber entrance paths ■ Duplicate Hardware: Transit Router/Switches/Firewalls/Load Balancers ■ Distribution & Access Layer Switches ■ Multiple up links per component
Efficiency	■ World-class data center with best-in-class network topology and connectivity options for optimum performance ■ High-speed and low-latency connection between customer data center and Oracle Cloud services ■ Uptime SLAs of 99.9% (PaaS) and 99.95% (IaaS) ■ World Class Security, Change Management, Backup, Support ■ Response time for Severity 1 Issues of 15 minutes ■ Published and committed Change Management cadence ■ Capacity on demand ■ Use of "Thousand Eyes," a network intelligence platform, to quickly and precisely pinpoint performance changes caused by device faults, congestion, route leaks, DNS failures and service provider outages.

Key Features of Hosting Platform	
Service	**Summary**
Remote Access	■ All customer connections inbound from the Internet encrypted via TLS. ■ Standard whitelisting service employed where incoming customer connections over TLS will be restricted to specific source IP addresses. ■ High-speed, and low-latency connection between customer data center and Oracle Cloud services allows customer to completely control remote access ■ Each cloud service is secured by a service firewall, and all incoming and outgoing traffic passes through it via the edge router using public IP addresses. Traffic for such inter-service communication never leaves the Oracle Cloud network at that data center.

Figure 3.10.1-58. Data Center Key Features. The most highly-secure, highly-efficient, and stable Data Center will be built by Team CNSI to host the evoBrix PMIS solution.

Hardware Component Specifications

Team CNSI's evoBrix PMIS solution is built on a resilient, redundant design with best-of-breed infrastructure and a highly robust network architecture. All hardware components including servers, switches, storage appliances, backup storage appliances, and firewalls have in-built redundancy in both the primary and standby/DR data center. The primary site will host Test (System Test, User Acceptance Test, Regression Test) and Production environments, while the standby/DR site will host Stage (Performance, Parallel Test, B2B) and DR environments. An overview of all Hardware Component Specifications that will host Team CNSI's evoBrix PMIS solution at the Primary site is explained in Figure 3.10.1-59.

Primary Site	
Compute Nodes	■ Compute for Application Servers • Storage I/O Control • Software defined network • Dynamic Firewall • Secure SSH access • Instance Anti-Affinity • High Availability ■ Oracle Database Cloud Service (DBCS) for Database Servers • Real Application Cluster (RAC) for High Availability • Transparent Database Encryption (TDE) and Network Encryption • Data Guard for DR Solution • Automatic Storage Management (ASM) for Storage with 3-way mirroring • 40Gbps InfiniBand Networking
Switches	■ 10 Gbps FastConnect Switch ■ 40 Gbps InfiniBand Switch
Firewalls	■ Monitor and control network communications at the external boundary of the network and at internal boundaries within the network ■ Deployed in a layered approach to inspect and filter packets ■ Use of network vulnerability assessment tools to identify security threats and vulnerabilities ■ DDoS protection/mitigation: A certified firewall appliance with dedicated DOS protection enabled ■ Network Intrusion Detection Systems (NIDS) • Intrusion Prevention Mode (IPS) • Intrusion Detection Mode (IDS)
Backup	■ A redundant and highly available cloud backup solution ■ End-to-end security and support ■ Local and remote data storage ■ On-demand storage and continuous accessibility ■ Usable copies of production data for various use cases

Primary Site	
	■ Fully managed solution ■ Faster deployment

Figure 3.10.1-59. Hardware Component Specifications at Primary site. Team CNSI chooses cost effective, highly efficient, and highly redundant hardware without compromising on system performance and SLA.

An overview of all Hardware Component Specifications that will host Team CNSI's evoBrix PMIS solution at the DR site is given in Figure 3.10.1-60.

DR Site	
Compute Nodes	■ Compute for Application Servers ● Storage I/O Control ● Software defined network ● Dynamic Firewall ● Secure SSH access ● Instance Anti-Affinity ● High Availability ■ Oracle Database Cloud Service (DBCS) for Database Servers ● 40Gbps InfiniBand Networking ● Real Application Cluster (RAC) for High Availability ● Transparent Database Encryption (TDE) and Network Encryption ● Data Guard for DR Solution ● Automatic Storage Management (ASM) for Storage with 3-way mirroring
Switches	■ 10 Gbps FastConnect Switch ■ 40 Gbps InfiniBand Switch
Firewalls	■ Monitor and control network communications at the external boundary of the network and at internal boundaries within the network ■ Deployed in a layered approach to inspect and filter packets ■ Use of network vulnerability assessment tools to identify security threats and vulnerabilities ■ DDoS protection/mitigation: A certified firewall appliance with dedicated DOS protection enabled ■ Network Intrusion Detection Systems (NIDS) ● Intrusion Prevention Mode (IPS) ● Intrusion Detection Mode (IDS)
Backup	■ A redundant and highly available cloud backup solution ■ End-to-End Security and Support ■ Local and remote data storage ■ On-demand storage and continuous accessibility ■ Usable copies of production data for various use cases ■ Fully managed solution ■ Faster deployment

Figure 3.10.1-60. Hardware Component Specifications at DR site. In the event of a disaster, the DR site will be fully operational within 4 hours (RTO). The DR site is sized equivalent to the Production Infrastructure, so that operations are not affected during a disaster.

ENV03

The Contractor's hosting solution shall provide the flexibility to integrate other solutions for security and regulatory purposes in the future and be cost-effective with burst capacity.

Team CNSI's evoBrix PMIS solution is hosted in Oracle's FedRAMP and HIPAA compliant Government Cloud. This hosting platform has all the cloud features in-built to support any future expansion based on workloads.

For security and regulatory compliance, the hosting platform is flexible enough to integrate with other solutions, that can be installed on a temporary or permanent basis. Team CNSI's hosting platform allows IT resources (infrastructure components), that are of the same type, to be added or removed quickly. This flexibility is because all infrastructure components are either built using Platform as a Service (PaaS) services, Infrastructure as a Service (IaaS) services, or Software as a Service (SaaS) services, thereby creating a highly flexible and elastic environment. Additional PaaS or IaaS services in Team CNSI's private cloud can be subscribed or cancelled to, on an ad hoc basis, using the "Pay as you go" subscription model.

Team CNSI's hosting platform also supports cloud bursting and it is cost effective. It permits additional capacity usage at a metered rate, when the demand for computing capacity spikes. Any additional capacity used is charged on an hourly basis and billed monthly in arrears ("Pay as You Go" model).

For example, if the current database server has 4 cores allocated and you are running a monthly job that requires additional computing power, then the cloud bursting feature will add additional cores to the database server, to meet the additional demand. This additional capacity used is charged on an hourly basis and billed monthly in arrears ("Pay as You Go" model).

ENV04

The Contractor's hosting environment for all module components shall be compliant with Statement on Standards for Attestation Engagements (SSAE-16) SOC 1 Type 2 and SOC 2 Type 2 and has Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance, or has a documented NIST 800-53 rev 4 at a "moderate" system risk assessment designation.

Team CNSI's system is built on a multi-layered security approach that protects the backend client data from unauthorized access. Team CNSI's FedRAMP and HIPAA compliant Data Centers perform annual audits to comply and achieve certification with Statements on Standards for Attestation Engagements/Service Organization Control (SSAE/SOC) and HIPAA standards. All these certifications will remain in place for the duration of the contract and Team CNSI can provide DPHHS with the most recent version of compliance certificates and audit reports. The following certifications are in place to provide for the confidentiality, integrity, and availability of the information systems:

- SSAE 16 SOC 1 Type II
- SSAE 16 SOC 2 Type II
- HIPAA/HITECH
- Federal Risk and Authorization Management Program (FedRAMP)

Additionally, Team CNSI's evoBrix PMIS solution includes security and privacy controls that are compliant with the most current version of the CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E) and National Institute of Standards and Technology (NIST) standards. Team CNSI's evoBrix PMIS solution adheres to the following security standards

- Federal Information Security Management Act (FISMA)
- Internal Revenue System (IRS) Publication 1075
- Patient Protection and Affordable Care Act (PPACA) or (ACA)

- NIST Special Publication 800-66 Revision 1
- NIST Special Publications 800-53 and 800-53A
- NIST Special Publication 800-47
- NIST Special Publication 800-88 Revision 1
- NIST Special Publication 800-111

ENV05

The Contractor's solution shall be available and accessible twenty-four (24) hours a day, seven (7) days a week, with the exception of planned downtime due to system upgrades or routine maintenance. All planned downtime and maintenance outages shall be coordinated and approved by the Department at least five (5) business days in advance.

Team CNSI reviews business process availability requirements and aligns them with our ITIL framework. This ensures that cost-effective contingency plans are in place and tested on a regular basis to ensure that the business needs of DPHHS are met. Team CNSI's Availability Management Plan includes but is not limited to the following aspects:

- Designing high-availability, redundant systems to support mission-critical applications
- Testing system availability to meet all DPHHS SLAs
- Monitoring and reporting high-availability to ensure that SLAs are being met

High Availability Architecture Design

Team CNSI's evoBrix PMIS solution addresses challenges related to additional volumes and new programs anticipated for the future, as well as issues related to performance, maintenance, and availability. In addition, the solution leverages virtualization technologies to logically partition physical servers, leading to a lower total cost of ownership. Given our cloud-based architecture, scalability and elasticity are features; our solution supports normal business activities with the ability to increase the demand on the system by 50% without modification to the software or degradation in performance.

Team CNSI's high-availability architecture includes:

- Clustering at physical host level to provide for physical host failure
- Application server cluster with load balancing
- Web server load balancing
- Oracle Database real application cluster for database high availability
- Oracle Data Guard solution for database replication
- Oracle Recovery Manager (RMAN) for database backups
- Flashback technology for point-in-time recovery
- Data Recovery Advisor for performing recovery analysis

Figure 3.10.1-61 depicts the high-level availability architecture covering clustering at the application server and database server level as well as web server load balancing.

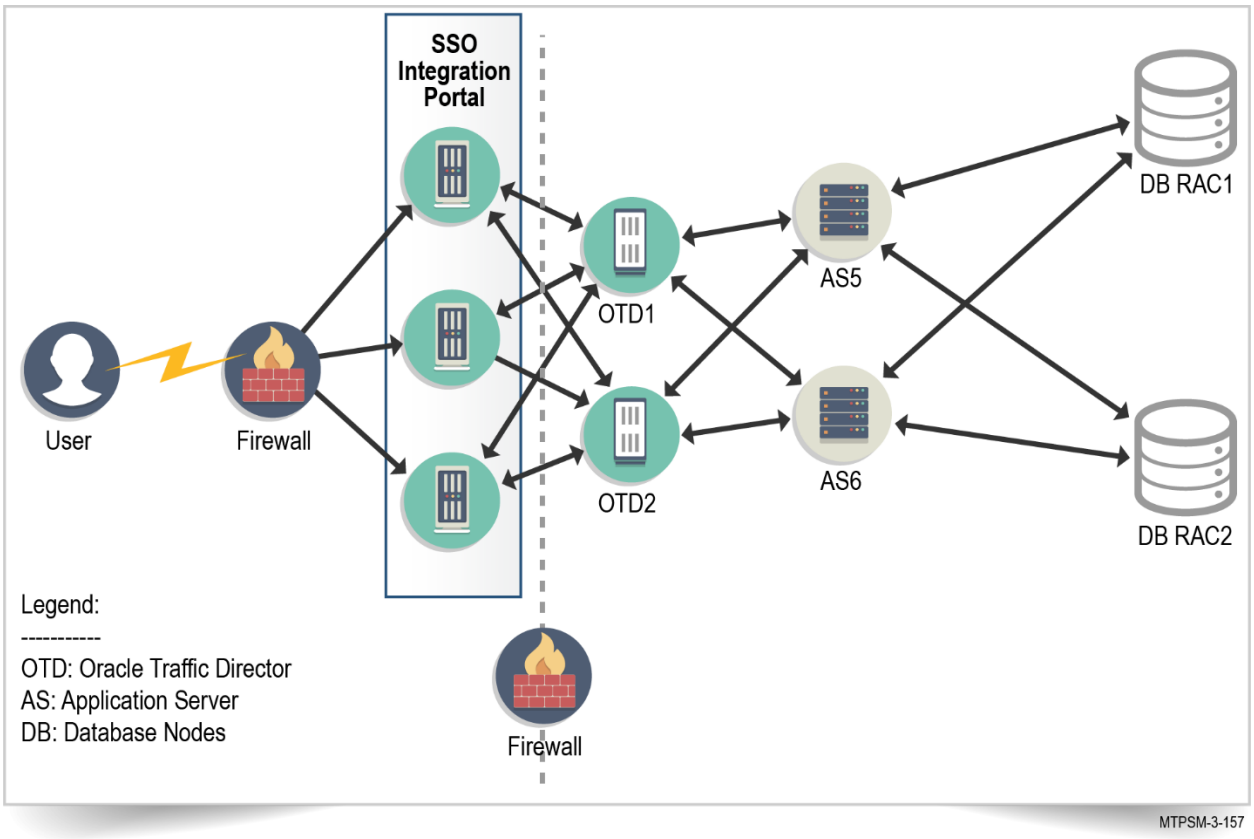


Figure 3.10.1-61. High Availability Architecture. Clustered architecture at the application server level and database server level provides load balancing and high availability capabilities.

There are three types of maintenance windows:

- Scheduled Maintenance (no downtime)
- Scheduled Maintenance (with downtime)
- Unscheduled Maintenance

Scheduled Maintenance (No Downtime)

This type of maintenance covers all regular maintenance activities such as system modifications and changes. This type of maintenance does not require downtime because high availability is achieved via multiple redundant services, resulting in no interruption to operations. Figure 3.10.1-62 contains a list of components that provide redundancy and scalability needed to support the system 24 hours a day, seven 7 days a week.

System Components	Built-in Redundancy
Telecommunications	The telecommunication circuits have redundancy with diverse paths.
Network	Firewalls, switches, and other network equipment are configured in redundant load balanced pairs to eliminate any single point of failure.
Application Servers	Pairs of load balancers interface with application servers that serve end users.

System Components	Built-in Redundancy
Database Servers	Oracle Real Application Cluster along with Database Backups and Data Guard Replication ensures high availability for databases

Figure 3.10.1-62. Redundancy of System Components. Team CNSI's solution provides redundancy to maximize availability for business operations.

Scheduled Maintenance (With Downtime)

This type of maintenance covers all regular maintenance activities that require downtime. There are some configuration parameters that cannot be altered online and hence require a downtime window. CNSI will collaborate with DPHHS to develop a regular monthly maintenance schedule and plan during the implementation planning phase. The maintenance plan is accompanied by an impact analysis plan as well as a timeline required for the downtime. All communication regarding the planning and approval of the planned downtime will be collaborated with DPHHS at least five business days in advance.

Unscheduled Maintenance

This type of maintenance covers high priority changes that cannot wait until the next scheduled maintenance window or release. Unscheduled maintenance is not typically a common occurrence; however, we have processes in place to address it. In such cases, Team CNSI will plan an ad hoc maintenance schedule in collaboration with DPHHS and will seek formal approval before executing the same. This ad hoc maintenance plan will also be accompanied by an impact analysis plan along with the timelines and contingency plans.

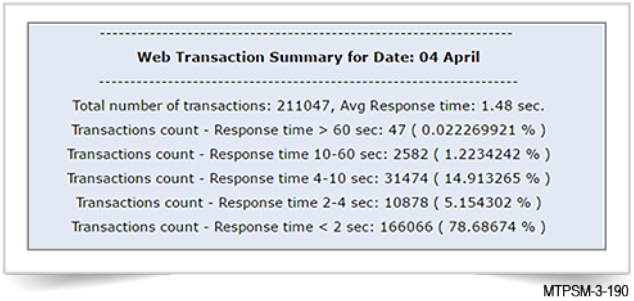
System Availability

Team CNSI's evoBrix PMIS solution architecture undergoes varied levels of high-availability testing in test and performance environments before propagating the changes to a production environment. High-availability testing ensures designing for tolerance, recoverability, and reduced occurrence of high-severity faults. It measures business impact from faults and helps in planning for reducing impact. The testing activities include stress testing, load testing, and distributed denial-of-service (DDoS) attack testing, as well as testing individual hardware component failure and cluster failover capabilities.

OEM, HealthBeat, Building Management System (BMS), and Data Center Infrastructure Management (DCIM) solutions, in combination, help to provide the necessary monitoring and reporting capabilities for this high-availability architecture. This monitoring and reporting framework will monitor, detect, and report any loss in the high-availability functionality across various layers of hardware and software components.

Team CNSI's solution is also reinforced by a high-performance load balanced application framework and a robust monitoring framework. Team CNSI developed a configurable tool to monitor SLAs. Additional details about this tool's capabilities are outlined in Section B2.4.1.1, Service Level Agreement, subsection SLA Automation Tool and Operational Performance Standards.

Figure 3.10.1-63 depicts one of the reports coming out of the SLA Automation Tool. This report provides details on the number of transactions as well as their response times in each day.



MTPSM-3-190

Figure 3.10.1-63. SLA Automation Tool Report. Web Transaction Summary report provides details on the response times of the web transactions across different buckets.

Monitoring and Reporting High-Availability

Team CNSI's evoBrix PMIS solution includes a comprehensive and complete system monitoring and reporting framework. This framework ensures that the high-availability components are working properly across the system. OEM, HealthBeat, BMS, and DCIM provide monitoring and reporting capabilities covering all layers of hardware and software components. Figure 3.10.1-64 provides a classification of monitoring tools and their respective infrastructure modules.

Monitoring Tool	Infrastructure Modules
Oracle Enterprise Manager	Databases and Database Servers SOA Suite Application Servers
HealthBeat	Application Interfaces/Web Services Servers
Building Management System	Data Center Power and Cooling
Data Center Infrastructure Management	Infrastructure

Figure 3.10.1-64. Monitoring and System Performance Reporting Tools. This classification of monitoring tools and their associated infrastructure modules forms the backbone of the monitoring framework.

Oracle Enterprise Manager (OEM)

Team CNSI's database administrators and system administrators rely on OEM to maintain, monitor, and configure proactive alerts for Oracle databases, SOA Suite, and Application Servers. Oracle Management Service (OMS) monitors various targets and collects the performance metrics. These metrics are then uploaded to the Repository through a Java Database Connectivity (JDBC) API. The OEM Console and Enterprise Manager Command Line Interface (EMCLI) enables administrators to access and manage OEM functionalities, which in turn sends notifications and alerts to the NOC. The NOC triages issues to the appropriate operations team for corrective action. Team CNSI's proactive monitoring enables us to predict when issues may arise in the future. By monitoring trending data, we can determine whether a system is likely to have issues. For example, if we see that a system is spiking on CPU usage and memory on a regular basis, that system may require a hardware upgrade or optimization to remove capacity concerns.

Figure 3.10.1-65 shows the OEM architecture. Various alerts are configured in OEM to issue immediate notifications as soon as an issue occurs. Alerts are sent to the necessary teams and a NOC team that monitors the system 24x7x365 and communicates the same to the respective teams. Figure 3.10.1-66 shows the OEM database load map showing the health of all the registered clustered databases in a single pane of view.

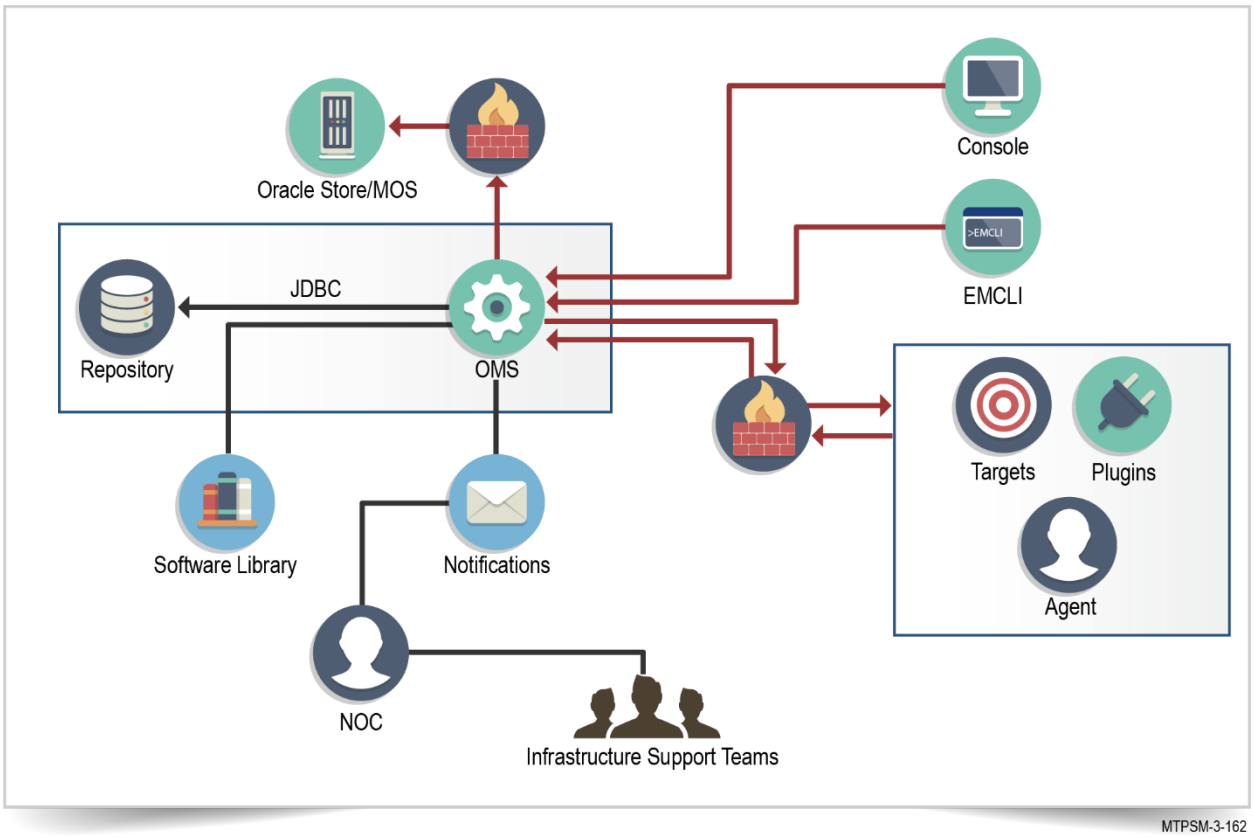


Figure 3.10.1-65. OEM Architecture. OEM monitors the availability and performance of the database and application servers and alerts the necessary teams.

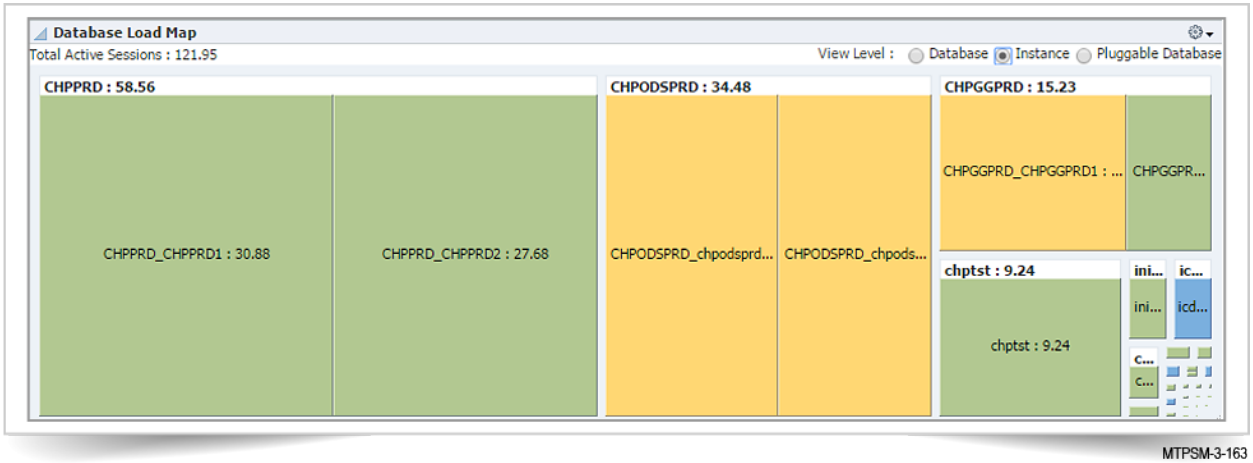


Figure 3.10.1-66. OEM Database Load Map. Portrays the health of all the registered clustered databases in a single pane of view.

Building Management System and Data Center Infrastructure Management

BMS alerts critical facilities staff and engineers of any issues. Depending upon priority, a ticket is executed and staff resolve or assign vendors for ticket completion and issue resolution. The BMS handles monitoring of power and cooling.

DCIM monitors all environmental systems (e.g., temperature, humidity, power usage, leakage, efficiencies of equipment and systems). Additionally, DCIM monitors all video and door access surveillance from a central NOC, staffed 24x7x365. Together, BMS and DCIM help to monitor and report any loss in high-availability functionalities across hardware and software components in the data center layer.

ENV06

The Contractor shall provide the ability to run multiple sessions /environments/applications/areas/views simultaneously. This includes providing sufficient environments and configurations (e.g., multiple environments, multiple application layers, hub architecture) necessary to perform all required functions (e.g., testing, training, production operations, modeling, disaster recovery).

Team CNSI's evoBrix PMIS solution is modular and highly scalable supporting multiple applications and sessions in different logical environments. These applications are configured in different layers. Team CNSI has established robust and proven ITIL compliant SaaS processes from implementations in Michigan, Illinois, and Utah. These processes enable a DevOps model to maximize system capability and, more importantly, productivity with business operations.

Environment Topology

Team CNSI's evoBrix PMIS solution is highly scalable and supports multiple environments starting from Development to Production. Every environment mentioned below supports concurrent sessions and applications necessary to perform parallel concurrent processing. The environment topology along with the purpose is listed in Figure 3.10.1-67.

Zone	Environment	Purpose
Build	Build & Deploy	This environment contains Applications, Tools, and Utilities that are required to perform Build, Deploy, Versioning, Modelling, Design, IDE, and Development functions.
Development/Test	Development	Used for Development purposes. Contains de-identified data. No PHI/PII data is present here.
	System Test	Used for Unit testing and System Testing purposes by Team CNSI's testing team to support operational releases. Contains de-identified data.
	UAT	User Acceptance Testing is performed here by business users to support Operational Releases.
	Regression	This is a Production Patch Environment and it support Emergency Operational Releases.
	Conversion	This environment is used for Data Conversion activities.
Stage/DR	Training/Outreach	This environment is used for Training purposes ("Train the trainer").
	Performance	Performance test and load test is performed in this environment before go-live and every major release. This has production like configuration and dataset.
	Disaster Recovery (DR)	Standby Environment that will become active during a disaster (within 4 hours).
Production	Production	Production environment.

Figure 3.10.1-67. Environment Topology. List of all environments in Team CNSI's evoBrix PMIS solution.

Application Topology and Hub Architecture

Every environment in Team CNSI's evoBrix PMIS solution is composed of multiple applications and areas necessary to perform the designated business functions. This application topology also includes applications that needs to be integrated with the DPHHS's Enterprise Service Bus (ESB) hub. The interaction between various applications and areas that are required for a logical environment is depicted in Figure 3.10.1-68.

Team CNSI's evoBrix PMIS solution will integrate with the DPHHS's Enterprise Service Bus (ESB) hub, as mandated by DPHHS's security requirements. A handshake is established first with the exchange of certificates between the PMIS and other state agencies. This establishes a 256bit SSL encrypted tunnel. Every web service request will need to contain a username/password that would have been provided to the account owner as part of registration/access to the application along with all the mandatory request fields as agreed to between Team CNSI and the State Agencies. A valid response is then provided to this web service request from the evoBrix PMIS solution upon a successful authentication and authorization.

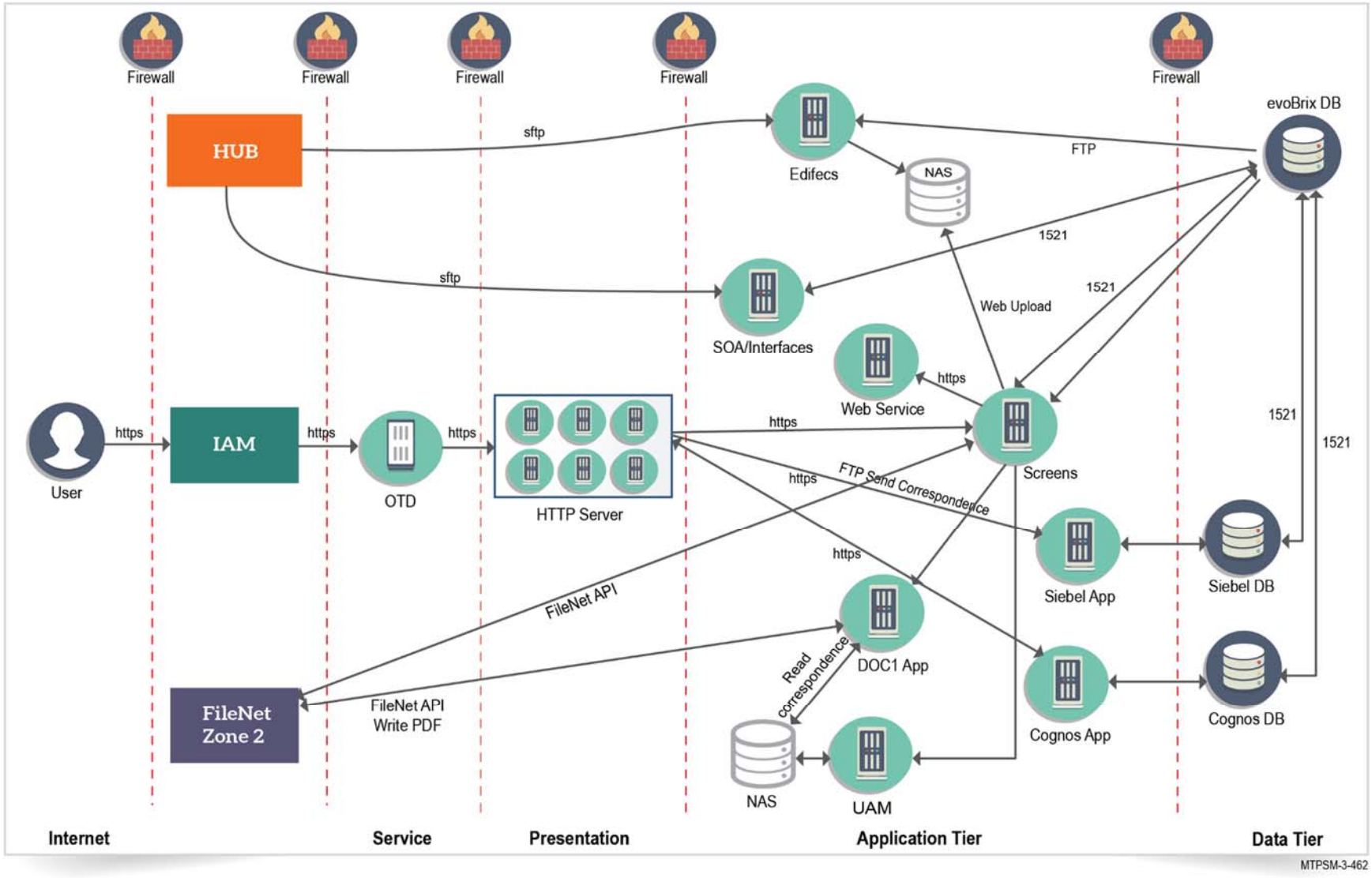


Figure 3.10.1-68. Deployment Topology Diagram. Interaction between different applications and areas present in a logical environment in Team CNSI's evoBrix PMIS solution.

Detailed information about various applications and areas that are required for a logical environment along with their version numbers and vendor information is specified in Figure 3.10.1-69.

Product/Application/Area	Version	Category	Vendor
IBM Cognos	10.2.2	Reports	IBM
IBM FileNet	5.2.x	ECM	IBM
IBM InfoSphere DataStage	11.5	Conversion	IBM
Oracle Database	12c	Database	Oracle
Oracle RAC	12c	Database Cluster	Oracle
Oracle JDK	1.6.x/1.7.x/1.8.x	Application Server	Oracle
Oracle Siebel CRM	8.1.1.14 PS 13	CRM	Oracle
Oracle SOA	12.1.3	Integration Tool	Oracle
Oracle WebLogic (Base)	12c	Integration Tool	Oracle
Oracle WebLogic (Cluster)	12c	Integration Tool	Oracle
Oracle Enterprise Manager	12c	Monitoring Tool	Oracle
Oracle Advanced Security	12c	Database Security	Oracle
Oracle MySQL	5.x	Database for OTRS	Oracle
Linux	OEL	Operating System	Oracle
Spectrum UAM	11	Correspondence	Pitney Bowes
EngageOne DOC1GEN	6.0.1	Correspondence	Pitney Bowes
EngageOne DOC1 Designer	6.x	Correspondence	Pitney Bowes
EDIFECS XEngine Server	8.8	EDI	EDIFECS
Avaya		IVR	Avaya

Figure 3.10.1-69. Application Topology. List of all applications present in a logical environment in Team CNSI's evoBrix PMIS solution.

Configuration Management – Views and Areas

Team CNSI understands the need for a robust Software Configuration Management system to support multiple application areas and views in every logical environment. Team CNSI's software configuration Management policies and procedures are based on our iVision360 SDLC methodology, tailored to configure Team CNSI's evoBrix PMIS platform and components to meet the MT PSM solution implementation and operational needs.

This approach will allow the following for evoBrix PMIS solution:

- Consolidated snapshot of Configuration Items (CIs) for the project
- Manage multiple subsystems, areas and views in each environment
- Snapshot of baseline contents
- Configuration Control for Configuration Management (CM) systems

- Specifications on building work products out of CM systems
- Maintain the integrity of the baseline

Team CNSI's knowledge and understanding of building, testing, and successful integration of various modules to provide the requisite services provided by a PMIS solution is based on multiple implementations certified by CMS, coupled with adherence to the industry best practices by following the ITIL-aligned CM policies, processes, and procedures. This provides a framework to avoid any unauthorized changes, manage the baselines to support multiple environments, and provide traceability and auditing for all CIs throughout the lifecycle of the evoBrix PMIS solution.

Hardware Change Management

This section describes the functions of change control board (CCB) as it relates to the management of hardware changes for the evoBrix PMIS solution. All Configuration Items (CIs) related to Hardware and Software License Asset Management, are identified, documented, and tracked in the Configuration Management Data Base (CMDB). Team CNSI uses Combodo's iTOP as the CMDB tool for Hardware and Software Asset Management. Additional details about iTOP and Team CNSI's CMDB solution is provided in SEC03 requirement.

The CCB represents the interests of project management by ensuring that a structured process is used to consider purchases or upgrades or decommission of hardware and supporting the installation of the hardware to support this solution. Direction is determined by consensus of all organizations represented at the board including, at a minimum, personnel from Team CNSI, and DPHHS PMO.

The Change Control Board:

- Requests that impact analysis of proposed hardware changes be performed
- Reviews the hardware changes
- Makes decisions regarding hardware
- Monitors progress of the hardware installation
- Communicates decisions made to affected groups and individuals

Testing

Team CNSI conducts multiple rounds of Iteration, System, Parallel, Integration, and Regression testing to correct defects discovered during testing. The testing activities occur in multiple environments across different applications. Once all test cases for the phase have met the acceptance criteria for exiting the test, a final assembly of all test results is created to demonstrate to DPHHS that the test has been completed successfully. At the end of system testing, Team CNSI submits all test cases and test scripts as part of the System Test Results report.

Environment Refresh Process

After every major operational release, Team CNSI's infrastructure teams (DBA/CM/Sys Admin Teams) performs a backup of the Production environment. This backup is used to refresh all Development, Test, and Stage environments. This refresh schedule is planned based on inputs from the Operations Team and is fully automated. During the refresh process, a copy of the production data is also de-identified using Team CNSI's dataSecureD product and the resulting de-identified data is then deployed into Development and System Test Database.

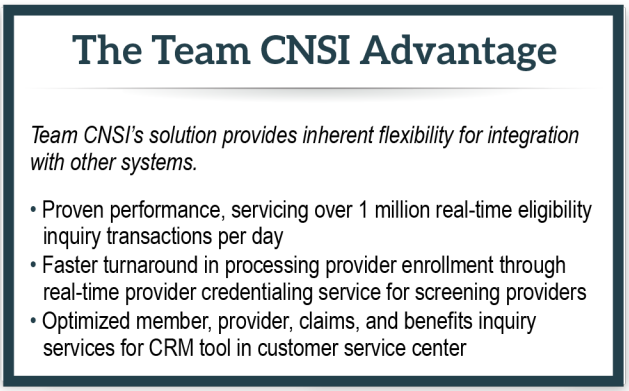
ENV07

The Contractor shall identify the physical location(s) where the Contractor's solution is installed and operating. The Department must have transparent access to this location(s).

Team CNSI's private cloud will be hosted in Oracle's FedRAMP compliant Government Cloud. The primary data center will be in Chicago, IL, and the DR Data Center will be in Ashburn, VA. Since these data centers are FedRAMP compliant and are operated by a third-party, Team CNSI will provide FedRAMP certification and audit information, when requested.

3.10.1.4 Integration

This section addresses integration requirements for the Contractor's solution(s) and operations. As part of the DDI, the successful vendor will be required to interface with the legacy MMIS and the MPATH Integration Platform once it is established. Once the MPATH Integration Platform is implemented, the Department expects the vendor to integrate with the MPATH Integration Platform through standardized interfaces. The ESB is the communication broker and web services orchestrator for MPATH Integration Platform which is administered by the MPATH Systems Integration Services Contractor. The Provider Services component(s) must ensure all service endpoints/APIs are clearly defined, exposed to the ESB and be able to receive and submit messages through the ESB to facilitate standardized data exchanges throughout the MPATH Integration Platform. The offeror must describe their approach to meet each of the integration requirements detailed in Attachment F, Requirements Matrix.



MTPSM-3-340

Team CNSI understands the technical and business considerations behind DPHHS' migration towards the use of real-time web services, and our evoBrix Integrator provides the technical and functional support needed to realize these goals. Developed from the ground up using Service Oriented Architecture (SOA)-based architecture in alignment with Medicaid Information Technology Architecture (MITA) principles, Team CNSI's evoBrix platform provides inherent flexibility for integration with other systems and promotes a high degree of interoperability, reuse of functionality, and ease of maintenance. In support of meeting the near real-time web services goal, Team CNSI provides infrastructure components required to implement web services; technical components that provide support to design, publish, and consume web services; and business services that provide prepackaged services that can be readily used by external agencies who need access to real-time data. We provide the following components and services to support integration services:

evoBrix Integrator components

- **evoBrix web services framework** – Team CNSI's framework helps users build and develop services using frontend programming application program interfaces (APIs) such as JAX-WS and JAX-RS. These services can speak a variety of protocols such as Simple Object Access Protocol (SOAP), XML/HTTP, RESTful HTTP, or CORBA and work over a variety of transports such as HTTP, JMS, or JBI.

- **Oracle fusion SOA** – Component of the evoBrix Integrator, the Oracle SOA tool provides an industry standard service orchestration framework using BPEL based process orchestration capabilities.
- **Oracle fusion Oracle Service Bus (OSB)** – SOA mediation layer capabilities OSB for services-based integration between other modules in the enterprise environment through the MPATH System Integrator platform.

Technical components

- **evoBrix Integrator** – Team CNSI's evoBrix Integrator supports automated data exchanges with various PMIS business process areas and interface partners.
- **OpenAPI** – Representational State Transfer (REST) API follows industry standard OpenAPI specification also called Swagger Specification. The contractors and external entities who need to access our services using these services will have a rich UI that serves as a sandbox for interactive testing of the REST API. They will get hands-on experience with the services, and it will speed up the integration process with parallel development.
- **Apache CXF Client libraries** – These provide very flexible libraries to discover, implement, and consume web services implemented by agencies external to MPATH.

Business Services

Team CNSI is working across public and private sectors to define a comprehensive, reusable, open-source technical architecture to support MITA business categories. The goal of this work is to provide a Medicaid-specific reference architecture that can be leveraged across State Medicaid Agencies (SMAs) to implement commutable, interoperable Medicaid Management Information Systems (MMIS). Through engagement with industry stakeholders to create a MITA reference architecture, CNSI is helping to create standard definitions for application services to combine business processes into standard objects to be packaged into modules. The development of a modular reference architecture across MITA business categories progresses the concept of modular design, reinforces the Medicaid Enterprise commitment to the Seven Standards and Conditions, and supports the technical evolution of SMAs

- **Pre-existing web services** – Our evoBrix solution comprises a rich portfolio of production-ready, real time services that are optimized for the Medicaid environment. They provide inquiry capability for most of the System of Record (SOR) data and business services to meet function needs of external systems.

The key interoperability capabilities of the proposed solution are as follows:

- SOA/Standards-based integration approaches using protocols including REST, SOAP, and COTS APIs.
- Support for standard content formats such as documents, XML, JSON, EDI for user, and machine-readable and understandable content.
- REST APIs leveraging Swagger specifications for producing, consuming, and visualizing APIs. Used to support service inquiries.
- SOAP APIs leveraging WSDL specifications for data exchange with business partners for post services. Versioning through the Mediation layer allows for rapid adoption of change. Web-services-based information exchange for real-time integration capabilities.
- COTS APIs expose COTS functionality as internal and external interfaces through standard APIs. Examples include Document Management API, Workflow API, Correspondence API, and Siebel API.

- Supports for standards-based information exchange for EDI transactions (e.g., HIPAA ANSI X12 standards). Support for secure FTP gateway. Compliance with CORE rules.
- File-based information exchange for standard and non-standard file based integration.

Secure information exchange using API keys, web service security 1.0 standards, and other security protocols for securing data during transit please refer to section 3.10.1.2 Security for further details about security protocols.

The proposed solution achieves real-time operation by leveraging SOAP and REST web services, which has the potential to transform DPHHS into a real-time enterprise. In fitting with DPHHS technical architecture, our MPATH solution's REST API or SOAP services would be exposed through DPHHS ESB for consumption by relevant trading partners. Team CNSI will expose all the service endpoints/APIs required to integrate with MPATH vendors through our OSB Infrastructure. In doing so, DPHHS can avoid the use of batch jobs, and allow trading partners to learn on a real-time or near real-time basis when outbound claims, provider, and member data are available for processing. The inbound services will accept information from DPHHS and trigger business logic or updates to user data objects for processing. These would enable DPHHS to move away from a batch-oriented environment and towards a near real-time world using web services on a service-oriented architecture. Team CNSI will provide Interface Control Documents (ICDs) for its services to the MPATH vendor. Since all service endpoints are exposed to the ESB, the external agencies will be able to receive and submit messages through the ESB.

Team CNSI follows a 'design first' approach when developing its REST APIs for target audiences who are the external customers and trading partners. Since the 'design first' approach advocates for designing the API's contract first before writing any code, we use Swagger Specification to publish the API description. The clients consuming these services will have a rich User Interface (UI) that serves as a playground for interactive testing of the REST API. The approach is transparent to the clients, speeding up the integration process with parallel development.

There are several instances of enabling real-time web services supported in our production environments that can be leveraged for meeting DPHHS needs. The following are the different scenarios of near real-time web services usage that are available in the evoBrix solution.

- **Scenario 1:** External systems and agencies that need real-time access to proposed MPATH SOR data. This is a typical usage scenario as several external systems and agencies need access to SOR data that is generated and maintained in proposed MPATH solution.
    - evoBrix solution comprises a rich portfolio of production-ready, real time services that are optimized for the Medicaid environment. It exposes feature-rich web services, including services for members, providers, and claims.
    - These services are consumed by any external state agencies and internal entities like Siebel CRM application.
- **Scenario 2:** MPATH business processes that need access to external web services in real-time to make business decisions and support Medicaid business process.
    - Our Provider Credentialing Services solution calls the real-time credentialing service exposed by LexisNexis during Provider Enrollment screening processes with provider's enrollment information. The real-time response received from LexisNexis is used to support the provider enrollment decision making process.

- **Scenario 3:** External system and agencies that need orchestration of real time business processes with MPATH business processes.
  - **Provider Site Verification** – evoBrix provides various real-time APIs to accomplish provider site verification. The API enables the site verification application to perform capture relevant details about a provider's site in real-time during a site visit. It also provides API to track the status of the site visit and alerts the site visit admin when a site visit has been performed and is ready for approval or rejection.

INT02

The Contractor's solution shall support retrieval and presentation of data associated with geographic indicators such as by state, by county, by zip code, by peer group, or other geographical indicators specified by the Agency.

evoBrix PMIS supports the retrieval and presentation of provider data. Using the evoBrix PMIS solution, authorized users can access the robust Provider List feature, an extremely powerful function within the Provider Services business area. Provider List allows the user to search on multiple provider attributes to locate a specific enrolled provider or group of providers sharing a common set of attributes (e.g., zip code and specialty). As shown in Figure 3.10.1-70, the Provider List page has three primary filters and two secondary filters. The secondary filters are Identifier and Indicator. This feature supports the retrieval and presentation of data associated with geographic indicators such as by state, county, zip code, or other geographical indicators. The user has the ability to save favorite search criteria by selecting the Save Filters button. Saved filters are retrieved under the My Filters dropdown. The list retrieved may be exported to Excel for additional analysis using the Save to XLS button.

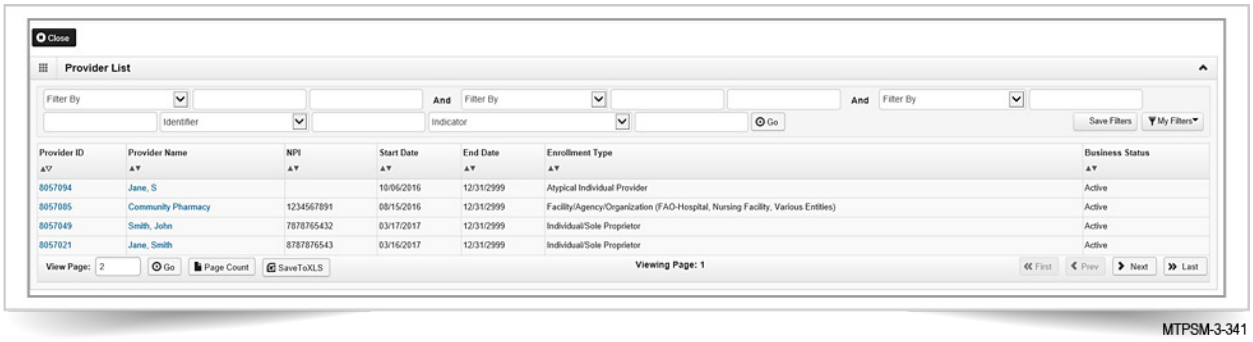


Figure 3.10.1-70. Provider List Page Showing Filter Capability. This screen highlights the three major filters, the secondary filters, the Save Filters and My Filter retrievals, and Save to XLS features.

INT10

The Contractor shall develop operational procedures in coordination with other enterprise module vendors to restore system availability.

Team CNSI's high availability framework is based on ITIL v3 standards and is built for multi-vendor operating environments. Team CNSI will make changes to the existing operational procedures in coordination with other enterprise module vendors in this engagement to reflect the DPHHS operating environment. This framework ensures that cost-effective operational procedures are in place to promote high availability of the system as well as to restore system availability. These procedures are tested on a

regular basis to ensure that the business needs of DPHHS are met. Team CNSI's operational procedures to restore system availability include but are not limited to the following aspects:

- Outage Planning and Coordination
- Communication Procedures
- Escalation Procedures
- Disaster Recovery Planning, Testing, and Execution Procedures

INT15

The Contractor's solution shall use XML standard messaging format to ensure interoperability.

Team CNSI's evoBrix PMIS solution utilizes evoBrix Integrator for supporting all the integration needs of the solution. evoBrix Integrator supports XML as a messaging format to ensure interoperability. The use of Web services supports a standards-based XML data exchange to enable interoperability between the system and other external applications to consume the data and interact with the system. Our architectural approach to interfaces allows interoperability with legacy systems and other SOA-based systems; this infrastructure provides interoperability for evoBrix PMIS and allows transitioning in new services as we replace the existing systems with new technology.

INT22

All service endpoints/APIs shall be exposed to the ESB and are able to receive and submit messages through the ESB.

In alignment with DPHHS technical architecture, our evoBrix platform REST API or SOAP services will be exposed through DPHHS ESB for consumption by relevant trading partners. Team CNSI will expose all the service endpoints/APIs required to integrate with MPATH vendors through our OSB Infrastructure. Team CNSI will provide Interface Control Documents (ICDs) for its services to the MPATH vendor. This infrastructure will aid DPHHS to avoid the use of batch jobs, and allow trading partners to access data on a real-time or near real-time basis, as depicted in Figure 3.10.1-71. Since all service endpoints are exposed to the ESB, the external agencies will be able to receive and submit messages through the ESB.



INT35

The Contractor shall provide an architecture that has clearly defined service endpoints.

Team CNSI's OSB solution includes clearly defined service endpoints that provide information related to various business services. This architecture provides an integration backbone that connects core applications and services without directly accessing underlying systems.

The evoBrix relies on open standards and standard APIs, such as the Java Business Integration (JBI) standard, for pluggability of third-party communities. The evoBrix architecture uses an enterprise class service bus (Oracle Fusion SOA) as the core orchestration tool of business processes across the different applications that support Medicaid operations. evoBrix supports robust authorization, authentication and validation features using Oracle Service Bus. The proposed solution is capable of handling common industry standard service requests such as SOAP and REST. Also, evoBrix has the ability to change the various attributes of the service without impacting existing clients. Our OSB component part of evoBrix

Integrator will allow Core MMIS to avoid point-to-point communication between different system components and will streamline flow of all information throughout the MT PSM implementation.

INT40

The Contractor shall provide technical, functional and performance documentation required by the IV&V Contractor for the solution in order to support IV&V reporting needs identified in the most current version of MECT.

Team CNSI understands the importance of the IV&V Contractor's role in supplying status and evaluation information to CMS in order to achieve Certification for the MT PSM as soon as possible. Team CNSI will provide technical, functional, and performance documentation required by the IV&V vendor in support of certification activities required in the MECT and the Medicaid Enterprise Certification Life Cycle (MECL). Team CNSI has experience in obtaining CMS certification for our solution in state of Michigan and Washington, including the PMIS module. We worked with the states of Michigan, and Washington to support their certification efforts.

Our Certification Leads have experience working with both the MECT and MECL. They will coordinate dissemination of PMIS-related MITA mapping. Our Certification Lead will form a collaborative partnership with the IV&V Contractor to establish the Certification Plan for MT PSM.

INT52

The Contractor shall collaborate with all State enterprise contractors and solutions to accurately collect, process, and distribute applicable HIPAA EDI transactions.

There are no applicable EDI transactions as part of Team CNSI's PMIS solution for the base module.

INT54

The Contractor's solution shall require (when appropriate), capture, and maintain the 10-digit NPI.

The evoBrix PMIS collects, validates and stores the provider's NPI along with the provider demographic information in the Basic Information screen. This is the first step of the enrollment process wizard. NPI is mandatory for all traditional medical providers. The evoBrix PMIS Basic Information screen is shown in Figure 3.10.1-72. For individuals, NPI, SSN, and the demographics information are required as part of this step. NPI is not required for Atypical Individuals. For organizations, NPI, provider's EIN/TIN number and the demographic information is collected. evoBrix checks NPI format, construct and business validations so as to ensure that the NPI that is stored goes through all the necessary validations.

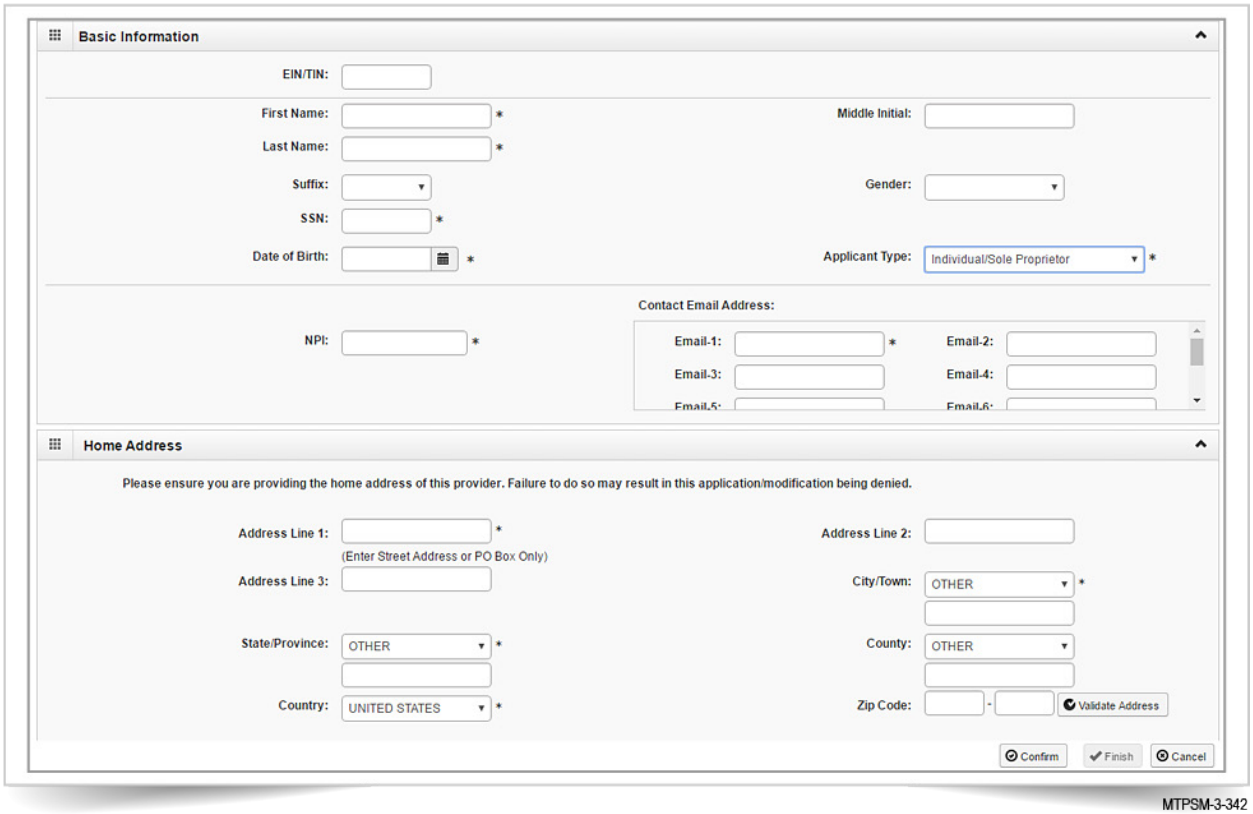


Figure 3.10.1-72. Provider Basic Information. The first step of the enrollment and modification business process wizard collects the NPI information of provider.

INT55

The Contractor's solution, shall accept the NPI in all applicable standard electronic transactions mandated under HIPAA.

The PMIS module stores NPI (billing, rendering, referring, prescribing providers) information based on provider enrollment, the same can be leveraged to validate the information submitted via HIPAA transaction.

There are no applicable EDI transactions as part of Team CNSI's proposed PMIS solution.

INT59

The Contractor shall ensure all hardware, software, and communication components installed for use by State staff are compatible with the State currently supported versions of the Microsoft Operating System, Microsoft Office Suite and Internet Explorer; and current technologies for data interchange.

Team CNSI understands that establishing and managing consistency of hardware, software and communication components across all the State staff computers is key to uninterrupted operations of the system. Team CNSI's ITIL-based Development and Operations (DevOps) approach provides a comprehensive set of practices, policies, procedures, and processes that deliver business value by providing consistent results during operations. Team CNSI will ensure all hardware, software, and

communication components installed for use by State staff are compatible with the State currently supported versions of the Microsoft Operating System, Microsoft Office Suite and Internet Explorer; and current technologies for data interchange. Team CNSI will establish the standard client access components based on the State supported versions. This will be documented in our design deliverables during the solution and configure phases. The standards will be utilized to build the test lab for our QA team to test and certify our deliverables.

INT60

Unless otherwise mutually agreed to in writing, the Contractor must maintain any and all hardware and software products required to support the Contractor's solution at their most current major version (patches, fixes, upgrades, and releases for all software, firmware and operating systems) or no more than one version back from the most current major version.

Team CNSI has developed an extensive operational system and support infrastructure comprised of well-documented processes and procedures. Team CNSI's approach is built on an ITIL framework augmented by our own best practices refined over years of collective health care administration operations experience in managing large, complex projects of similar size and complexity. A key part of aligning with ITIL involves designing processes or "services" so changes are introduced into an operations environment in a controlled and systematic manner. Changes to hardware configuration items (such as a major hardware upgrade, which includes upgrading firmware or major release levels of the operating system), software versions, and communication components often result in a bigger impact on the associated COTS software products running on it and the version of the evoBrix application running on top of it. Such changes are typically rolled out in a major release schedule after through testing and certification. Team CNSI will maintain any and all hardware and software products required to support our solution at their most current major version or no more than one version back from the most current major version. The versions for initial production will be decided during the Solution and Configure phase and documented in the DSDD. Time critical security related releases for patches, and fixes for all software, firmware and operating systems will be conducted as per our operational procedures. Once in production, any major version upgrade or change will go through a Change Management Process and go through a full release cycle that will include impact analysis, complete regression testing, and verification before promotion to production.

INT61

The Contractor's solution shall allow internal and external stakeholders to upload and view electronically submitted documents.

The evoBrix PMIS solution offers provider/State staff users an easy-to-use interface to conduct secure upload and retrieval of their electronically submitted documents. The module seamlessly integrates with the FileNet content management solution by IBM, which is Team CNSI's Document Management System (DMS). FileNet provides advanced document management features and technology frameworks that meet DPHHS requirements. FileNet will be the single repository for all system documents and provider support materials.

Providers can upload documentation in support of their enrollment application, such as a copy of their license and of any certifications. State staff can also upload documentation on behalf of the providers. When the user(s) invoke the upload functionality, the evoBrix PMIS internally calls the FileNet API to archive the uploaded document within DMS and index the document based on pre-configured parameters,

to aid in document retrieval later. Please refer to section 3.10.1.8 Enterprise Content Management for further details about the Document Management capabilities of the solution.

Any uploaded documents can later be viewed through PMIS self-service portal, it also provides rich filter capability that eases and narrow down on searches performed. The self-service portal's Document Archive List is shown in Figure 3.10.1-73.



Figure 3.10.1-73. Document Archive List. This page retrieves a list of documents that have been uploaded to the Document Management System.

INT62

The Contractor's solution shall ensure information and event notifications include aggregated and integrated information.

evoBrix Notification framework provides a consistent approach to all the notification needs of the system. Notifications from all the system events are accessible via the online screen "My Inbox." The users can view their notification items in the list page in evoBrix PMIS and act upon the task. Figure 3.10.1-74 shows the provider enrollment and modification event notifications. The framework ensures that all information and event notifications include aggregated and integrated information and are consistent across evoBrix PMIS.

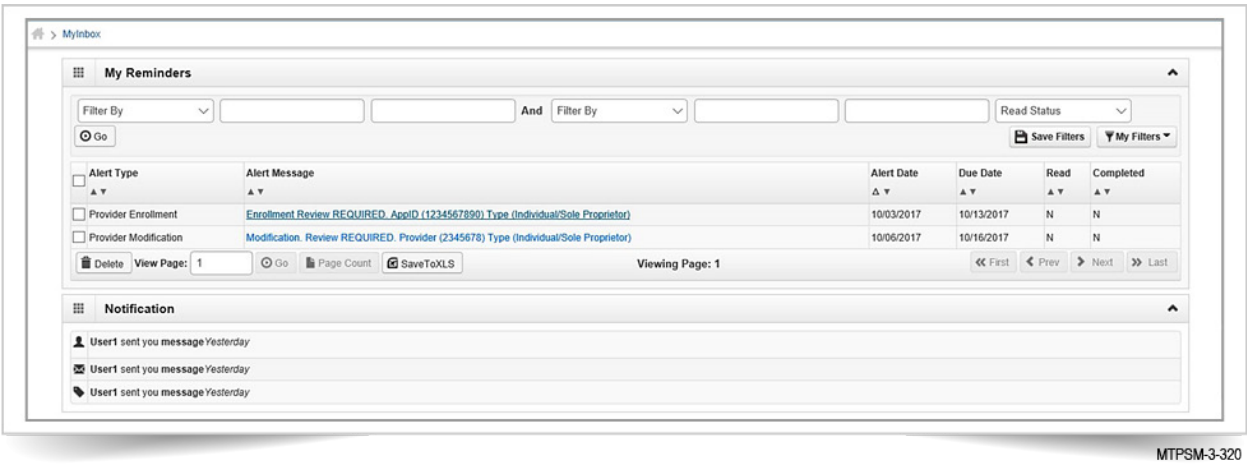


Figure 3.10.1-74. evoBrix My InBox Screen. evoBrix Notification framework ensures that information and event notification are consistent across the system.

INT63

The Contractor's solution shall have business process orchestration in an event-driven environment that maximizes process automation.

Team CNSI's evoBrix PMIS solution includes a configurable workflow process that provides the flexibility to define State-specific business processes. The integrated workflow management solution provides improved automation, reduced manual intervention, configurable work routing, and task management. This proven workflow solution comes with table-driven configurable rules, task routing, assignment, and tracking capabilities. The solution will maximize process automation by enabling orchestration of business processes with event-driven capabilities. Refer to section 3.10.1.9 Workflow for more detailed information about our solution's workflow capabilities.

INT65

The system shall provide the ability to share and federate data with other data sharing partners.

Data Sharing and exchange is the primary function of the evoBrix Integrator component. Team CNSI's evoBrix Integrator will support automated data exchanges with various Medicaid business process areas and interface partners. CNSI's evoBrix Interface Service Repository (ISR) component within evoBrix Integrator architecture uses an enterprise-class service bus (Oracle SOA Suite) as the core orchestration tool of business processes across the different applications that support Medicaid operations. The Infrastructure includes a variety of services to support connections between disparate systems and utilizes the ESB as its underlying messaging infrastructure. It also encompasses a wide range of transports. This facilitates distribution of information across-platforms within the Medicaid enterprise quickly and easily.

Team CNSI's evoBrix ISR framework will be used to interface with State agencies and all approved trading partners. It offers a robust and comprehensive framework to interface with all state-approved Trading partners and federal provider related data sources using a secure connection to facilitate business functions to meet the requirements of department policy, and federal/state rules and regulations. The evoBrix ISR solution that supports scheduling, audit, error logging, and escalation features along with detailed reporting on interface execution status, combined with notification modules to track execution of the various interface transactions thus ensuring processing of MT PSM interfaces within timeframes. The evoBrix ISR solution was built for scalability by design with a multitude of adaptors to connect with a variety of platforms. The Message infrastructure provides location transparency and the automated routing of messages to the target services, which makes distribution of information across platforms easy; this infrastructure will streamline the ability to share and federate data with other data sharing partners. Team CNSI's ISR framework is illustrated in Figure 3.10.1-75.



INT66

The Contractor's solution shall provide the ability to create/edit, send, receive and process X12, NIEM standardized transactions and NCPDP D.0 transactions relative to the Contractor's scope of work.

The base scope of work does not include any applicable X12, NIEM, and NCPDP D.0 standardized transactions. Our solution does provide that ability and does include applicable transitions of that sort in Option A.

INT68

The Contractor shall collaborate with the Systems Integrator to automatically report system availability to the SI availability solution. The frequency of each module component verification will be defined by the Department.

Team CNSI's proposed solution offers essential services to Medicaid members and providers. A disruption to its operations can adversely affect that community along with DPHHS and other stakeholders. Therefore, it is critical to ensure continuous access and create a highly available infrastructure to support the business operations of the system and to ensure that service levels are being met. To meet these needs our solution includes HealthBeat, which provides DPHHS with configurable, automated, and real-time visibility into business operations, SLA compliance, and system monitoring.

There are three key components at the center of healthy operations that our operations staff monitor to ensure continuous operations and prevent disruption, as follows:

- Measures are designed to track effectiveness of business operations (i.e., hold time for calls at the contact center or first-time closure success rate for calls)
- Application operations and health, which are measures that track performance of the application in performing the tasks it was built for (e.g., number of active users and providers in the system and prior authorization approval rates)
- Infrastructure, which is made up of the hardware and software components that form the backbone of the system and support the application and business operations (e.g., the servers, the network)

Monitoring and Reporting System Availability

Team CNSI's proposed solution includes a comprehensive and complete system monitoring and reporting framework that will automatically report system availability to the SI availability solution. This framework ensures that the high-availability components are working properly across the system and provides monitoring and reporting capabilities covering all layers of hardware and software components.

The following reporting capabilities are available to automatically report system availability to the Systems Integrator's availability solution

- Reports
- Dashboards
- Charts
- Kiosk
- Notification Alerts and Emails

The classification of monitoring tools and their respective modules is specified in Figure 3.10.1-76.

Monitoring Tool	Monitoring Area	Infrastructure Modules
SLA Automation Tool	SLA Management	Application Interfaces/Web Services Servers
HealthBeat	Business Operations Monitoring	Application Interfaces/Web Services Servers
Oracle Enterprise Manager	Databases and Infrastructure Monitoring	Databases and Database Servers SOA Suite Application Servers
Building Management System	Data Center Monitoring	Data Center Power and Cooling
Data Center Infrastructure Management	Data Center Monitoring	Infrastructure

Figure 3.10.1-76. Monitoring and System Performance Reporting Tools. This classification of monitoring tools and their associated infrastructure modules forms the backbone of the monitoring framework.

SLA Automation Tool and Operational Performance Standards

Team CNSI's SLA automation solution provides DPHHS with configurable SLA management capabilities. It is one of the tools that allow Team CNSI and DPHHS to track and ensure that SLAs are being met. Figure 3.10.1-77 shows the SLA automation tool architecture. Our solution uses an SLA Automation Engine which is configured to automatically or manually track various SLAs related to system and business functions, such as interfaces and report generations. Our solution allows Team CNSI to have visibility of daily system and business functions and their corresponding SLAs performances. The tool is also equipped with tracking, reporting, and management capabilities using Team CNSI's HealthBeat as the front-end application. For example, the tool allows Team CNSI to measure SLAs on Interfaces processing. This visibility allows Team CNSI the necessary visibility to monitor performance and provide SLA course correction when necessary.



The SLA Automation engine runs on a configurable interval to generate service transactions based on the configured SLA's frequency schedule. The system retrieves data input from various source systems via REST or SOAP web service requests for multiple service configurations at any given time. The retrieved data – such as process start/end times and status codes – is matched to the SLA transaction based on unique criteria linked with the reference number, and automatically updated with the provided data. In the

event of a non-compliant transaction, notification alert emails are generated and sent to email addresses linked to that service configuration.

Business Operations Monitoring

Indicative of Team CNSI's commitment to service and transparency, we are including HealthBeat, which provides DPHHS with configurable, automated, and real-time visibility into business operations, SLA compliance, and system monitoring. This section provides an overview of HealthBeat's business operations monitoring. HealthBeat for system monitoring is covered in detail in Section B2.4.1.2, Availability Management, subsection Monitoring and Reporting High-Availability.

HealthBeat enables the setup of a hierarchy of MITA business, system, and application objectives or goals that can be linked with metrics to events and services. This will allow Team CNSI and the states using evoBrix to monitor the health of business and system processes not only in the short term but also over the long term to track historical trends. Such an approach allows Team CNSI to use real-life data in the business process configuration and ensures continuous business process improvement across all business process areas.

HealthBeat, upon contract award, comes configured with most of the SLAs identified in the Solicitation. We say most of the SLAs since many SLAs by their nature are not candidates for real-time monitoring (i.e., deliverable submissions). Currently, HealthBeat contains provider related metrics and is continuously evolving to provide meaningful metrics to business operations users. Figure 3.10.1-78 shows the HealthBeat SLA history view.

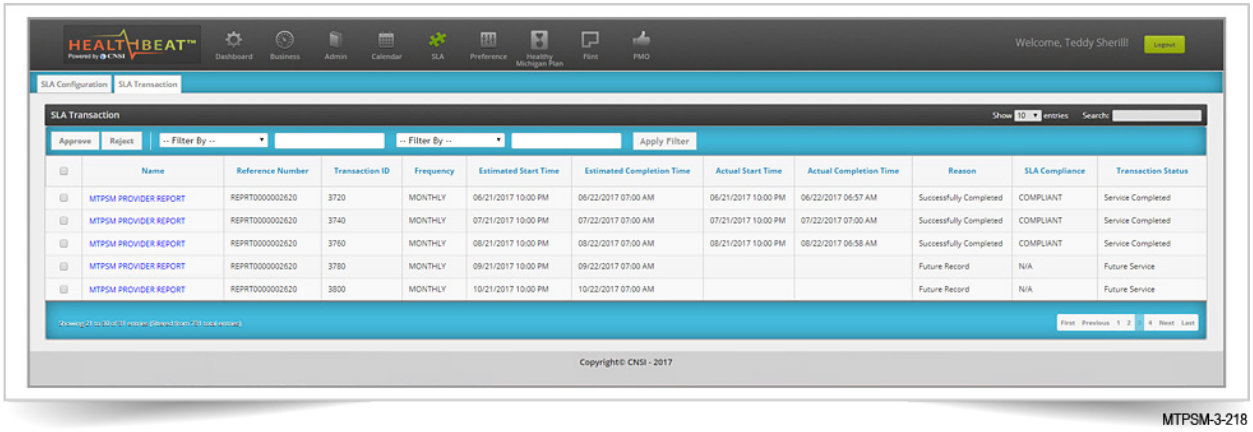


Figure 3.10.1-78. SLA History View in HealthBeat. HealthBeat provides SLA configuration, management, and monitoring capabilities for transparency of operations.

HealthBeat provides a comprehensive application activity monitoring framework along with the capability to facilitate continuous process improvement. As the system handles each process, it collects process-related data in the data store. This data is then used to display the process dashboard and provide visibility to the process metrics and the health of the operation. The system uses workflow-based analytics to provide feedback on potential bottlenecks and application performance issues. Thresholds are configured to display performance in the traditional "red," "yellow," and "green" dashboard status. Team CNSI operations staff sets appropriate thresholds during service design.

Related to system monitoring, HealthBeat reports accurate data on items such as end-user response time, CPU utilization, and hourly load averages on different servers. This allows Team CNSI to see the system from a higher point of view and help make informed, strategic decisions on daily operations or future

changes in policy and programs. Application management and monitoring, web services management, systems management and monitoring, network management and monitoring, performance monitoring, and event monitoring are all managed via the framework of HealthBeat. Figure 3.10.1-79 shows how HealthBeat monitors system resources of real application clustered (RAC) databases.

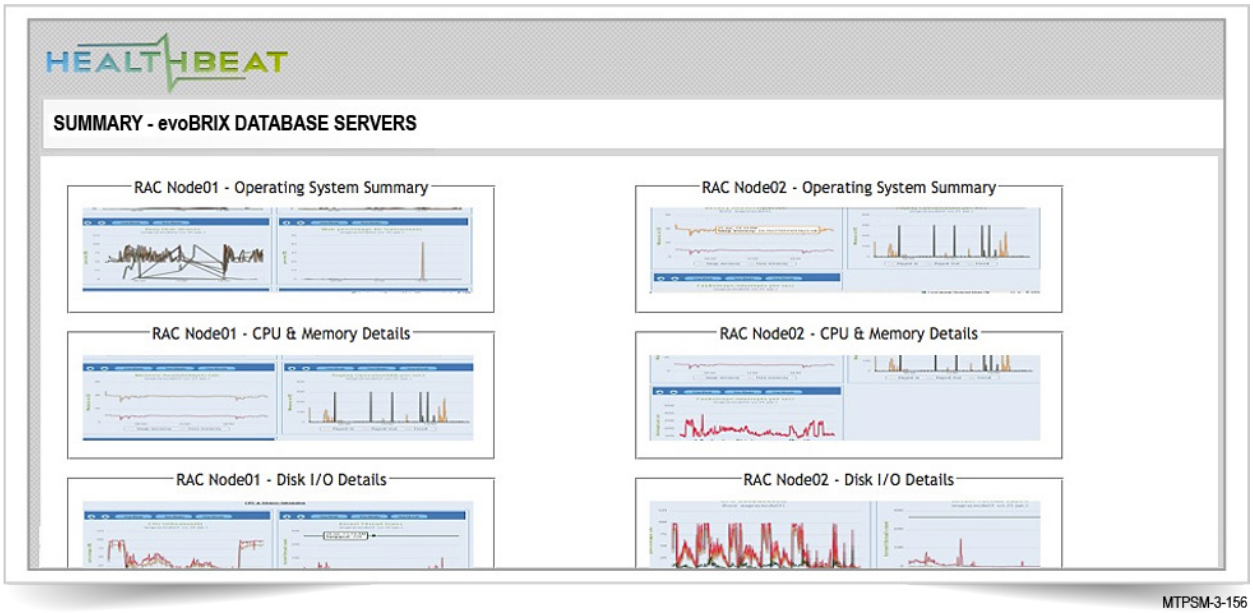


Figure 3.10.1-79. HealthBeat for System Monitoring. Monitoring of clustered databases.

HealthBeat also provides various reporting mechanisms, including dashboards and graphs that can be used to report on the metrics associated with performance standards. Team CNSI uses the HealthBeat tool to collect and report on final performance measures and standards. HealthBeat uses automation to extract, analyze, and report data from various business processes and systems, and to provide a centralized reporting database. This tool provides a robust interface to the various components for gathering and compiling data, allowing near-real-time access to workload and system performance information.

Operational management staff regularly monitor data displayed through the dashboard and can proactively respond if performance indicators begin to decline. In this way, Team CNSI can implement corrective actions before a “red flag” situation occurs. In addition, email alerts are established to notify appropriate Team CNSI and State staff based on configured exception thresholds. Team CNSI also compiles information collected through HealthBeat and summarizes it in our regular reporting mechanisms, including statuses and required workload reports.

The tool produces visualizations of data in various formats, including dashboards and graphs that provide quick summaries for trending. Figure 3.10.1-80 shows the HealthBeat architecture that is configurable and automated.

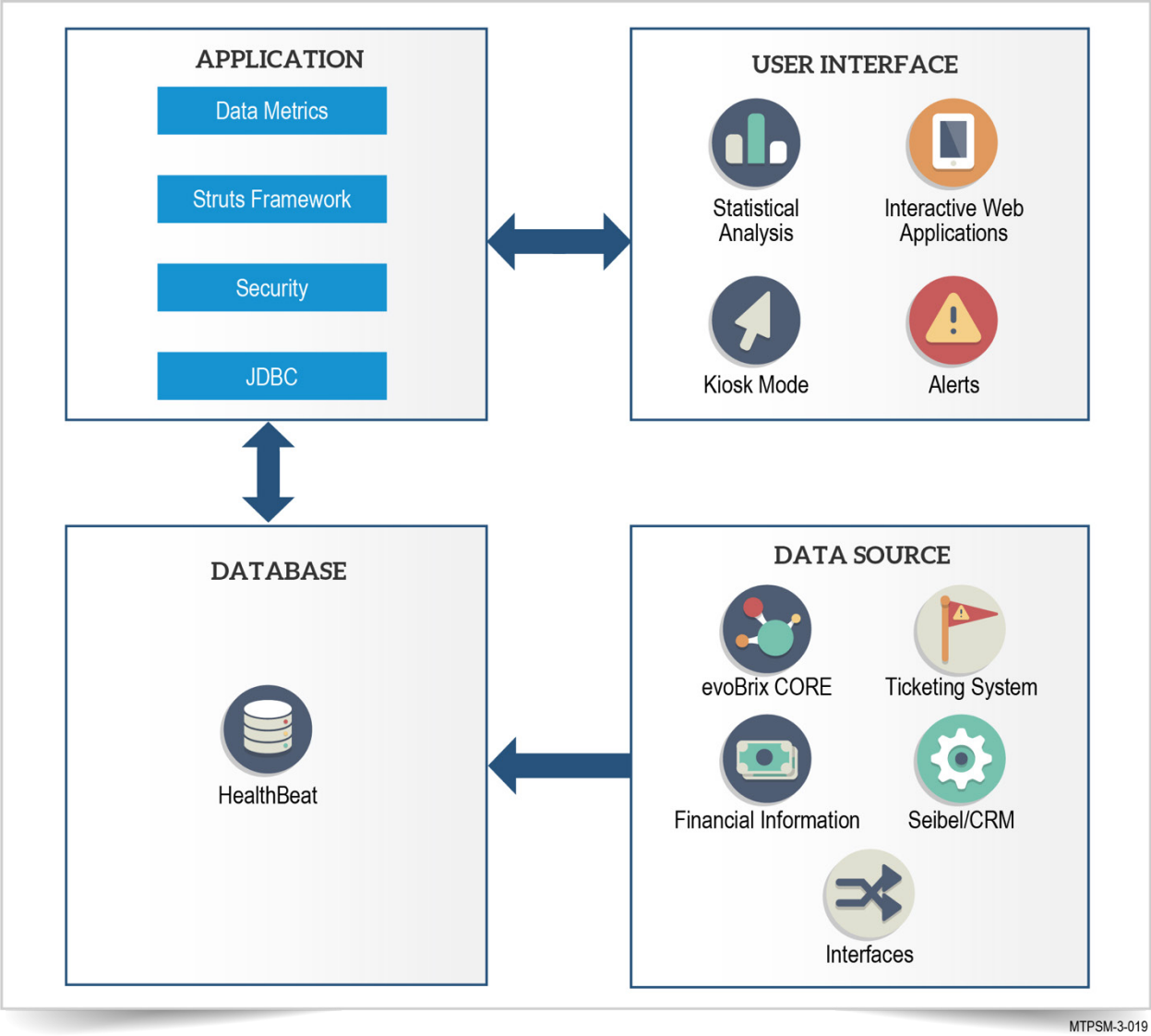


Figure 3.10.1-80. HealthBeat Architecture. Provides DPHHS with configurable, automated, real-time visibility into business operations.

Oracle Enterprise Manager

Team CNSI's database administrators and system administrators rely on OEM to maintain, monitor, and configure proactive alerts for Oracle databases, SOA Suite, and Application Servers. Oracle Management Service (OMS) monitors various targets and collects the performance metrics. These metrics are then uploaded to the Repository through a Java Database Connectivity (JDBC) API. The OEM Console and Enterprise Manager Command Line Interface (EMCLI) enables administrators to access and manage OEM functionalities, which in turn sends notifications and alerts to the NOC. The NOC triages issues to the appropriate operations team for corrective action. Team CNSI's proactive monitoring enables us to predict when issues may arise in the future. By monitoring trending data, we can determine whether a system is likely to have issues. For example, if we see that a system is spiking on CPU usage and memory on a regular basis, that system may require a hardware upgrade or optimization to remove capacity concerns.

Figure 3.10.1-81 shows the OEM architecture. Various alerts are configured in OEM to issue immediate notifications as soon as an issue occurs. Alerts are sent to the necessary teams and a NOC team that monitors the system 24x7x365 and communicates the same to the respective teams. Figure 3.10.1-82 shows the OEM database load map that shows the health of all the registered clustered databases in a single pane of view.

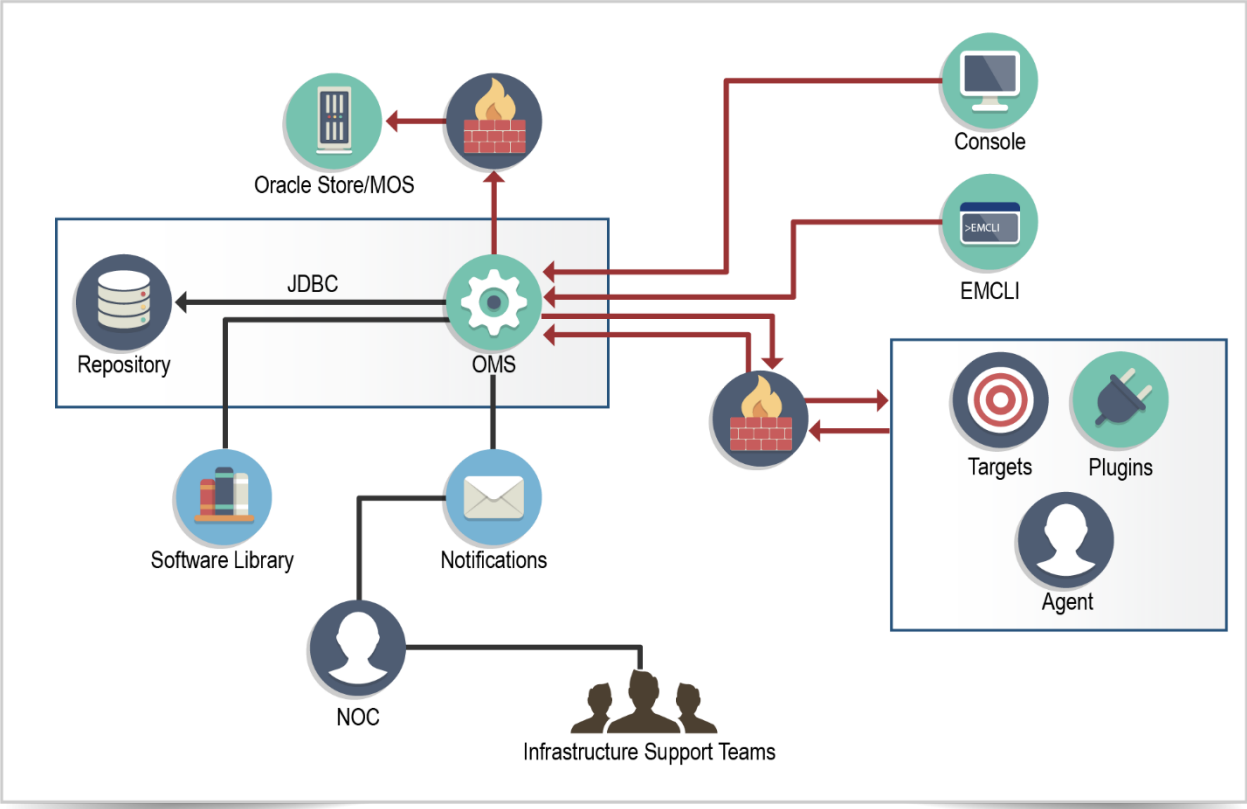


Figure 3.10.1-81. OEM Architecture. OEM monitors the availability and performance of the database and application servers and alerts the necessary teams.

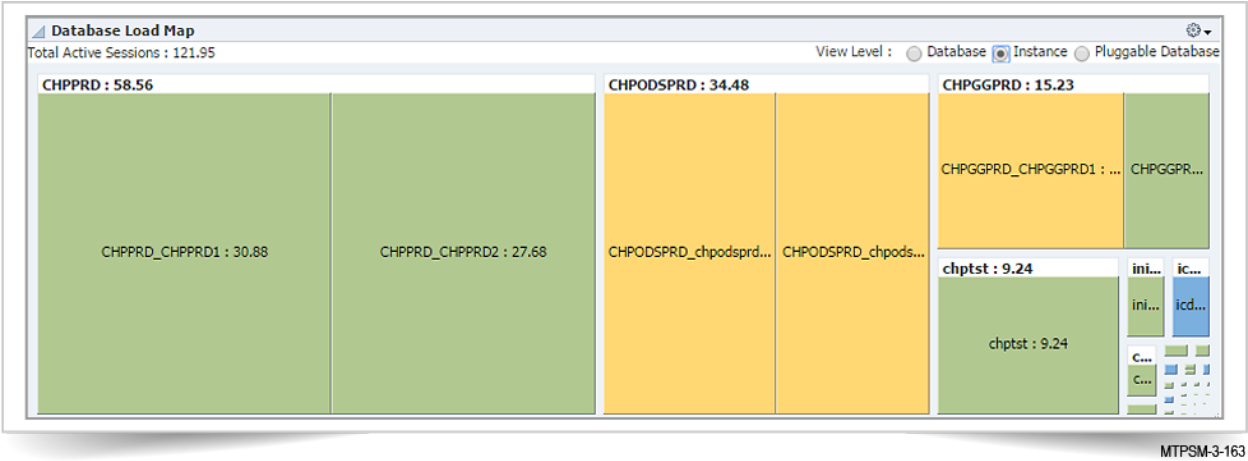


Figure 3.10.1-82. OEM Database Load Map. Shows the health of all the registered clustered databases in a single pane of view.

Building Management System and Data Center Infrastructure Management

Building Management System (BMS) alerts critical facilities staff and engineers of any issues. Depending upon priority, a ticket is executed and staff resolve or assign vendors for ticket completion and issue resolution. The BMS handles monitoring of power and cooling.

Data Center Infrastructure Management (DCIM) monitors all environmental systems (e.g., temperature, humidity, power usage, leakage, efficiencies of equipment and systems). Additionally, DCIM monitors all video and door access surveillance from a central NOC, staffed 24x7x365. Together, BMS and DCIM help to monitor and report any loss in high-availability functionalities across hardware and software components in the data center layer.

INT70

The Contractor shall identify and describe the licenses necessary for the scope of work to support the infrastructure that will provide sufficient bandwidth and redundancy to ensure accessibility, reliability/fault tolerance and acceptable performance.

Team CNSI's proposed solution is based on a highly available and redundant system, designed to support mission-critical applications. The system has fault tolerance and accessibility capabilities built at various layers. Team CNSI's high-availability architecture includes the following infrastructure components along with the licenses required to support the high-availability architecture, as shown in Figure 3.10.1-83.

Infrastructure Type	Feature	Solution	License Type
Database	Accessibility, Fault Tolerance	Real Application Clusters	Oracle Database Cloud Services
Storage	Fault Tolerance	Automatic Storage Management	Oracle Database Cloud Services
Application Server	Accessibility, Fault Tolerance	WebLogic Cluster	Oracle Java Cloud Service
Load Balancer	Accessibility, Fault Tolerance	Oracle Traffic Director	Oracle Traffic Director
Physical Host	Fault Tolerance	Oracle Compute	Oracle Compute
Standby Database	Reliability, Fault Tolerance	Oracle Data Guard	Oracle Database Cloud Services
Backups	Reliability, Fault Tolerance	Recovery Manager (RMAN)	Oracle Database Cloud Services
Network	Performance	Oracle Fast Connect VPN 1g/10g	Oracle Fast Connect VPN 1g/10g

Figure 3.10.1-83. Team CNSI's High-availability Architecture. Components and licenses required to support the high-availability architecture.

Figure 3.10.1-84 depicts the high-level availability architecture covering clustering at the application server and database server level, as well as web server load balancing.

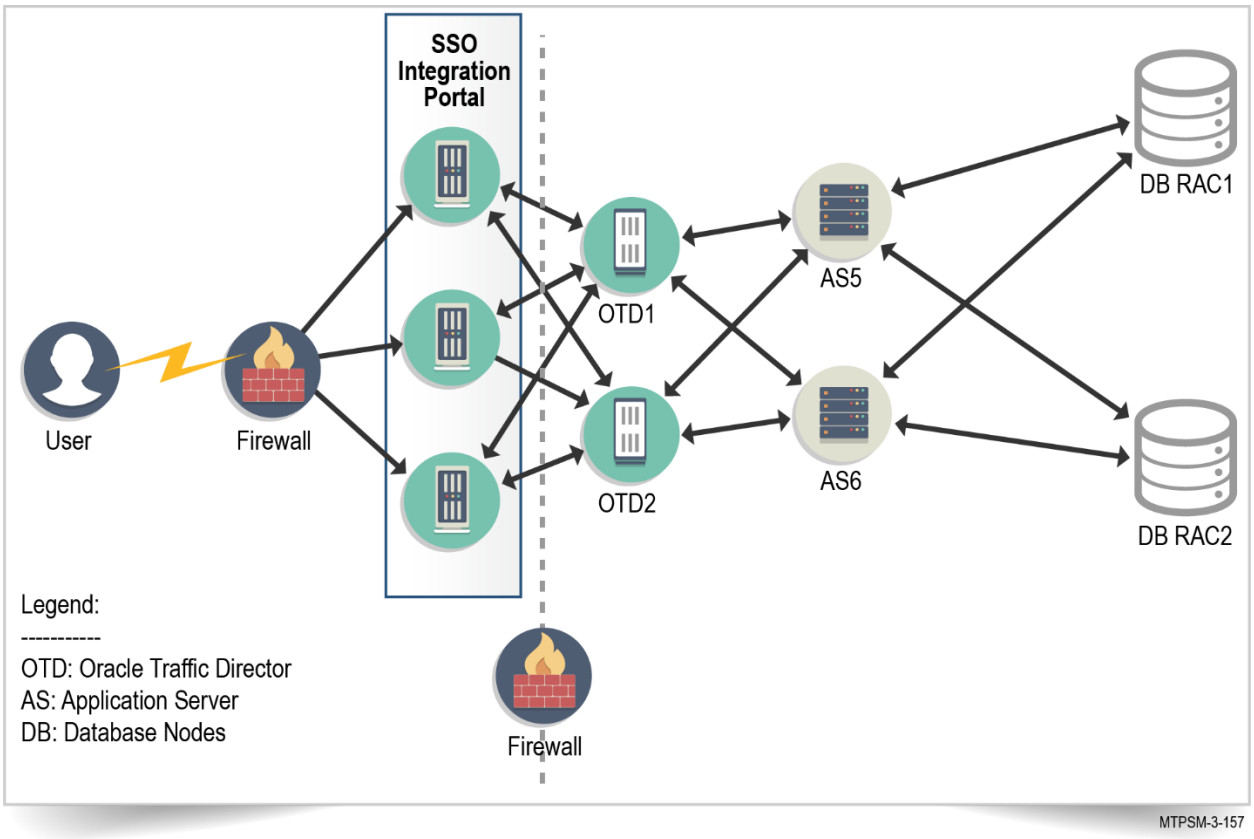


Figure 3.10.1-84. High Availability Architecture. Clustered architecture at the application server level and database server level provides load balancing and high availability capabilities.

INT73

The Contractor shall be responsible for understanding the business processes to automate and orchestrate appropriate workflows, business rules, data flow and metadata within the solution and work collaboratively with the SI.

Team CNSI will work collaboratively with the State and the SI to understand the business processes that need to be automated as part of this implementation. This analysis will be done during solutioning phase of the project. The business processes will be captured in the Detailed System Design Document (DSDD) and include details of the workflows that need to be orchestrated along with the related business rules, data flow and metadata. The State approved DSDD will contain all the understandings and act as the scope of work for building and orchestrating Workflows in the solution.

INT74

The Contractor's solution shall have the ability to identify errors in transactions and immediately notify the source system of the specific errors including whether the errors have precluded loading and/or using the data.

Team CNSI's evoBrix platform provides the ability to intake or ingest externally sourced data relevant to the functioning of MT PSM business operations via evoBrix ISR solution as illustrated in Figure 3.10.1-

75. The ISR solution integrates with external systems via MT PSM System Integration Services. Data exchange and file transmission is handled by ISR in a secure manner with external entities using secure file transfer protocol (SFTP), FTPS or SSL. The solution validates and process the files in near real time or in batches on a scheduled basis. Any error records during the process get loaded into ISR error tables. Audit information is stored in ISR tables to track the transaction from start to end. In similar way, auditing and error handling is performed for real time webservices where we log complete requests and responses, giving complete visibility within the system and capturing services errors in error log tables. The evoBrix ISR solution finally sends the email to the external entities and notifies them of the status of the transaction, in addition to providing audit and error information. Team CNSI's reporting solution generates multiple scheduled and ad hoc custom reports based on MT PSM monitoring requirement, and error information will be sent in the reports.

INT78

The Contractor shall provide an environment where components can be added or replaced quickly.

Team CNSI's private cloud will be hosted in the Oracle Government Cloud, which is both FedRAMP and HIPAA compliant. These data centers utilize a robust and redundant infrastructure architecture coupled with elastic capabilities. This cloud platform is highly flexible wherein Components can be added or replaced quickly.

There are two ways by which expansion happens in Team CNSI's private cloud:

Horizontal Expansion – Cloud Services

Team CNSI's hosting platform allows IT resources (infrastructure components), that are of the same type to be added or removed quickly. This flexibility is because all infrastructure components are either built using Platform as a Service (PaaS) services, Infrastructure as a Service (IaaS) services, or SaaS services, thereby creating a highly flexible and elastic environment. Additional PaaS or IaaS services in Team CNSI's private cloud can be subscribed to or cancelled, on an ad hoc basis, using the "Pay as you go" subscription model. The classification of Infrastructure components and its equivalent Cloud Services is specified in Figure 3.10.1-85.

Infrastructure Components	Cloud Service Type	Cloud Service
Database	PaaS	Oracle Database Cloud Service (DBCS)
Virtual Machines (VM)	PaaS	Oracle Compute Classic Cloud Service
Application Server	PaaS	Oracle Java Cloud Service (JCS)
Integration Platform	PaaS	Oracle Service Oriented Architecture Cloud Service (SOA CS)
Storage	PaaS	Oracle Cloud Block Storage
Backup Storage	PaaS	Oracle Cloud Object Storage
Backup Service	PaaS	Oracle Cloud Backup Service
Provider Screening	SaaS	Lexis Nexis Screening
Provider Fee Collection	SaaS	First Data Fee Collection Service

Figure 3.10.1-85. Infrastructure components and its equivalent Cloud Services. This classification maps how each infrastructure component is subscribed as IaaS, PaaS, or SaaS services.

For example, if DPHHS has a requirement to install and configure a security or compliance tool for a short period of time:

- Team CNSI creates a new VM with a specific number of cores using the IaaS Service – "Oracle Compute Classic Cloud Service"
- Allocates the necessary SAN space for the VM, that was created earlier, using the Oracle Cloud Block Storage IaaS Service
- The VM is then backed up regularly using Oracle Cloud Backup Service and the backups are stored using Oracle Cloud's Object Storage Service
- All the above services are billed using "Pay as you go" subscription model on an hourly basis
- Once the security or compliance task is over, the above services are then cancelled.

Vertical Expansion – Cloud Bursting

Team CNSI's hosting platform also supports cloud bursting and it is cost effective. It permits additional capacity usage at a metered rate, when the demand for computing capacity spikes. Any additional capacity used is charged on an hourly basis and billed monthly in arrears ("Pay as You Go" model).

For example, if the current database server has four cores allocated and you are running a monthly job that requires additional computing power, then the cloud bursting feature will add additional cores to the database server, to meet the additional demand. This additional capacity used is charged on an hourly basis and billed monthly in arrears ("Pay as You Go" model).

INT79

The Contractor's solution shall allow internal and external users to enter data using electronic forms and receive documents electronically from other systems.

The evoBrix PMIS solution provides State staff and providers with a full range of online, real-time inquiry and update functions through web-based data entry screens. The solution maximizes the opportunity to collect valid and complete information throughout the provider's association with DPHHS. The module provides a browser-based and interactive system supporting the day-to-day business needs of the providers and DPHHS user communities. The evoBrix PMIS provides an interactive enrollment application that comes with structured, online screens driven by the enrollment Business Process Wizard (BPW).

The evoBrix PMIS solution highlights are listed below:

- Configure enrollment process workflow per state-defined criteria
- Accept electronic forms, supporting documents/attachments
- Perform enrollment process electronically

Team CNSI's evoBrix ISR configurable solution supports automated data exchanges between MT DPHHS and other systems.

INT80

The Contractor's solution will interface with the State's designated financial processing solution.

Team CNSI's evoBrix Integration framework will be utilized to interface with MT DPHHS designated financial services entities. Team CNSI's integration framework is comprised of the below components to integrate the systems with other information systems including MT DPHHS financial processing sources.

- Batch Interfaces via ISR
- Web services via evoBrix integrator

Batch Interfaces via ISR

Team CNSI's evoBrix ISR configurable solution supports automated data exchanges between MT DPHHS and the approved agencies including financial sources. The evoBrix ISR solution uses an enterprise class service bus (Oracle SOA Suite) as the core orchestration tool of business processes across the different applications that support Medicaid operations. The framework supports inbound, outbound interfaces and pass-through data exchange within evoBrix and with interface partners. The ISR solution supports secure data exchanges using available standards in the industry such as SFTP, FTPS, and SSL.

Web Services via evoBrix integrator

The evoBrix integrator solution leverages Oracle Service Bus for Service mediation for real-time web services. It supports robust authorization, authentication, and validation features using Oracle Service Bus. The solution is capable of handling common industry standard service requests such as SOAP and REST. Also, evoBrix integrator has the ability to change the various attributes of the service without impacting existing clients. The solution will allow MT PSM to avoid point-to-point communication between different system components and will streamline flow of all information throughout the MPATH Medicaid enterprise.

INT81

The Contractor's solution shall have the capability to receive and display data, messages, and alerts from other systems in real-time.

Team CNSI ISR solution supports real-time data trading of interfaces based on the business/operations need between state approved trading partners. Team CNSI's evoBrix ISR solution supports Data trading in near real-time via evoBrix OSB web services. The evoBrix architecture uses an enterprise class service bus (Oracle Fusion SOA) as the core orchestration tool of business processes across the different applications that support Medicaid operations. Team CNSI's evoBrix Integrator's configurable ISR solution can handle MT PSM integration for transmittal of data for different systems to align with the conceptual solution architecture. This solution provides an integration backbone that connects core applications and services without directly accessing the underlying systems. evoBrix supports robust authorization, authentication, and validation features using Oracle Service Bus. The solution is capable of handling common industry standard service requests such as SOAP and REST. Also, evoBrix can change the various attributes of the service without impacting existing clients. This infrastructure provides the capabilities to receive and display data, messages, and alerts from other systems in near real-time.

INT85

The Contractor's solution shall support web services, specifications, and adapters (e.g., ODBC, Web Service (WSDL, WS-*, SOAP, REST, UDDI, ODATA), JSON-WDP, MS SQL, SQL Server, Oracle, FTPS, SFTP, HTTPS, MSMQ).

Part of the evoBrix Integrator, the Oracle SOA tool provides an industry standard service orchestration framework using BPEL based process orchestration capabilities. evoBrix Integrator supports integration capability through web services and adaptors for connectivity as an out-of-the-box feature. Oracle SOA supports all the web service standards and security standards such as WSDL, WS-*, SOAP, REST, UDDI, and ODATA. The tool has adapters to connect with MS SQL, SQL Server, Oracle and other databases. Also, the tool provides adapters for FTP, FTPS, SFTP, HTTPS, and MSMQ. Payloads from XML, COBOL VSAM, and JSON are also supported.

INT86

The Contractor's solution must be capable of receiving, translating, and processing data to and from the variety of protocols (e.g., FTP, FTPs, SFTP, HTTP, HTTPS, JMS, JDBC, ODBC, NET, AS2, AS3, POP3, SMTP, SSH, TCP, CICS). The Contractor shall include in their response a list of protocols supported.

Team CNSI's evoBrix PMIS utilizes evoBrix Integrator for supporting all the integration needs of the solution. evoBrix Integrator supports out-of-the-box integration capabilities for receiving, translating, and processing data to and from the variety of protocols such as FTP, FTPs, SFTP, HTTP, HTTPS, JMS, JDBC, AS2, AS3, POP3, SMTP, SSH, TCP/IP, and CICS. These are available as standard integration adapters in the Oracle Fusion SOA which is part of the evoBrix Integrator.

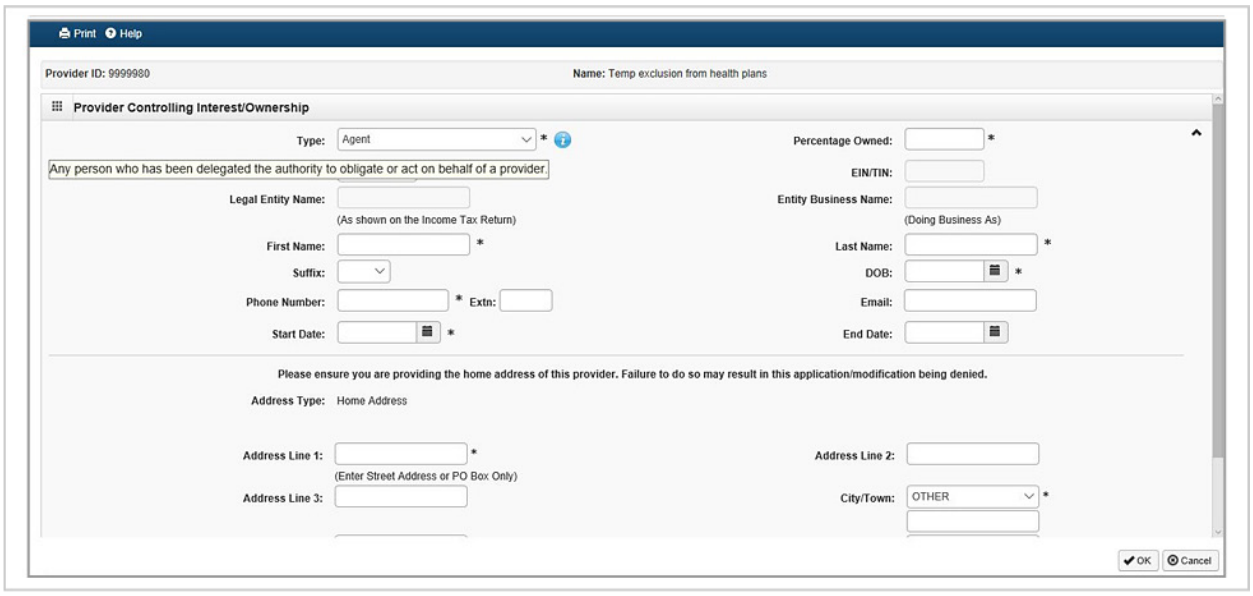
As part of Transport and Exchange Management, Oracle SOA enables secure and reliable messaging by supporting numerous transports and messaging services. Within each standard the user can define the protocol, transport parameters, channel attributes, exchange parameters, and security requirements.

- **Transports**: Oracle AQ, JMS, File, FTP, FTPs, sFTP, HTTP, HTTPs, SMTP, IMAP, POP3, TCP/IP
- **Messaging Services**: AS1, AS2, ebMS, RNIF

INT87

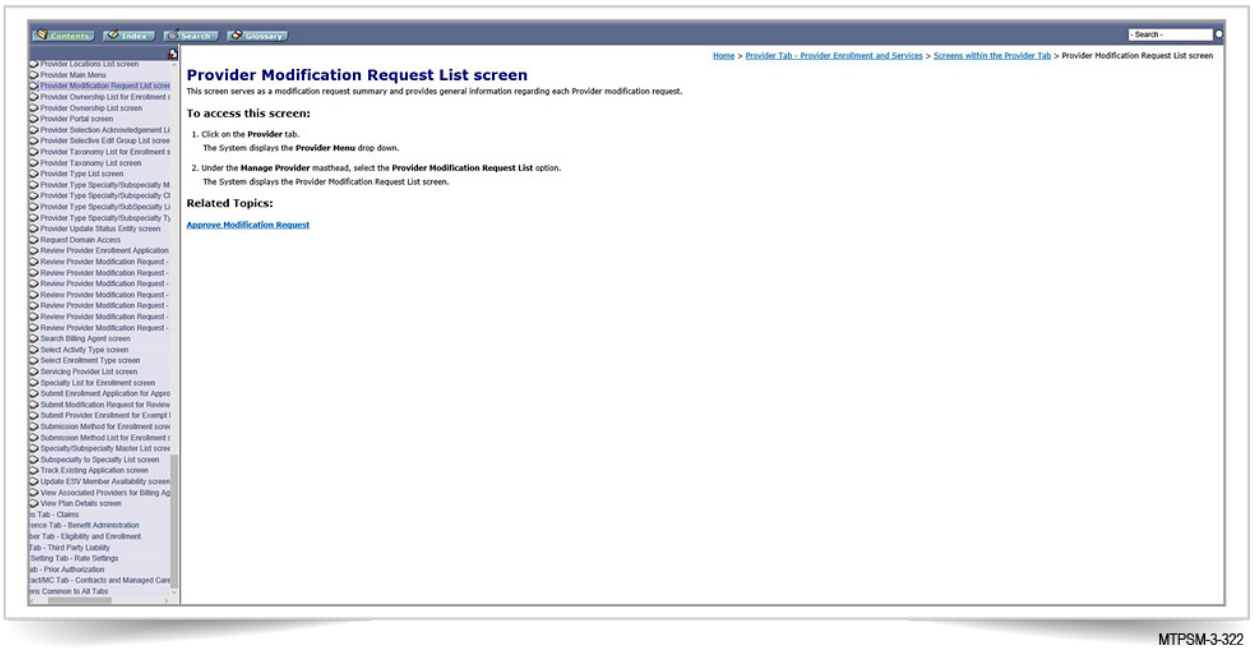
The Contractor's solution shall provide context sensitive help (situational clarification and support associated with process specific steps), to support user activities (e.g., provider enrollment and maintenance activities).

The evoBrix PMIS solution comes with a robust set of online user guides, and context-sensitive help for each screen. We also have developed a set of system administration procedures which acts as a useful aid for operational staff. Figure 3.10.1-86, Figure 3.10.1-87, and Figure 3.10.1-88 show the context sensitive help screen for provider enrollment and maintenance activities. Besides the training and other user guides, the context sensitive help provides a quick reference and easy reference for user to perform activities such as provider enrollment and provider maintenance.



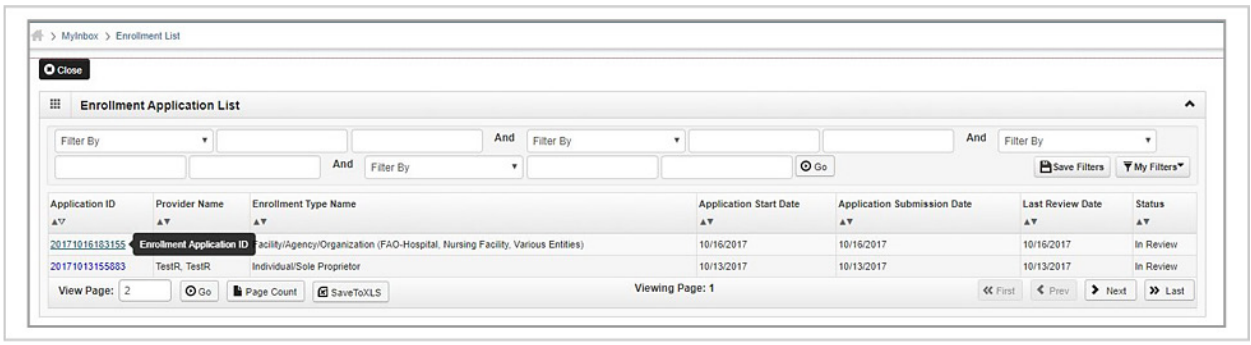
MTPSM-3-396

Figure 3.10.1-86. Ownership Type Clarification. User-friendly situational clarification on different types of ownership during provider enrollment process.



MTPSM-3-322

Figure 3.10.1-87. Provider Modification Help Context. User-friendly help for Enrollment and Maintenance screen.



MTPSM-3-391

Figure 3.10.1-88. Provider List Navigation Help. User-friendly help for navigation and action performed on Enrollment and Maintenance screen.

INT88

The Contractor shall implement a solution where module components are loosely coupled and can be added or replaced quickly.

One of evoBrix's inherent strengths is its modular design for handling changes or system modifications efficiently. The system is highly configurable via the use of rules engines and configurability tools. The modularity and configurability has enabled our customers to adapt to changes as necessitated by mandates, policies, or market needs, as well as the introduction of new programs or modifications to existing programs. evoBrix's modular capability includes:

- Modular and extensible technical architecture that utilizes configuration capabilities, including a rules engine, to enable DPHHS to quickly and cost-effectively adapt to the changing environment of Medicaid
- Individual solution components are SOA-based and loosely coupled to each other, enabling a high level of reuse and interoperability within the DPHHS ecosystem
- Security components and infrastructure that facilitate information exchange, data sharing, and data access in a distributed environment
- Alignment to technology and data standards
- Scalable infrastructure architecture, design, and technology components to provide horizontal and vertical scalability
- Flexibility to modify business rules to support business and policy changes with minimal involvement of developers, greatly improving time-to-market of business requirements
- Performance and system monitoring of the modular components at business and technology levels

evoBrix is in alignment with the MITA Modularity Standard.

- MPATH solution capabilities supporting functional and technical services
- Web service interfaces as REST, SOAP, and COTS APIs
- Well-defined, open interfaces with service definitions conforming to WSDL, Swagger RESTful API Documentation specifications SOA mediation layer leveraging Oracle Service Bus (OSB)
- Rules engine with an integrated rules repository to house all Medicaid rules
- Ability to submit business rules to HHS-designated repository with COTS grade product configuration capabilities
- Systems Development Lifecycle methodologies confirming to CMMI product engineering standards

evoBrix offers the core business services, which are functionally rich, aligned to MITA business architecture, and federally compliant. Each functional module consists of a set of business processes partitioned as discrete, scalable, and reusable components. The modular design and service-oriented assembly of these processes promote flexibility, adaptability, and rapid response to changing business needs.

INT93

The Contractor shall provide electronic notification including detailed release notes for Major and Minor version, patches, updates and fixes deployed to the production environment.

Team CNSI has developed an extensive operational system and support infrastructure comprised of well-documented processes and procedures. Team CNSI's approach is built on an ITIL framework augmented by our own best practices refined over years of collective health care administration operations experience in managing large, complex projects of similar size and complexity. Our release procedures include detailed electronic notification via email to the release stakeholders which includes detailed release notes for Major and Minor versions, patches, updates and fixes deployed to the production environment. The details of notification will be defined in the state approved release management process.

INT94

The Contractor shall work collaboratively with module vendors to reconcile ODS data elements with the all data elements for each module component.

Team CNSI's evoBrix solution for MT PSM is supported by standardized data models for meeting the day-to-day technical and business operational needs. We understand that the State intends to have an Operational Data Store (ODS) to be created and maintained by the System Integration Services (SIS) vendor as an additional MPATH module. Team CNSI has extensive experience in collaborating and working with vendors and external agencies based on experience managing operations for multiple States (Michigan, Illinois, Utah, and Washington). The evoBrix solution for MT PSM contains data definitions and a comprehensive data dictionary for all elements defined in the proposed solution and can be considered for generating reconciliation reports to help the State reconcile the data elements in the SIS vendor managed ODS as well as support responses to inquiries and report requests. Team CNSI understands the importance and relevance of standardized documentation for sharing the data design details of the MT PSM solution for facilitating the MT DPHHS program operations, one of which is the timeliness and accuracy of the data elements and data within the ODS. We will leverage the established processes and frameworks for metadata management available within Team CNSI's evoBrix platform and collaborate with the MT SIS vendor and other module vendors to reconcile the State's ODS data elements with the equivalent elements coming from the MT PSM solution's database which is the system of record.

3.10.1.5 Data Management

Data management within the Offeror's proposed solution and operational data management policies must at a minimum meet HIPAA, HITECH, ARRA and other federal and state privacy and security requirements as they exist on the release date of this RFP and be configurable to assist in meeting future requirements. The Offeror must describe their approach to meeting each of the Data Management and Data Services requirements detailed in Attachment F, Requirements Matrix.

The Team CNSI Advantage

Team CNSI brings a proven evoBrix platform to support the PMIS solution with a matching enterprise-grade data model and interface framework to efficiently manage the application and backend processing needs of the Medicaid enterprise.

- Multi-tenant compliant logical and physical data models
- Standardized/scalable models for diverse needs of current/future business operations
- Use of flexible fields for extensible model support
- Full-fledged audit and data versioning support
- Flexible data model maintenance, reporting, and data dictionary generation
- Generic supportive model frameworks to provide common functionality across subject area models/application
- SOA-based interface standards for data trading within and outside evoBrix PMIS

MTPSM-3-138

Team CNSI has more than 18 years of experience developing and operating MMIS and ensuring that those systems – and the highly sensitive data they process and store – meet or exceed State and Federal privacy and security standards. Our team will bring this wealth of experience and our extensive set of mature practices to the implementation of the evoBrix PMIS solution to help drive the secure design and implementation of all solution components, including IT infrastructure, systems, and application components. Team CNSI has developed expert knowledge of all applicable industry and Federal standards, models, and practices related to security of state Medicaid systems, and the most recent standards outlined by HIPAA, HITECH, American Recovery and Reinvestment Act (ARRA), and the ACA. Our security architecture and design is based on a defense-in-depth approach rooted in industry best practices and honed by years of experience in design and development of MMIS solutions in the states of Washington, Michigan, and Illinois. Because of our experience and the maturity of our security practice, Team CNSI is accustomed to playing a key role in helping State and Federal agencies extend their own security practices. We have contributed significantly to agency and system security plans in the states of Washington, Michigan, and Utah, as well as CMS, the U.S. Census Bureau, and the Department of Defense. Our approach to developing security controls and procedures for the Team CNSI evoBrix PMIS solution is to tightly integrate the strategies and best practices we have developed with the existing MT DPHHS security framework and extend or strengthen it wherever necessary.

Data is the lifeline of a Medicaid enterprise and the timely availability of data that is both reliable and secure is key for successful operations. Team CNSI's evoBrix modular platform is designed with a sound data management strategy that is key for managing the current and future data needs of the evoBrix PMIS solution, and is one of the most vital elements of an extensible, interoperable infrastructure. The solution not only has a robust baseline information architecture but also has the right data management strategy to manage the changes typically associated with health care regulations and reforms. The data management strategy establishes the basic governance processes to handle the complex set of systems and applications, interfacing and interoperating both within the evoBrix PMIS solution and with the partner/vendor systems that comprise the broader MT DPHHS Medicaid enterprise.

Team CNSI understands that timely, secure, and relevant accessibility to the enterprise data is key for the evoBrix PMIS solution. Factoring in the specific data accessibility requirements for MT PSM, both for implementing a well-defined operational system as well as giving due consideration to the future needs in the expansion of such a system, Team CNSI has adopted a framework that facilitates the data access and management needs of a diverse group of users without sacrificing the data manageability and security within the Medicaid enterprise. Towards that end, Team CNSI's overall approach for data accessibility and management for the system of record encompasses the traits shown in Figure 3.10.1-89.

Data Management Premise	Data Management Approach
Trustworthy Data Source	Data will be made accessible and available to users that reflects its current (latest) state from the "system of record," which is the PMIS solution that is part of the evoBrix transactional system. It entails that the proposed solution will congregate the necessary and relevant data from external and internal sources and help manage it via entities that are designed based on the relational data modeling paradigm.
Platform Neutral Data	Data will be made available to a user or an application system via multiple means including, but not limited to, a web-browser, mobile devices, web-service requests/responses, direct inquiry via Structured Query Language (SQL), or through data extracts managed by SOA Interfaces.
Readily Located Data	Data without metadata is not of much use. Team CNSI's evoBrix PMIS solution comes with standard structured, complete, and accurate metadata for the underlying data models, that can be used not only to document the content of data sets but also to provide a semantic directory to pinpoint the right data to meet the needs of the users.
Real Time Data	Data is useful and relevant only when it is timely. Data changes over time, so it is crucial that the system is not only able to accommodate it, but also provide for an audit trail of the changes. Team CNSI's evoBrix PMIS solution is built to support data availability needs on a real-time basis for the day-to-day activities in the transactional system, which helps manage the various business functions such as enrolling and managing providers, manage communications and correspondence with providers, among others. It ensures that business operations, no matter where or who the user is, get a consistent picture of the data that reflects the system of record.
Application Neutral Data	Team CNSI's evoBrix PMIS solution supports a Data Services layer, a foundational component in the overall architecture, that provides seamless support that is application neutral for all data inquiry, processing, reporting, and analytic needs. The architecture ensures that many types/kinds of modern applications can leverage the same data to help support operational needs.
De-identified Data	Data de-identification, alternatively referred to as anonymization or masking, is key for ensuring data privacy, confidentiality, and data protection. The evoBrix platform provides a facility to de-identify the PMIS solution production data should the data be leveraged for provisioning/setting up a development/non-production environment for supporting solutioning/configuration activities.
Data Interchange Format	Team CNSI's evoBrix PMIS solution is capable of presenting data in several formats suitable for data interchange with other systems, including but not limited to, popular file formats such as Microsoft Excel, fixed/variable-width ASCII, Extensible Markup Language (XML), and via Java Database Connectivity (JDBC)/Open Database Connectivity (ODBC) interfaces. Team CNSI's approach is to permit the accessibility of the data to the users to support data inquiry, processing, analysis, visualization, and reporting processes both within and outside the evoBrix PMIS solution.

Figure 3.10.1-89. Approach for Data Accessibility and Management of System of Record Data. Team CNSI's approach/solution is beneficial to MT DPHHS for addressing the various data management needs.

DM04

The Contractor's solution shall maintain record/audit trail of errors during update processes, accounting for originating source and user.

Team CNSI's evoBrix PMIS solution has a comprehensive data model that supports record level history/ versioning and audit capability. evoBrix captures every change in the system and maintains the history, providing the information for a specific period. It also captures audit information, such as what changes have been made, who made the changes, and when. Based on Team CNSI's extensive experience in implementing and supporting operations for multiple States, we have refined an approach to support an audit trail of all pertinent events, giving due consideration to storage space and performance constraints. Changes, additions, or deletions to data (including operational and security data) and the associated errors or exceptions, if any, are tagged with information that includes the originating source (such as a specific

inbound interface from a designated source, a business operations user making a change in the system, etc.), the date and time, and information about the user who initiated the change. Any errors captured as part of the data updates received from an external interface through the Enterprise Service Bus (ESB) are sent as a back feed to the designated source through an outgoing interface. The source system then verifies and performs necessary actions on the data. The corrected data is received in the evoBrix PMIS solution in the next interface run.

DM09

The Contractor's solution shall provide audit trails to allow information on all transactions to be traced from receipt of the transaction through the completion of the transaction, capture at a minimum date/timestamp, data source, worker id, action taken and log any errors encountered for reporting.

Data updates to Team CNSI's evoBrix solution data mart could happen from different sources – application screens updating transactional data, Team CNSI's evoBrix ISR solution updating reference and transactional data, and inbound Electronic Data Interchange (EDI) file transactions. Each of these sources are responsible for logging audit information in the transaction and reference data marts. Audit fields are a part of every data mart table, and include but not limited to, the originating user/application identity responsible for the data modification, and the modified time. In addition to this, audit fields such as Effective Date, From Date, and To Date are applicable for functionalities like enrollment, which is active only for a certain time period. Team CNSI's evoBrix PMIS solution maintains history of such transactions as part of audit requirements and traceability.

Any exceptions while processing transactions through evoBrix PMIS solution screens or EDI file processing are captured and logged into error/exception tables in the evoBrix error data mart. The error information contains the occurrence time, originating user or application identification, module or program name, error code, message, and, in specific cases, the error description or the record identification for which the exception occurred. Error transactions for critical modules are summarized and reported using Team CNSI's evoBrix Reporting Solution for necessary action.

While the application and EDI updates happen as part of the application module inside Team CNSI's evoBrix solution, interface files are handled by Team CNSI's evoBrix Interface Service Repository (ISR) solution. Through its various interface methods (fully automated workflow, user-intervened workflow, or screen uploads), Team CNSI's evoBrix ISR solution receives data from various internal and external sources, and incorporates them into evoBrix solution reference and transactional data mart. As a part of the MT PSM operations process, any error information is logged into the ISR data mart. The error information will include, but is not limited to, transaction record identification, interface run time, originating user or application identification, interface identification, interface run status, occurrence time, error code, and message. Errors are reported via email notifications, Team CNSI's Reporting Solution, Team CNSI's HealthBeat solution, or error report extracts depending on the interface method. Any escalations on source data correction or processing are notified for respective actions.

DM10

The Contractor shall ensure that all narrative descriptions of codes and abbreviations are available for reporting.

Team CNSI's evoBrix PMIS solution maintains up-to-date versions of all provider related reference data such as enrollment types, provider types, specialty, and sub-specialty to name a few. All codes have

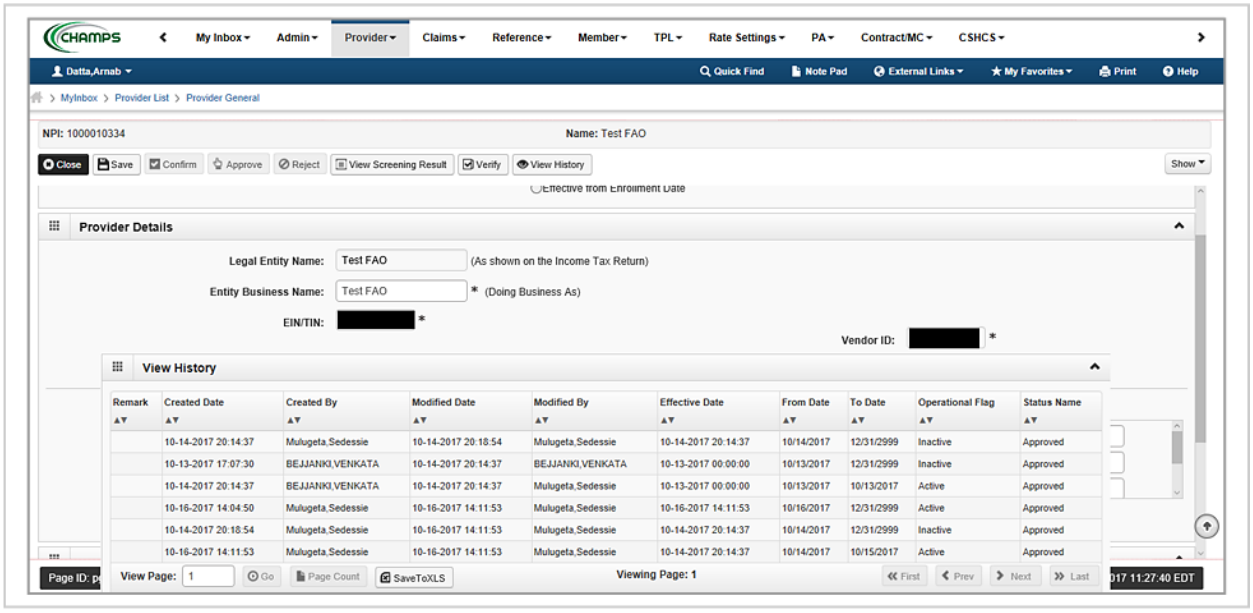
corresponding short and long descriptions which are a part of the reference data. These narrative descriptions could be extracted into reports using SQL query extracts, screens, or Team CNSI's Reporting solution. Please refer to section 3.10.15 for more details on Team CNSI's Reporting Solution.

DM108

The Contractor's solution shall provide a configurable workflow process for resolving near matches for providers that can link, void or end date extraneous records (i.e., duplicate provider records).

Team CNSI's evoBrix PMIS solution eliminates duplicate provider records by using a single master record to store all relationships a provider may have with the State. Even if a provider is associated with multiple provider types, the evoBrix PMIS solution retains the information under a single enrollment that is permanently linked to the provider's unique National Provider Identifier (NPI) and Taxpayer Identification Number (TIN). If the system must process the same record, the evoBrix PMIS solution will always slice and dice the records (i.e., versioning) based on the date segment of the records and will not create duplicates, thus maintaining data integrity. Figure 3.10.1-90 illustrates the high-level process flow for managing code updates in the evoBrix PMIS solution

For any updates to existing provider records, the evoBrix PMIS solution uses a configurable provider matching process that grades the match level of an incoming provider record by comparing it with the master provider record already existing in PMIS. The algorithm that does the comparison assigns points to various factors based on their relevance to the master record. When the incoming provider record does not reach a pre-defined threshold of points, it is considered a no-match requiring manual intervention. This triggers a notification with all necessary details requiring the business operations user to intervene and take manual action to resolve any discrepancy in matching the provider or rejecting it should it be deemed a duplicate.



MTPSM-3-385

Figure 3.10.1-90. Data Record Versioning for Transactional Records. Team CNSI's evoBrix PMIS solution slices and dices the records for managing changes to data from different sources/users based on the date segments of the records maintaining data integrity.

DM11

The Contractor shall develop and maintain an electronic data dictionary using industry best practices to be approved by the Department. At a minimum, the data dictionary shall contain for each field: field name in human readable format, field description, database field name, database table, field type and length, valid values and their corresponding descriptions.

Team CNSI's evoBrix PMIS solution is designed on an integrated data model, managed via the industry standard erwin Data Modeler, as a single point of access to all relevant transactional and operational data. The data model determines the structure and flow of data throughout the solution and is an abstract formalization of objects and their relationships within the system to ensure cross-referential integrity across diverse business process areas to prevent data inconsistencies. The evoBrix data models and the supporting data dictionaries implemented in the relevant database schema help maintain the compatibility and integrity of data by enforcing business rules. Leveraging the erwin Data Modeler as a standard ensures the conformity of data model objects and simultaneously provides a standardized framework for rapid data model conception, comparison, maintenance, database schema generation, and reporting; this serves to ensure the timely availability of the relevant models for the transactional and operational systems for day-to-day business use.

Team CNSI understands the importance and relevance of standardized documentation for sharing the data design details of the evoBrix PMIS solution for facilitating the MT DPHHS program operations. The evoBrix PMIS solution will follow industry standards for data element definition. The system documents the data dictionary by cataloging the different aspects of attributes, including size and other constraints. Team CNSI publishes a standard business data dictionary that shows the definition, semantics, and element usage across different systems, and uses the concept of creating crosswalks between the different definitions of industry standards. The alignment and adoption of industry standards-based approach ensures easier reporting and allows the evoBrix platform to leverage industry benchmarks to improve the overall program delivery.

The data dictionary is defined and maintained as part of the evoBrix physical data model using erwin Data Modeler. The model is always in sync with the database, ensuring that the data dictionary is always current with any data element changes in the system. Figure 3.10.1-91 lists the different components managed within the context of a Data Dictionary.

Data Dictionary Component	Details
Data Model Convention	Describes the data modeling technique and naming convention used in designing the evoBrix online transaction processing (OLTP) tables
Subject Area	Describes the logical grouping of tables and their definition based on the business data
Table Structure	Describes the technical meta-data of data elements in each evoBrix table as listed below - (a) Table name (b) Field name (c) Field description (d) Field datatype, length, and format (e) Database constraints (Referential integrity, Check/Not Null constraint, etc.) for the field, as applicable (f) Valid values and descriptions for the field, as applicable
Word Glossary	Describes the abbreviation list used in the table and column naming convention
Meta Data Elements	Describes common data elements found on all evoBrix tables

Figure 3.10.1-91. Data Dictionary Component. Team CNSI's standard business data dictionary.

DM115

The Contractor's solution shall collect, store, and maintain the data necessary for T-MSIS reporting as required by CMS.

Team CNSI's evoBrix PMIS solution ensures the data required for T-MSIS is captured and stored per CMS federal specifications. evoBrix maintains T-MSIS valid values information in the data repository and creates a configurable crosswalk table between CMS values and evoBrix values. Any future modifications on T-MSIS data requirements can be easily handled by Team CNSI's configurable evoBrix solution.

The majority of the T-MSIS data elements can be directly mapped from evoBrix Data Model and State-specific customizations through configurable transformation rules that would be leveraged seamlessly while extracting the data. Wherever necessary, Team CNSI will work with the State business teams to define additional crosswalks to align State-specific values with CMS values as per defined standards. Team CNSI's T-MSIS experience will help state build the crosswalks efficiently.

Team CNSI evoBrix data model supports all the provider segments (Location and contact, Licensing info, Identifiers, Taxonomy classification, Medicaid enrollment, and Bed Type information). To illustrate an example, Figure 3.10.1-92 shows the crosswalk for OWNERSHIP-CODE that was configured as part of our existing solution. Additionally, Team CNSI's expertise with end-to-end T-MSIS implementations in the States of Washington and Utah can help MT DPHHS meet the T-MSIS requirements as needed.

State Valid Values		CMS T-MSIS Valid Values	
Ownership Code	**Ownership Name**	**Ownership Code**	**Description**
GC	Government - City	11	Government - City
GCC	Government - City-County	13	Government - City-County
GCO	Government - County	12	Government - County
GF	Government - Federal	09	Government - Federal
GHD	Government - Hospital District	14	Government - Hospital District
GRP	N/A - Individual Only Practices as Part of a Group	88	N/A - The individual only practices as part of a group. e.g., as an employee
GS	Government - State	10	Government - State
PC	Proprietary - Corporation	05	Proprietary - Corporation
PI	Proprietary - Individual	04	Proprietary - Individual
PO	Proprietary - Other	07	Proprietary - Other
PP	Proprietary - Partnership	06	Proprietary - Partnership
VNPO	Voluntary - Non-Profit - Other	02	Voluntary - Non-Profit - Other
VNPRO	Voluntary - Non-Profit - Religious Organizations	01	Voluntary - Non-Profit - Religious Organizations

Figure 3.10.1-92. Sample Ownership Code T-MSIS Mapping. Team CNSI's evoBrix PMIS solution supports the mapping of Provider Segments for facilitating CMS T-MSIS reporting.

DM116

The Contractor's solution shall capture and maintain the provider related data items needed to support Payment Error Measurement (PERM) processing.

Team CNSI understands that MT DPHHS shares provider related data items for PERM processing with CMS. The evoBrix PMIS data model maintains the relevant provider data elements needed for generating the provider file as per the federal requirements published by CMS. Figure 3.10.1-93 lists the data elements from the provider module that is typically used for PERM processing. Team CNSI will work with MT DPHHS to enhance this list to support the ongoing needs for PERM processing.

PERM Processing Provider Data Element	Provider Data Element Description
Provider Number	Provider ID or a unique number to uniquely identity the provider in evoBrix PMIS
Provider NPI	Provider NPI
Provider Name	Name of the provider
Provider Type	State-specific provider type value
Provider Specialty	State-specific provider specialty code
Provider Street Address Line 1	Provider address first line
Provider Street Address Line 2	Provider address second line
Provider City / Town	Provider city name
Provider State	Provider state name
Provider Zip Code	Provider zip code (either 5 digits, or zip + 4-digit area code)
Provider Phone	Provider phone number, with the area code
Provider Fax	Provider fax number, with the area code

Figure 3.10.1-93. PERM Processing Provider Data Elements. Team CNSI's evoBrix platform supports the necessary data elements for facilitating the PERM processing for the PMIS solution.

DM117

The Contractor's solution shall retain in the module, after implementation, seven (7) years of electronically imaged documents and data. After seven (7) years, the data will be purged (deleted) from that module. All active records (active providers, active members, active cases, etc.) and 100% of all history for any entity or case that has been active within the last seven years will be retained. Any entity and/or case that has been continuously inactive for the last seven years will not be retained, will be purged, and will no longer be accessible by users in that module.

Team CNSI's evoBrix PMIS solution is part of the transactional system that supports the storage of the converted/ongoing operational data for managing the various aspects of enrolling and maintaining providers for MT DPHHS. Typically, transactional systems will have a defined data retention policy that gets established once the target system goes live. As mandated by MT DPHHS, Team CNSI will implement the 7-year retention requirements for the transactional data records for the evoBrix PMIS solution. Historical data that fall outside the retention time limits that are continuously inactive for the last

seven years will be physically removed from the evoBrix PMIS transactional system. Team CNSI will also ensure that any active provider records with the supporting datasets including electronically imaged documents, along with 100% of all history for an entity that has been active within the last seven years, will be retained.

DM13

The Contractor shall be able to demonstrate the ability to support requirements for backup and archiving consistent with Department SLAs and CMS, State, and industry standards. The Contractor shall also adhere to data retention requirements cited in 45 CFR 164.316 and the State's Administrative Rules.

Team CNSI's backup processing approach is reliable and robust and is based on adhering to the following principles:

- Data is stored in native format
- Data deduplication and replication
- Usable copies of production data for various use cases
- Fully managed and fully monitored solution by dedicated operations team

Backups retention is decided based on the Department's data retention requirements cited in 45 CFR 164.316, the State's Administrative Rules, and industry standards. In addition to that, a different SLA is considered for the data archival. Team CNSI maintains 36 days of backup retention and 50 days of SAN level retention for other operations such as the States of Michigan and Washington.

Team CNSI's backup and recovery approach is based on using the following tools:

- Oracle Backup Service:

  Team CNSI uses Oracle Database Backup Service, as illustrated in Figure 3.10.1-95, which is a low-cost alternative for storing backups in an offsite location. It is a cloud object-based storage offering that enables Team CNSI's evoBrix PMIS solution to store database backups. Oracle Database Backup Service can be used as the Primary backup for second or third tier databases, or use the cloud backup as a secondary copy for long term archival requirements.

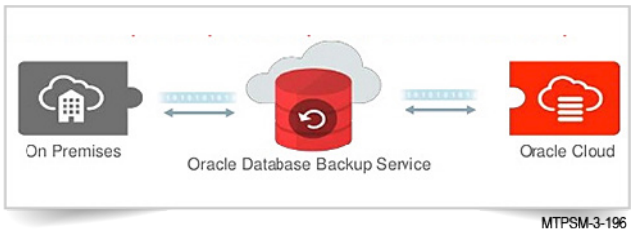


Figure 3.10.1-94. Database Backup Service. Team CNSI's Oracle Database Backup Service could be used for long term archival requirements.

- Oracle Recovery Manager (RMAN):

  Team CNSI uses the Oracle Recovery Manager (RMAN) solution to configure and backup the Oracle databases to an external media. The RMAN backup strategy is incremental in nature thereby saving storage costs without compromising on recovery or recovery timelines. The backup strategy is created considering the criticality of the environments and by meeting Department requirements without compromising on the data recovery as shown in Figure 3.10.1-95.

Environment	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Production	---------- Incremental ----------						
Test/UAT	---------- Incremental ----------						
Development	---------- Incremental ----------						

Figure 3.10.1-95. Database Backup Strategy. Team CNSI's Database backup strategy is built to meet the needs of the Department requirements to address access to and recovery of critical data.

To further improve the cost savings and performance of the backups, following RMAN special features are used as illustrated in Figure 3.10.1-97.

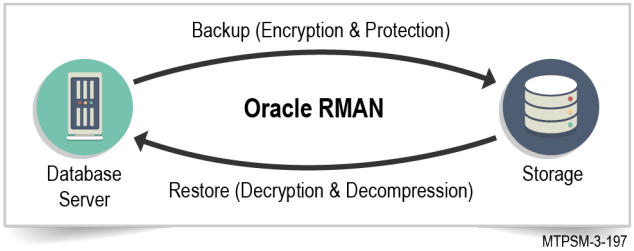


Figure 3.10.1-96. Database Backup and Restore. Team CNSI's Oracle Database Backup and Restore using RMAN supports encryption and compression for improved security and smaller footprint.

- Compression: It conserves bandwidth by reducing the size of the backups before they are sent to the storage. Recovery Manager (RMAN) supports binary compression using multiple levels like HIGH, MEDIUM, BASIC, and LOW.
- Encryption: For improved security, encryption can be configured for RMAN backup sets. Encrypted backups cannot be read if they are obtained by unauthorized users. This feature requires the Enterprise Edition of the Oracle database.

- Oracle Flashback

The Oracle Flashback Database and restore points are related data protection features that allow Team CNSI's evoBrix PMIS solution to rewind data back in time to correct any problems caused by logical data corruption or user errors within a designated time window. These features provide a more efficient alternative to point-in-time recovery and does not require a backup of the database to be restored first. Figure 3.10.1-98 highlights the use of Oracle Flashback.

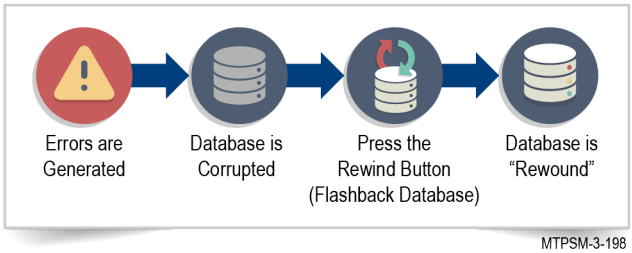


Figure 3.10.1-97. Oracle Flashback. Team CNSI's Oracle Flashback provides a mechanism to rewind data back in time for addressing logical data corruption within SLA timelines.

DM14

The Contractor's solution shall maintain an audit trail of all changes to data, including changes that were made in error and subsequently backed out of or suspended.

Team CNSI's evoBrix PMIS solution offers a configurable Security Framework that provides a secure environment for information management and protects against unwanted loss or disclosure of data. Authenticated access and RBAC enforces security in the PMIS module. The security framework

maintains extensive user audit logging for the audit trail in support of HIPAA Security and Privacy to track changes made to any data stored in PMIS. Authorized users can access audit trail information using the web portal to keep track of who initiated the change, what changed, when the change was requested, who approved/denied the change, and when was it was approved/denied. The solution provides the ability to reverse or back out changes made in error while still retaining the associated audit trail.

DM15

For audit and reporting purposes, the system shall provide and maintain the following data for all reference codes:

a. Effective date

b. End date

c. Date when last changed

d. Who made last change

e. Short description

f. Long description

Team CNSI's evoBrix PMIS solution maintains a complete audit trail of changes made to any data stored in the system. This includes both reference and transactional data. Audit trail entries for reference codes include the following data elements that are also available for reporting purposes:

- Effective date: The date evoBrix PMIS began using the updated information
- From date: The beginning date of the effective date span
- To date: The end date of the effective date span
- Date Modified: The date the change was applied to the system
- Modified By: User ID of the person or system acting on the change
- Short Description: The short description of the reference code
- Long Description: The long description of the reference code
- Operational Flag: A flag that shows whether the system is actively using the information (Active) or has been "soft-deleted" and is retained only for historical purposes (Inactive)
- Remark: A free-form text entry field that allows the user to provide a narrative statement concerning the action taken

DM17

The Contractor's solution shall provide the ability to store and apply updates to all applicable codes upon new release at an interval appropriate for the data or when requested by the Department.

Team CNSI understands the need for an efficient, secure, and scalable integration solution as well as operations to ensure that updates to all applicable codes are applied upon new release at an interval appropriate for the data or when requested by the department. Given our experience with system operations in multiple states and specifically in a multi-tenant SaaS model, Team CNSI production data management processes ensure scheduled production updates for applicable codes are completed as planned. Team CNSI's evoBrix PMIS solution is designed to ingest and/or process support data for applicable codes through three different channels. The channels are designed with varying business requirements in mind, ranging from a user-intervened work flow to an end-to-end fully automated model. Figure 3.10.1-98 illustrates the high-level process flow for managing code updates in the evoBrix PMIS solution.

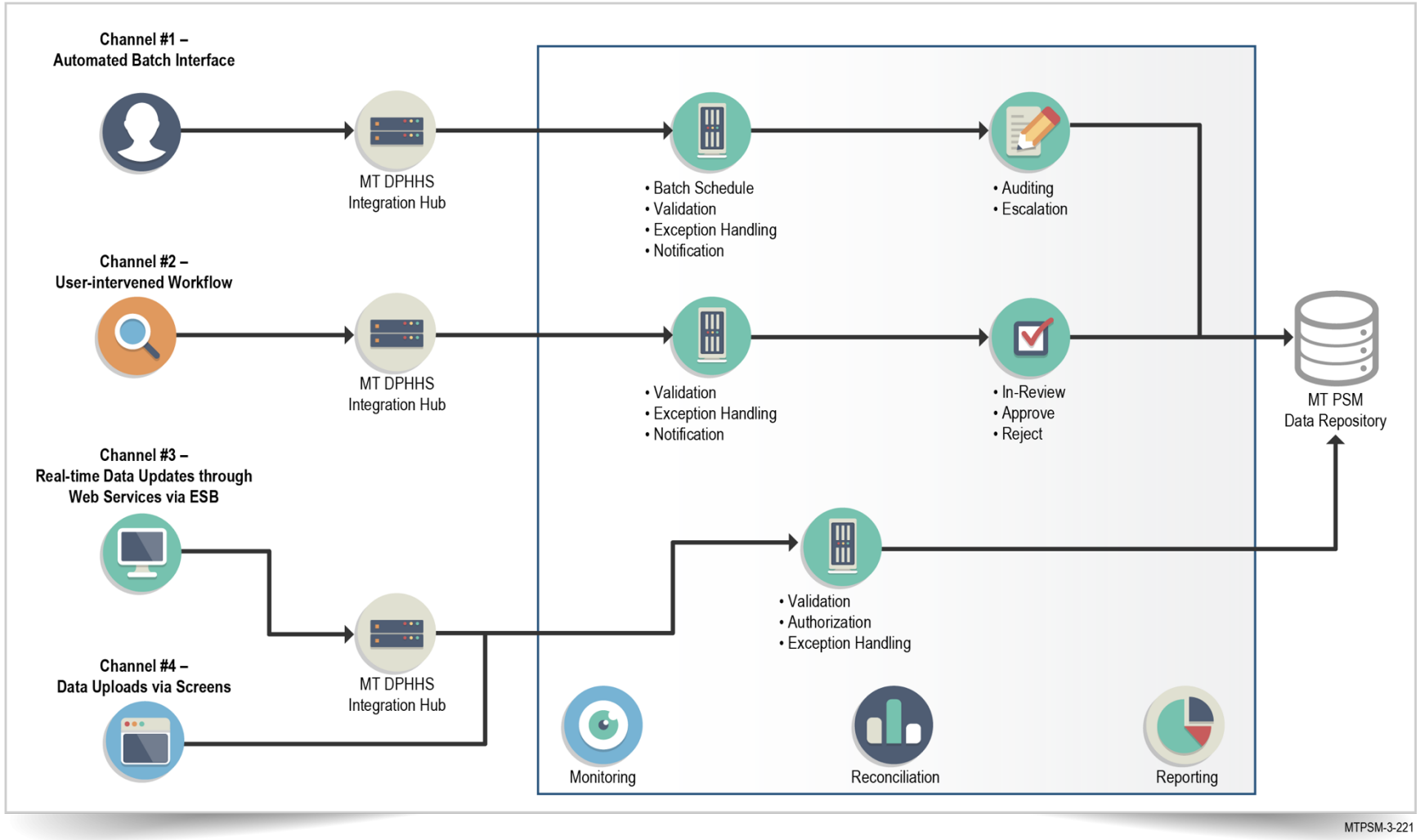


Figure 3.10.1-98. High-level Process Flow of Multiple Intake Channels leveraged for Code Updates. Team CNSI's evoBrix solution has multiple intake channels for ingesting support data for facilitating MT PSM business and system operations.

Batch Interfaces via Interface Service Repository (ISR)

Scheduled interfaces load support data files automatically into Team CNSI's evoBrix PMIS solution staging through the evoBrix ISR solution. The data is then validated and processed per business requirements before loading into the target data mart. As a part of the MT PSM Operations process, error information is logged into the ISR data mart and is reported via Team CNSI's Reporting Solution. Any escalations are notified for respective actions.

Unlike fully automated batches, user intervened workflow follows a certain update schedule or calendar wherein business operations request a specific dataset to be uploaded and validated. The dataset is loaded into test environments to be validated, assessed for impact, and verified by Team CNSI's business operations. Exceptions, if any, are identified for corrective action in the dataset or the target system as required. The dataset is then approved and considered "production ready."

Real-time Data Updates via Web Services using Enterprise Service Bus (ESB)

Team CNSI's evoBrix PMIS solution leverages ESB to connect core services and exchange support data without directly accessing underlying system. Applicable codes upon new release received through web services go through robust authorization, authentication, and validation features provided by Oracle Service Bus before it is made available in the evoBrix PMIS solution data repository. The solution is also compatible with industry standard Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) protocols.

Data Updates via Screens/Upload Functionality

Applicable codes, upon new release or when requested by the department, could also be updated via Team CNSI's evoBrix PMIS solution's screen upload functionality. This could be an unscheduled request where business operations could upload a certain support data set, which then goes through validation based on business rules before it is made available in the evoBrix data repository.

DM18

The Contractor's solution shall perform batch control including logging and reporting.

Batch interfaces are the preferred way to load data that is updated on a frequent basis during Team CNSI's evoBrix PMIS solution's operations. Team CNSI's evoBrix ISR solution provides a configurable design that features management of scheduling, loading, auditing, testing, error logging, reporting, and escalation. The ISR solution receives batch files on scheduled basis or through screen uploads. Received files will go through file level validation, record level validation, and business level validation to make sure only correct data is getting loaded into the evoBrix PMIS data mart. The error records during the validation process are logged into evoBrix error tables. Audit information, including start and end time of the transaction, total number or records in the file, total error records, total successful records, and originating source will be stored in evoBrix audit tables.

Batch statuses, transactional errors, escalation, and audit information are reported through email notifications, Team CNSI's Reporting solution, or Team CNSI's HealthBeat solution. The evoBrix ISR solution will also report unsuccessful file transfers and uploads to approved MT DPHHS agencies, as well as confirm successful file transfers and uploads. The solution also provides configurable screens to administer the various aspects of the evoBrix interface operations, and provides a dashboard for reporting

the status of all the scheduled interfaces. In addition to reporting solutions, the evoBrix solution generates database reports as well to communicate the granular outcome of the individual batch process.

DM19

The Contractor's solution shall archive all versions of reference information and update transactions.

Team CNSI's evoBrix PMIS solution adopts a data modeling paradigm that ensures no aspect of the reference information or changes to the transactional data are lost by archiving all versions of the changes. The solution uses a unique concept of slicing and dicing the data to systematically segment the data record to support a temporal report of events. Data segmentation helps visualize the data changes as "time slices" for varying time horizons. Figure 3.10.1-99 illustrates the concept of slicing/dicing a data record to accommodate a data change with versioning support. The versioning is implemented using a combination of the following attributes:

- From date: The beginning date of the effective date span
- To date: The end date of the effective date span
- Operational Flag: A flag that shows whether the system is actively using the information (Active) or has been "soft-deleted" and is retained only for historical purposes (Inactive)
- Status: The code identifier that identifies the workflow status of the record (In-Review/ Approved/Rejected).

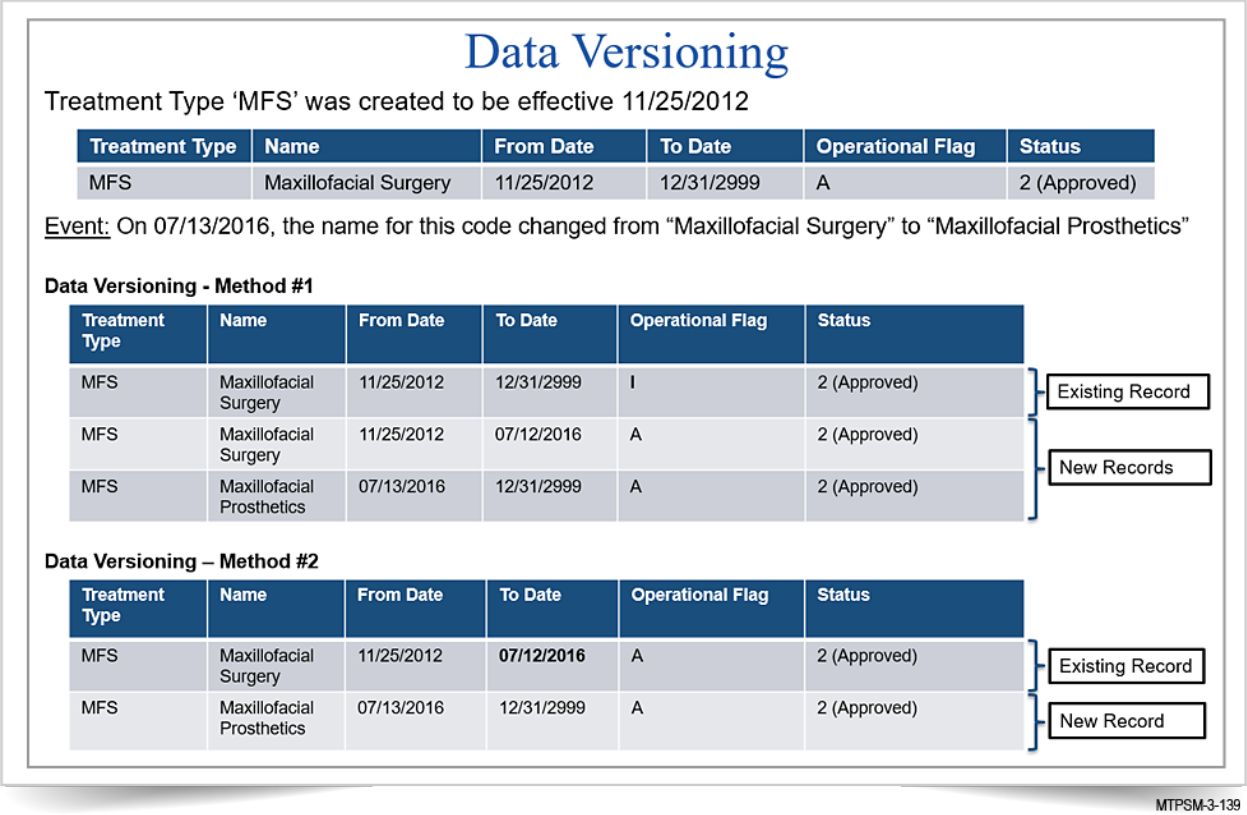


Figure 3.10.1-99. Data Versioning. Team CNSI's evoBrix solution supports a comprehensive versioning mechanism to archive historical data changes.

DM20

The Contractor's solution shall have the ability to void or reverse recent changes by rolling back to prior configurations.

Team CNSI's evoBrix PMIS solution handles the configuration of reference data through front-end screens as well as backend data inserts. The system uses code identifiers/system generated identifiers to link reference data with transaction records. This makes sure that any change in pre-configured reference data will not affect existing transactions. Editable reference details are stored with appropriate statuses and effective date ranges in a detail table. When there is a need for a rollback of already configured reference data, the system can inactivate and end date the existing records and create new records with the latest details. Transactions will always use the latest active details applicable for the reference data. When there is a need to void a reference data, the system can inactivate/end date the newly created reference data record.

The application and database are designed to prevent the creation of duplicate or orphan records. The system is designed to ensure that one set of processes update one set of entity tables, ensuring that there is data and business integrity enforcement for a given entity. The process has built-in exception handling features to roll back errors. The database design prevents the ability to create records or data without the appropriate application controls and checks. These constraints and checks prevent such occurrences and provide the ability to roll back a transaction that has violated these rules.

DM21

The Contractor's data management strategy shall include the following concepts: Data Integrity (data cannot be modified undetectably), Data Availability (access is not inappropriately blocked or denied), Data Authenticity (validation of transactions), Data Security (encryption and Department approved security protocols and processes), Non-repudiation of Data (parties to a transaction cannot deny their participation in the transaction).

Team CNSI's evoBrix PMIS solution fully meets or exceeds all MARS-E specifications for security. The evoBrix security standard is written to comply with CMS, NIST, FISMA, and HIPAA standards applicable to the system.

The evoBrix solution is designed with layered security zones, as shown in Figure 3.10.1-100. This layered design is used to put the most sensitive data behind multiple layers of security. The layered design also allows progressively more restrictive controls on systems to reduce risk of unauthorized access to data and systems.



Data Integrity, Authenticity, Non-repudiation, and Auditability

The evoBrix system interfaces with the supporting vendor modules within the larger MT DPHHS enterprise system. All users accessing the evoBrix system initially authenticate to the MT DPHHS system using the MT DPHHS federated single sign-on (SSO) authentication system. That identity information is then passed onto the evoBrix security system for use by the RBAC controls for authorization to data within the evoBrix system. The RBAC model ensures that the user can only alter or modify data that they are authorized to access and change.

All access to the data is tracked within the system. All transactions are monitored and recorded using application-level auditing and database auditing using Oracle Audit Vault. This allows for a full audit trail of who accessed what information, and who modified what information. The audit trail gives MT DPHHS and Team CNSI a solid set of tools to respond to any inquiries and assertions that there are issues with records. The evoBrix system tracks all changes using Oracle Audit Vault and records all identity data. Every change to a record and all views of data in the system are recorded; the name of the person accessing the system and the date and time that they performed the actions are recorded.

The Oracle Audit Vault Server (OAVS), shown in Figure 3.10.1-101, includes reports to assist in documenting compliance. The OAVS streamlines compliance reporting. The OAVS reporting is also used for generating reports for audit trails, and for looking at database information usage.

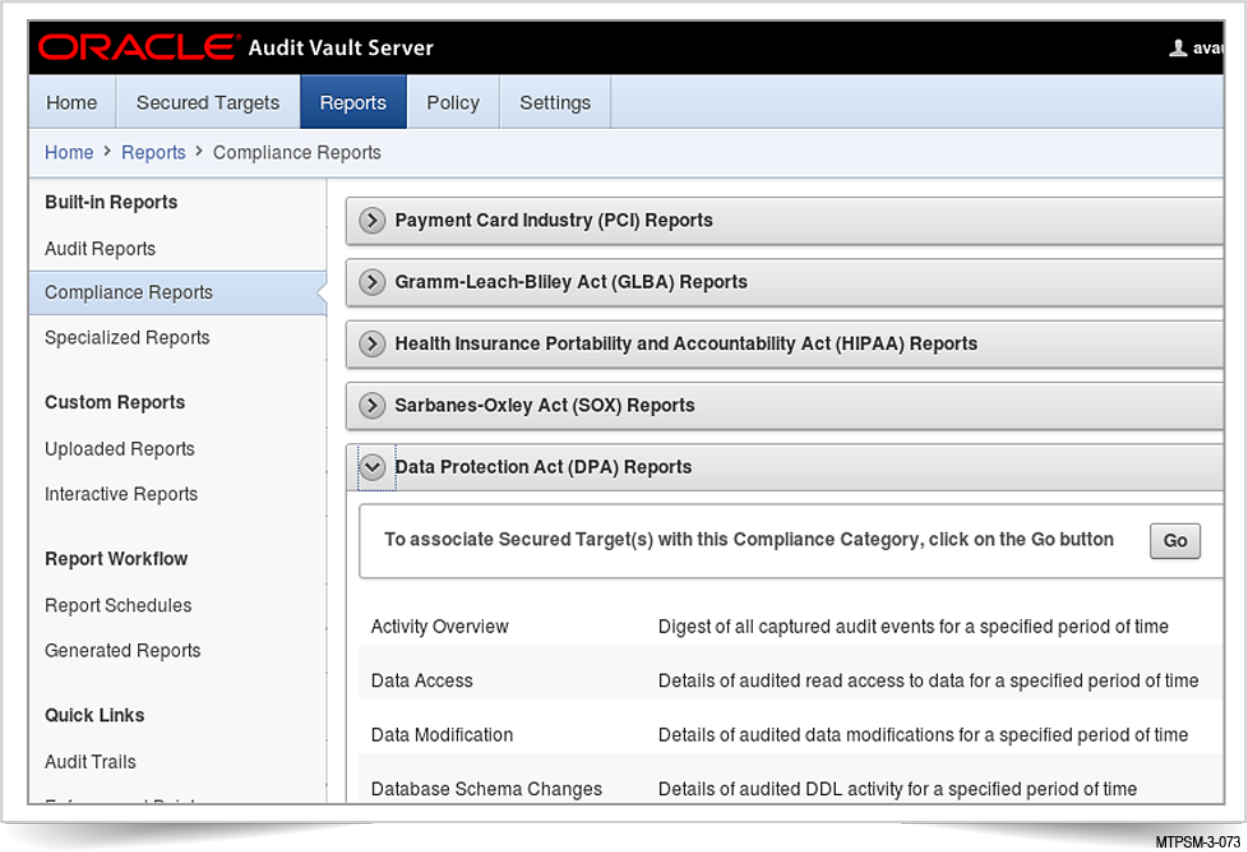


Figure 3.10.1-101. Oracle Audit Vault. Oracle Audit Vault enables reporting on identity of user data access.

Using this tool, Team CNSI will be able to:

- Log every auditable event
- Report on every auditable event
- Protect all database logs from unauthorized modification or deletion
- Protect all database logs from unauthorized viewing
- Provide users the ability to generate reports based on ranges of dates
- Be configured to ensure compliance with related Federal and State audit requirements

Data Availability

The evoBrix system is designed for high availability and fault tolerance. The primary system is housed in a cloud data center. All equipment is isolated in the data center. The systems are only accessible via keycard locks to prevent access to systems by anyone other than authorized personnel. All access to systems is monitored and logged. The data center has full power redundancy, as well as fire and environmental protections. All hardware and network equipment in the primary site is duplicated and redundant; single component failure will not bring down the system. In addition, software components are duplicated and deployed in a cluster for high availability.

The evoBrix system also has a fully-equipped secondary site that is geographically separated from the primary system to prevent failure due to facility disruption from natural disasters. The secondary site is built to the same exacting security and facilities standards as the primary site. All data is replicated in real time to the secondary site so that in the event of the primary site not being available, the secondary site will fully take over all tasks and workload. Based upon our annual testing, the secondary site becomes fully operational within four hours.

Data Security

Team CNSI's evoBrix PMIS solution protects confidentiality by encrypting all data. The data stored in the system databases and on servers is fully encrypted using Oracle encryption technology. At the application layer, Team CNSI's evoBrix PMIS solution leverages advanced Oracle security tools, including Oracle Advanced Security pack with Transparent Data Encryption (TDE) and Oracle Data Vault. This combination of tools ensures strong encryption of database indexes and columns containing sensitive information.

All connections to the evoBrix system use SSL technology for fully encrypted connection. All file transfer connections use secure file transfer protocols for encrypted transfer. Where flat file transfer is required, Team CNSI evoBrix uses Titan Secure FTP to ensure encryption of the file in transit and a 256bit AES encryption is used to encrypt the files. Administration and operational staff use encrypted VPN connectivity to access the servers. All database data transferred on the network uses the Oracle network encryption technology to protect the data in flight. Thus, all data in flight is encrypted as well. This avoids the risk of data loss on the network.

Central key management is another element of the Team CNSI strategy for the evoBrix system to reduce exposure of sensitive data and ensure reliability and security of the evoBrix solution. To ensure protection of encryption keys used to protect data and services throughout the system, we leverage Oracle Key Manager to centrally authorize, secure, and manage all encryption keys. Oracle Key Manager is a FIPS 140-2 Level 3 compliant key management system, offering a strong and scalable solution.

Team CNSI's evoBrix PMIS solution is designed to never send system-generated emails with Protected Health Information (PHI)/Personally Identifiable Information (PII). The only email sent out would be a notification that information in the system has been updated and informing the user that they need to log into the system to access updates.

All data transfers between the Team CNSI evoBrix PMIS solution and other parts of the MT DPHHS system are through encrypted file transfers. Titan Secure FTP is used for any transfers of files between trusted systems. All transfers of data are governed by the rules in the RBAC system. The RBAC system restricts access to only data the user is authorized to access, view, or modify. All connectivity to the application, and to systems, are through encrypted network connections. All data stored on the system are encrypted.

Connection Specific Redaction and Confidentiality

Team CNSI's evoBrix PMIS solution security model is based on RBAC, which allows easy, granular control for access to information. Users only see the information to which they are authorized to have access; if a user is not authorized to view a particular set of information, the information is automatically restricted from view. User access to information is easily controlled by the assignment or removal of particular roles to the person. The RBAC model reduces the cost of identity security management and lowers the risk of accidental release of sensitive data. The RBAC model is proven, tested, and currently operational in multiple states managed by Team CNSI.

The use of the RBAC model in the evoBrix system ensures full confidentiality of PHI and PII information. Users of the system can only access a limited set of data based on authorization in the system. The evoBrix system facilitates easy removal of people from the list of authorized people to view information. The connector between the evoBrix system and the larger MT DPHHS system is also governed by the RBAC controls to prevent data leakage to other subsystems inside the MT DPHHS system.

DM22

The Contractor's solution shall provide entity search capability including the ability to search by entity type, entity name, entity address elements, entity phone number(s), unique identifier for entity type, any alternate identifiers including EIN, SSN, TIN and other demographic elements.

Team CNSI's evoBrix solution application screens provide the ability to search for Providers (entities) based on various criteria using the "Manage Provider" menu option and the search results are rendered through the "Provider List" page. Provider List allows the user to search using multiple provider attributes to locate a specific enrolled provider (such as Provider Name, SSN, NPI, Phone number) or a group of providers sharing a common set of attributes (such as EIN/TIN, zip code, and specialty).

The Provider List page has three primary filters and two secondary filters which could be customized by each user according to their preference. The user can then save their favorite search criteria using the "Save Filters" option. This can then be retrieved later under the "My Filters" dropdown whenever the user wishes to reuse them. The results retrieved may be exported and saved to an Excel workbook for additional analysis using "Save to XLS" option. Figure 3.10.1-102 shows a sample provider list page from Team CNSI evoBrix solution with the various filter options to facilitate an enhanced search for business users.

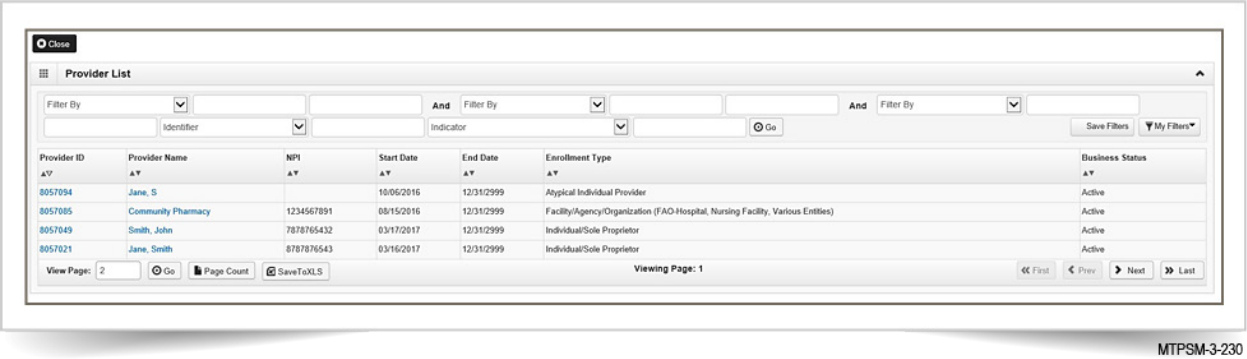


Figure 3.10.1-102. Provider List Page Showing Filter Capability. This screen highlights the three major filters, the secondary filters, the Save Filters and My Filter retrievals, and Save to XLS features.

DM23

The Contractor shall provide real-time access to transactional data for all module components

Team CNSI's evoBrix PMIS solution provides the ability for authorized users to view, manage, and maintain real-time transactional data through online screens. The solution also maintains a complete audit trail of changes made to any transactional data stored in the PMIS data mart.

DM24

The Contractor shall ensure complete transparency of all data fields in reports generated by the system including: providing the Department with SQL, pseudo code, narrative description, analytic protocols and assumptions to document the logic and formulas used in all calculations.

The design component details of Team CNSI's Reporting solution, such as business requirements, report layout design, and functional logic for specific requirements, are tracked and maintained in the Detailed System Design Document (DSDD). In addition to this, the source code or SQL for the underlying database objects that are responsible to provide reports data could be accessed and viewed through Team CNSI's evoBrix solution database.

DM25

The Contractor shall create and maintain a suite of State/Contractor-defined on-line reports to allow users to choose from pre-built defined parameters (such as provider number, procedure code, date of service, etc.) to generate customized reports for monitoring the daily operations of the system and Fiscal Agent Operations.

Team CNSI's evoBrix PMIS solution maintains a set of pre-built operational reports that are available for use from day one of implementation. In addition to this, users could design their own reports with pre-defined parameters as filters using IBM Cognos BI tools in Team CNSI's Reporting Solution. Please refer to section 3.10.15 for more details on Team CNSI's Reporting Solution.

DM26

The Contractor shall certify that any and all unmasked or unscrambled Department data will reside in data centers located in the continental United States. Additionally, this data will only be accessible by resources within the continental United States that have completed the necessary HIPAA and PHI training. Any data that will be accessed by resources that are not physically located in the United States will be masked or scrambled (which would make it impossible to establish a connection between claims data and a specific member or provider associated with the claim) thereby removing the HIPAA and PHI connection between interested parties and the claim data.

Team CNSI certifies that any and all unmasked or unscrambled Department data will reside in data centers located in the continental United States. This data will only be accessible to resources in the continental United States that have completed the necessary HIPAA and PHI training. Any data accessed by resources that are not physically located in the United States will be masked or scrambled thereby removing the HIPAA and PHI connection between interested parties and the data.

Team CNSI uses a defense-in-depth approach to security built on a simple set of key principles:

- Employee education and awareness – Everyone who touches PHI data goes through annual security and HIPAA training
- Multiple layers of physical and environmental controls
- Multiple layers of logical controls and procedures
- Continual monitoring and assessment
- Encryption of data transmission and stored data

- RBAC to ensure that information access is restricted to only appropriate access based on a user's role
- Change management and configuration management to prevent security and stability issues from unauthorized changes
- Intruder Detection System (IDS) monitoring to prevent unauthorized access

Team CNSI ensures that data in all development environments for the evoBrix PMIS solution only house scrambled, masked, or de-identified data to support the solution configuration and development activities. As part of our experience from implementing and supporting multiple Medicaid systems for the States of Michigan, Washington, Illinois, and Utah, Team CNSI leverages a custom data de-identification solution, dataSecureD, to safeguard both the PHI and PII information in the data. The dataSecureD solution is fast, reliable, and secure and comes with pre-configured components and templates purpose-built for Team CNSI's evoBrix solution. The dataSecureD solution leverages a highly scalable framework for scrambling the data using in-database MapReduce principles, ensuring not only the structural and data integrity to not be compromised, but also provide the means to make it repeatable for multiple runs with full restartability.

DM31

The Contractor's solution shall be configured and maintained to validate and standardize addresses according to United States Postal Service (USPS) verification, validation and standardization rules.

Team CNSI's evoBrix PMIS solution uses Pitney Bowes Spectrum Universal Addressing Module to validate postal addresses. Team CNSI periodically updates the Spectrum Universal Addressing Module database to keep up with the changes in the USPS addresses. The evoBrix solution utilizes address validation functions to ensure efficient handling of USPS addresses, reduce costs associated with returned mail handling, and to ensure compliance with regulatory requirements.

DM37

The Contractor's solution shall facilitate real-time data processing including data cleansing, data loading, data brokerage, integration, validation, reconciliation, and synchronization with the State's enterprise.

Team CNSI's evoBrix PMIS solution can intake or ingest externally sourced data relevant to the functioning of MT PSM business operations via evoBrix ISR. The ISR solution integrates with external systems via evoBrix System Integration Services. Data exchange and file transmission is handled by ISR in a secure manner with external entities using secure file transfer protocol (SFTP), FTPS, or SSL. The solution validates and processes the files in near real time or in batches on a scheduled basis. Any error and audit information is logged into ISR solution's error and audit data marts respectively.

Team CNSI's evoBrix PMIS solution is built on a relational database modelling paradigm with normalized data structures. This model will ensure structural and referential integrity along with inherited relationships amongst various entities. For data exchange with external systems, the proposed platform provides a comprehensive data reconciliation framework that mirrors the same structural and data integrity with external systems. The evoBrix ISR solution can send the required extracts with the defined data sets to the MT DPHHS data warehouse on a schedule or request basis ensuring the data from the evoBrix system of record is synchronized with the larger State's enterprise.

DM38

The Contractor's solution shall optimize and consolidate data management storage.

Team CNSI's evoBrix PMIS solution stores all database files in Oracle Cloud's Block Storage service. Block storage enables OLTP databases, which have high input/output operations per second (IOPS) requirements, to store and retrieve data efficiently, by bypassing the host operating system and interacting directly with virtual block devices. Chunks of data are stored in blocks, each with an address, but with no other metadata. Applications decide where data is stored, and they retrieve data by calling the appropriate block addresses directly. Block storage optimizes storage for IOPS and block-based access and provides POSIX-compliant file systems for Oracle Cloud Infrastructure Object Storage Classic instances. In addition, Team CNSI's evoBrix PMIS solution includes Oracle Advanced Compression 12c feature which will provide 50% to 60% space savings.

Team CNSI's evoBrix PMIS solution uses Oracle Cloud's Object Storage service for storing both database and application backups. Oracle Cloud's Object Storage service provides a low cost, reliable, secure, and scalable solution for storing unstructured data and accessing it anytime from anywhere. It is ideal for data backup, archival, file sharing, and for storing large amounts of unstructured data such as logs, sensor-generated data, and VM images.

DM39

The Contractor's solution shall maintain all data sets defined by the HIPAA Implementation Guides to support storage of all transactions required under HIPAA Administrative Simplification Rule (e.g., Gender, Reason Code) for seven (7) years.

Team CNSI brings a data retention framework that is configurable to meet the varying data retention needs for different business areas of the evoBrix PMIS solution. The framework has the capability to address the data retention needs for audit, history, core partitioned, and non-partitioned entities managing the current and historical transactional/operational data for providers. Any provider data that falls outside the defined data retention period would be considered as operationally non-relevant historical data and the data retention framework will physically delete the applicable data record in the Team CNSI evoBrix PMIS solution. Data from all supporting inbound and outbound interfaces will be retained for a period as defined by Montana DPHHS. The HIPAA Code Sets such as HCPCS and NDC defined by HIPAA Administrative Simplification rule that are referred within Provider transaction data are maintained indefinitely, while the transactional data sets defined by the HIPAA Implementation guides will support storage for seven years.

Although the data retention framework is designed to be implemented at varying frequencies, such as daily, monthly, annual, or ad hoc, Team CNSI considers it important to ensure that day-to-day business operations aren't impacted due to the implementation of the data retention policies. The physical deletion of data is managed via a combination of daily archival for high-volume transactional entities followed by a physical removal from the archival entities during the monthly or annual maintenance cycles, and via direct physical daily deletes for low-volume transactional entities, thus balancing the needs of the data retention requirements on one hand and the optimal system performance on the other.

DM40

The Contractor's solution shall maintain a normalized RDBMS with referential integrity and is optimized to meet performance requirements.

The evoBrix physical data model addresses data needs of enterprise wide Medicaid operations for Team CNSI's evoBrix PMIS solution. The evoBrix solution has the physical data model for all business areas of Provider Management Information System such as the Provider Staging, Provider Maintenance, Provider Credentialing Services, Site Visit solution, along with the supporting components for interfaces and RBAC. It is a stable and proven data model that evolved over multiple versions and encompasses best practices learned from MMIS implementation across multiple States.

The evoBrix physical data model balances the normalization needs of a data model with the performance needs of large volume transaction processing system. All data items are listed, and then all interrelated rules (known as dependencies) are identified. Database design starts with the assumption that all data items are placed in a single table and then proceeds to break down the table into smaller tables. In the resulting set of tables, joins are needed to retrieve the original relationships.

Both the entity-relationship approach and the normalization approach were applied, as appropriate, to develop the evoBrix solution. The degree of normalization also varies. We use higher normalization in the case of tables that are frequently modified by either inserts or updates, enabling easier maintainability. Normalization levels are lower on tables that are used to inquire and report on data to allow for faster query response. Particular sets of tables used heavily in both modification and inquiry pose challenges. Performance and volume testing and, more importantly, implementation experience, were used to reduce impacts to both functions. Team CNSI has conducted specific performance benchmarks testing to determine the throughput of the system and has resolved several issues that relate to data modeling based on the results. This proposed data model is currently operational in the states of Washington and Michigan.

In addition, our solution strategy for incorporating future modification is to accommodate additional data elements (specific to state needs) as additional columns, referred to as flexible fields or flex fields. This reduces the amount of rework on the user interface and avoids additional background processes when changes are initiated, while still allowing for backward compatibility.

Physical Data Model Components

The evoBrix platform is built on a Relational Database Management System (RDBMS) implemented using the Oracle RDBMS. The evoBrix Physical Data Model comprises of the components as shown in Figure 3.10.1-103.

Database Schema Component	Details
Subject Area	Logical grouping of tables to make business sense
Table	Physical entity that stores data
Column	Physical attribute that stores characteristics that define a table record
Relationship	Business constraints defined between two tables
Column Datatype	The physical data type of the column to indicate type of data stored

Database Schema Component	Details
Primary Key	The column/set of columns that uniquely identify a transaction record
Foreign Key	The unique key of the parent table that defines the relationship between a table and its parent
Column Constraint	Conditions imposed on a column regarding the data stored in it, for example, NOT NULL / Check Constraint

Figure 3.10.1-103. Database Schema Component. Details of components of the evoBrix PMIS Physical Data Model.

DM41

The Contractor's solution shall provide a method to access, query, and report against archived data external to the Operational Data Store (ODS).

Team CNSI's evoBrix PMIS solution comes with multiple channels for accessing, querying, and reporting against the transactional/archived data that resides in the evoBrix solution database, including data that is not transferred to the ODS. First and foremost, users can leverage the evoBrix application screens to perform a range of data inquiries to view the transactional data as well as store them in standard Excel reports. Users can also leverage Team CNSI's robust business intelligence solution managed through IBM COGNOS that provides the means to report against transactional/operational data within the evoBrix solution database. Users can also access and run queries against the evoBrix PMIS solution database to address key day-to-day needs for managing business operations. Team CNSI can also provide access to users to archived data that is retained in the system, within the established data retention timeframe, to be able to query them and generate reports.

DM43

The Contractor shall demonstrate through data analysis that the implementation outcomes have been validated and are accurate.

Data analysis and validation will be planned and performed across various phases of the project starting from Development, SIT, UAT, and production implementation. For each entity of data (files and file types) moved from the legacy system to Team CNSI's evoBrix PMIS solution, the following test process validations will be performed as part of the solution implementation to ensure we track and measure the implementation outcomes:

- Verify that all source data required to be moved into evoBrix tables have been populated and are accounted for in evoBrix. This includes both data loaded manually as well as data loaded through Extract-Transform-Load (ETL) data conversion jobs.
- Verify that any data transformations, translations, and edits were successfully completed as part of the data loading process. This verification ensures that the content of the data loaded from the legacy system to evoBrix has not been adversely impacted.
- Verify that the loaded data is accessible through evoBrix. This testing may be done using the evoBrix online application or, alternatively, through SQL queries of the evoBrix database if the data is inaccessible online. The purpose of this test is to verify that the loaded data can be retrieved, modified, and acted upon through evoBrix. Note that not all data loaded into evoBrix may be accessible through the graphic user interface (GUI). In such cases, queries will be executed to validate that the data has been transferred in its entirety and is accessible.

- Retrieve source data in legacy screens and corresponding converted data in the new evoBrix screens and validate that target data is correctly displayed.

DM45

The Contractor's solution shall maintain a history of provider information (i.e., full audit history or equivalent capabilities). All transactions, including the execution of database scripts, need to be recorded in the full audit history.

Team CNSI's Security Information and Event Management (SIEM) solution is built using the next-generation SIEM product "Alert Logic." This log management solution helps to meet compliance requirements and identifies security issues across the entire environment. It collects, processes, and analyzes the evoBrix data, and helps to unlock the insights hidden in the log data with 24x7x365 expert monitoring and analysis. Team CNSI's SIEM solution capabilities are highlighted below in Figure 3.10.1-104.

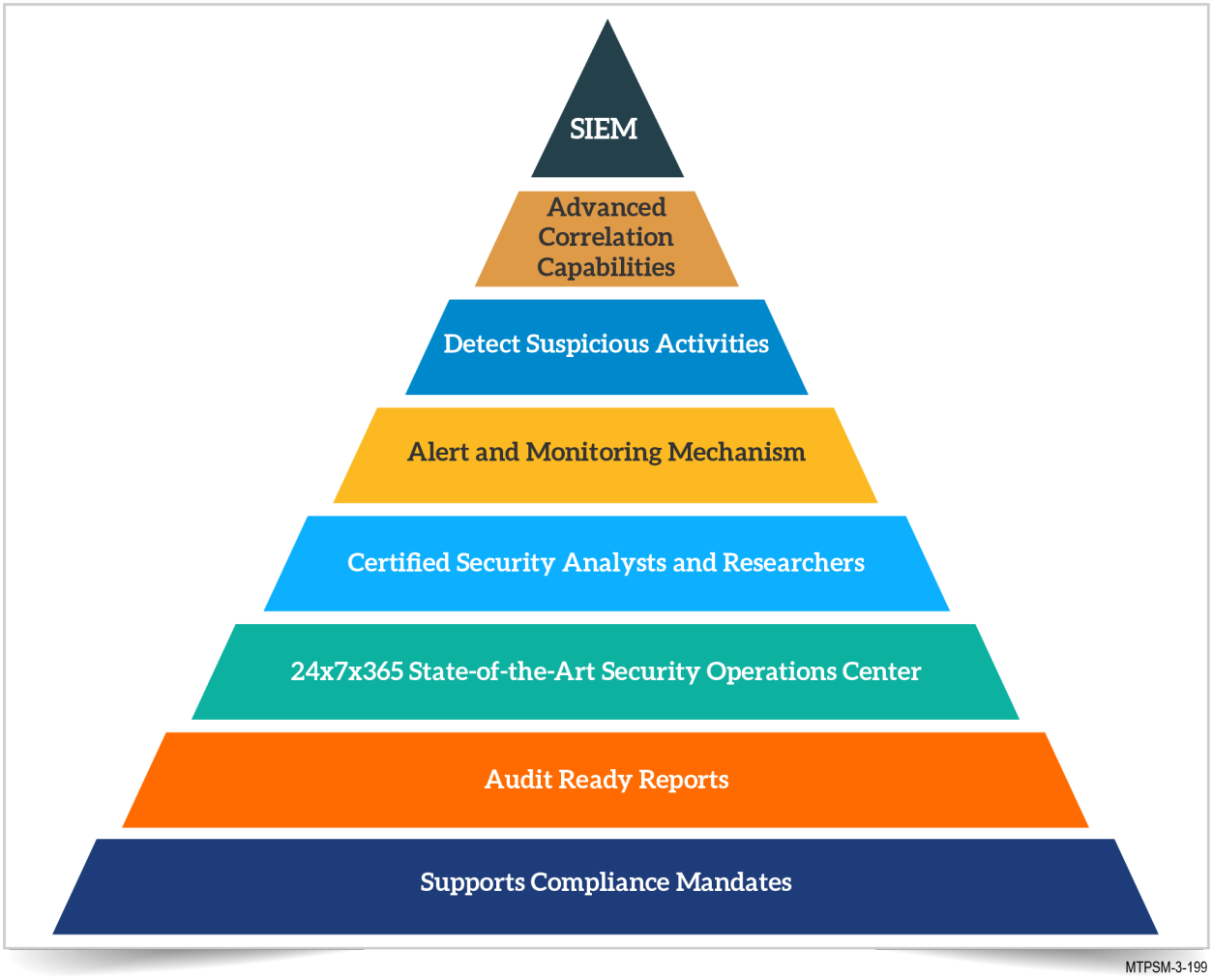


Figure 3.10.1-104. Audit History Support. Team CNSI's SIEM solution helps address audit compliance requirements by providing traceability to the history of provider information for MT PSM.

A key benefit of our approach is to enable a coherent audit trail of a user's movement within the system. This allows audit and security personnel to reconcile audit logs across systems and provide a complete picture of a user's activity. This approach also improves the overall state of system security and reduces complexity of user administration within the system by ensuring account synchronization, including user de-provisioning, across State resources. Auditing is enabled across the system and includes but is not limited to all changes to any application data. Audit reports are run at any time to assist auditors or investigators in determining who had what access to the system. Database auditing is based on CIS Benchmarks v2.1.0 and State-specific standards.

Based on large scale auditing needs refined through experience from managing multiple MMIS implementations, Team CNSI leverages an innovative CIS Audit Scan Tool that is setup to run across all the environments periodically and notifies respective teams to take necessary measures. The tool:

- Scans all the databases and operating systems (OS).
- Compares the results with CIS benchmarks.
- Creates a detailed HTML report with the results and findings. The detailed HTML report is categorized into two main sections:
  - Compliant. Compliant section shows the various aspects of the database and OS that are in line with CIS and State-specific security standards.
  - Non-Compliant. Non-Compliant section shows all the areas which are not compliant with the standards.

DM46

The Contractor shall develop and maintain a process to archive and access archived data (including legacy MMIS component data).

Team CNSI provides flexibility without bundling in complexity for data retention across the gamut of modules within Team CNSI's evoBrix PMIS solution by leveraging a combination of OLTP/SAN. The functional-area specific transaction data is archived based on retention policies specified by State. Transaction history is archived within the system in History/Detail tables. These can be accessed through the evoBrix application screens when required.

All active records and the supporting legacy and historical data, including legacy MMIS component data for an entity, that has been active within the last seven years will be retained. Data related to any entity that has been continuously inactive for seven years will not be retained. This data will be backed into tapes and purged from the evoBrix system.

The interface records are stored as files in SAN and will live in staging tables for a period of one month after receiving the file. Once data outlives its life cycle, it will be archived on State specified media (e.g., tapes, CDs) and made available for storage as appropriate. The requirements for data retention will be gathered during the design phase and the policies will be tailored specifically for the State.

DM47

The Contractor shall participate in ongoing data governance meetings as required by the Department.

Team CNSI has established data management strategies which are our basic governance processes to handle the complex set of systems and applications interfacing and interoperating with the MPATH program. This approach becomes even more relevant as the State defines and continues to refine the policies to adhere to changing regulations within the Medicaid landscape. This is primarily because the inculcation of additional data elements and reuse of existing elements for different purposes is a typical aspect of shifting business models. Drawing expertise from our successful approach for data governance in previous implementations, Team CNSI will play an active part in regular data governance meetings requested by MT DPHHS and assist the Department in:

- Defining Data Asset Owners: The initial step in the implementation of a data governance program involves defining the owners or custodians of the data assets in the enterprise. Team CNSI will use its existing best practices to establish clear guidelines regarding who is accountable for each aspect of the data, including accuracy, accessibility, consistency, completeness, and updates.

- Defining Data Access Processes: The second step in the approach is to define the data management processes. Team CNSI will document processes concerning how the data is to be stored, archived, backed up, and protected from mishaps, theft, or attack.

- Defining Data Control Procedures: The third step is to define, and put into place, a set of controls and audit procedures that ensure ongoing compliance with government regulations and industry best practices. Those practices include procedures governing physical transfers, firewalls, encryption, remote working, staff training, and general security, as well as schedules for regular monitoring of the above during the life of the contract.

DM51

The Contractor's solution shall provide the ability to modify transactions in real-time.

Team CNSI's evoBrix PMIS self-service portal provides secure access to the underlying data for a diverse user base including business and technical operations staff, providers, and the State. Multi-channel support and self-service capabilities for portal users ensure ease of access to data and empower business users to view and manipulate data in a more agile and efficient manner. They also allow for configuration of features for a personalized user experience. Team CNSI's evoBrix PMIS solution is aligned to ADA standards, with a user-centric design based on industry-standard usability principles for intuitiveness and ease of use. It offers a functionally rich set of features for handling application data to support engagement tools for enrollment, interactive communication, training, outreach, and ongoing collaboration with providers. The solution implements a rich user interface with a variety of self-service features for providers and business operations users. End users will have easy access to data and be provided with a complete view of all their interactions with the system and operations staff on a real-time basis; the solution also provides the ability to modify transactions in real-time to meet the operational and workflow requirements of the evoBrix PMIS solution to achieve the contractual service levels.

The evoBrix system, with its Service Oriented Architecture (SOA)-based integration engine, will seamlessly integrate data from other systems, external agencies, and business partners in the MT DPHHS enterprise environment. The Provider Enrollment and the broader PMIS within evoBrix enables MT DPHHS to manage the business processes involved end to end in provider enrollment and management balancing it with real-time data access and support. The evoBrix system provides multi-channel access to business data for user access and manipulation through web portals, other devices and channels.

Accessibility services are integrated with security services to ensure that only authorized users are provided with access to secured data.

DM52

The Contractor's solution must have the flexibility to quickly accept new and incremental data items from module components required by the ongoing component, product or service integration.

Team CNSI's evoBrix PMIS solution's adaptability and extensibility capabilities will allow MT DPHHS to add new functionality and modify existing functionality due to changes in policies, mandates, and business needs providing the necessary agility for the Medicaid enterprise. Key capabilities in this area include:

- Adaptability to business process changes via configurability by leveraging rules-based architecture utilizing our rules engine, RuleIT.
- Adaptation and extensions of business rules, via rules configurator and rule authoring tools.
- Automation of business processes via workflow services.
- Business process configurability and workflow management via workflow enablement tools.
- evoBrix Configurator supports configurability of business process variations and changes and extending business rules via meta-data driven design. Extensible Message Management for application and business messages.
- Configurable user interfaces and services.

The evoBrix solution is also scalable to accommodate any additional data elements introduced due to changes in existing processes, new functionalities, and new interfaces. The PMIS solution utilizes the concept of flexible (flex) fields in the applicable transaction tables to handle new element additions and customization, reducing the changes to the underlying code. Instead of defining the actual attributes and fields for certain tenant-specific business elements directly in a target entity, the flex-field provides logical placeholders. Team CNSI's evoBrix PMIS solution team will define what those flex fields should store based on MT PSM business needs (i.e., defining the meta-data details), whether they should be mandatory or optional, the formats/lengths/precision/scale, the default value (if any), and the order in which the flex fields are to be displayed. A flex-field table's sole purpose is to not only reuse it for multiple tenants/States for accommodating a specific business function depending on the tenant-specific usage, but to be able to provide support for future business needs for a given State without adversely impacting the underlying data structures that house the operational data.

Figure 3.10.1-105 shows a sample transactional entity, PROVIDER_DETAIL, with a "numeric" flex-field (FLEX_FIELD_NUM1) and the configuration of this flex field for storing an additional phone number for one tenant and the reuse of that same flex-field for storing an additional fax number for another tenant or potentially store additional data elements for future expansion within the MPATH Medicaid enterprise.

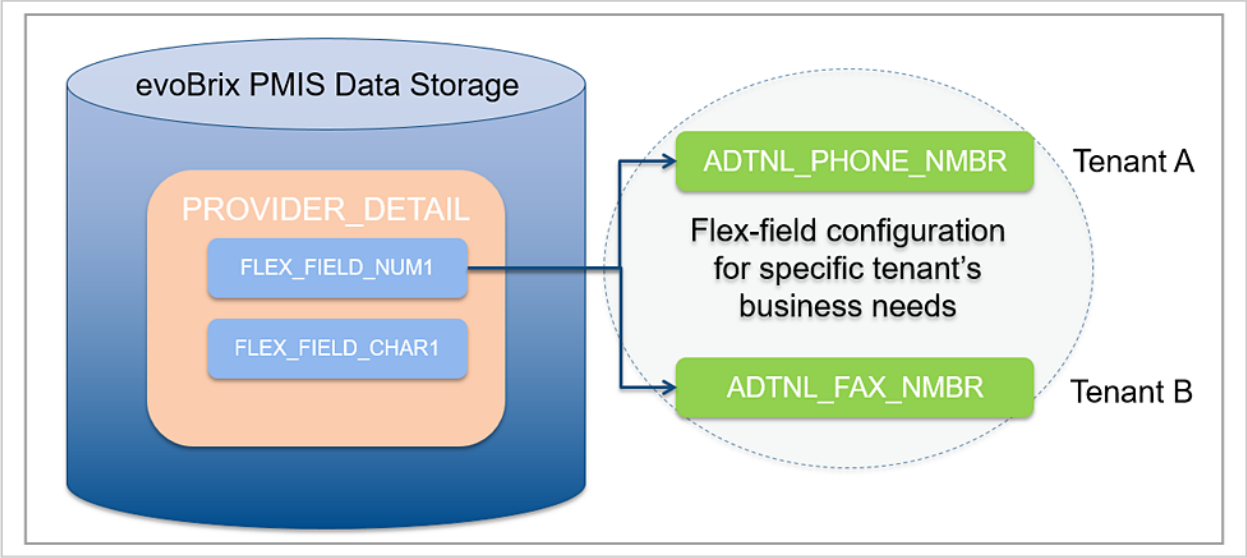


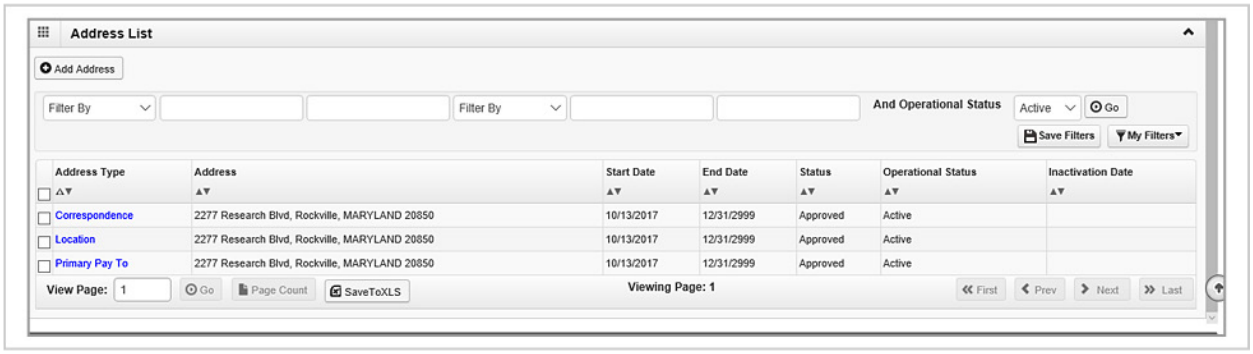
Figure 3.10.1-105. Support for Flex-fields. Team CNSI's evoBrix PMIS solution supports the use of flexible (flex) data fields to accept new and incremental data items from MT DPHHS module components without adversely affecting the operational system.

DM53

The Contractor's solution shall provide an address type, effective dates, and the ability to select the type of address for provider mailings.

Team CNSI's evoBrix PMIS solution accepts and validates all provider addresses through the Basic Information or Location screens during the enrollment process. The types of addresses accepted are dependent on the type of the provider enrolling into the evoBrix PMIS solution. All the addresses are then validated and standardized against the most current USPS address database using Pitney Bowes Spectrum Universal Addressing Module. The evoBrix PMIS solution supports different address types for provider mailings as shown in Figure 3.10.1-106. Some of the commonly used address types are listed below:

- Home Address
- Primary Practice Location address
- Service Location address
- Pay-to Address
- Correspondence Address
- Remittance Advice Address



MTPSM-3-386

Figure 3.10.1-106. Support for Different Address Types. Team CNSI's evoBrix PMIS solution supports an array of address types for provider mailings.

DM54

While the Department prefers real-time/event driven process, the Contractor shall provide a tool to easily administer and execute scheduled events (e.g. reports, file transfers, processes, notifications) to be performed on a regular basis (e.g. daily. weekly, monthly).

Team CNSI's evoBrix Integrator Services offers batch and near real-time data trading of interfaces between the evoBrix PMIS solution and the MT DPHHS approved trading partners. The solution transfers the Medicaid data required by the state-approved trading partners for the successful implementation of the business needs based on the roles. The solution supports inbound and outbound interfaces, service mediation, and pass-through (DB2DB) data exchange within evoBrix and with interface partners. The solution provides features for management of scheduling, auditing, error logging, and escalation along with detailed reporting on interface execution status, combined with notification modules to track execution of the various interface transactions. The ISR solution is based on a modular, scalable framework and will allow for current/future interfaces. The transactional data is sourced and made available to the evoBrix PMIS data mart on a near real-time basis through evoBrix Integrator. To reduce the management, technical stress, and the load on the evoBrix data repository, data trading can be done through batch processing on a scheduled basis. The framework also provides configurable screens to administer the various aspects of the interface and provides a dashboard for reporting the status of all the scheduled interfaces. Figure 3.10.1-107, Figure 3.10.1-108, and Figure 3.10.1-109 show sample evoBrix Interface configuration screens detailing the basic interface information, the interface transport details for exchanging the interface data to external systems, and interface run details.

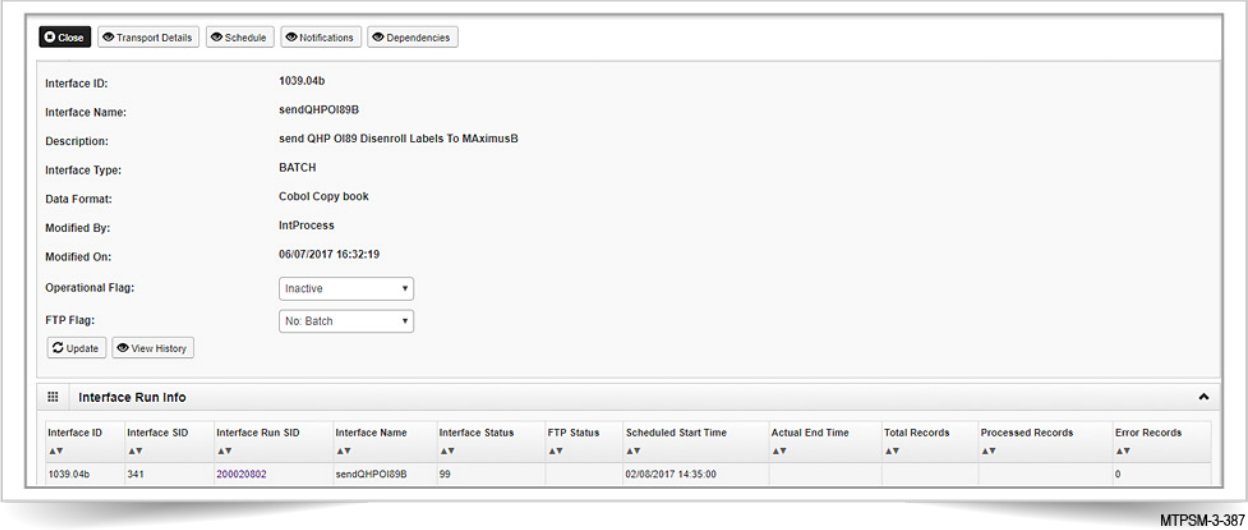


Figure 3.10.1-107. Basic Interface Information Screen. Team CNSI's ISR solution provides configurable screens to view the basic details of an interface.

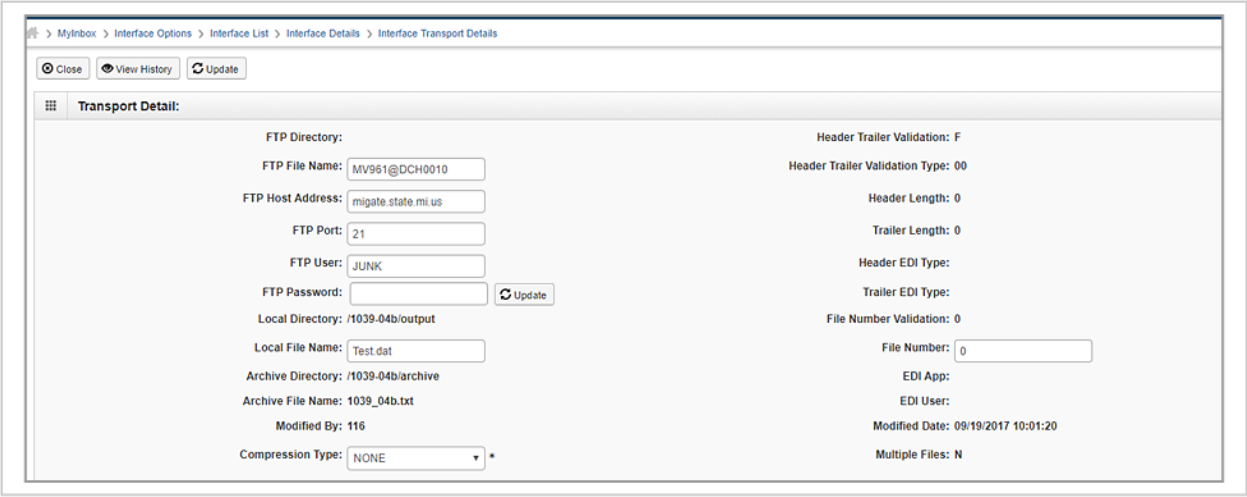
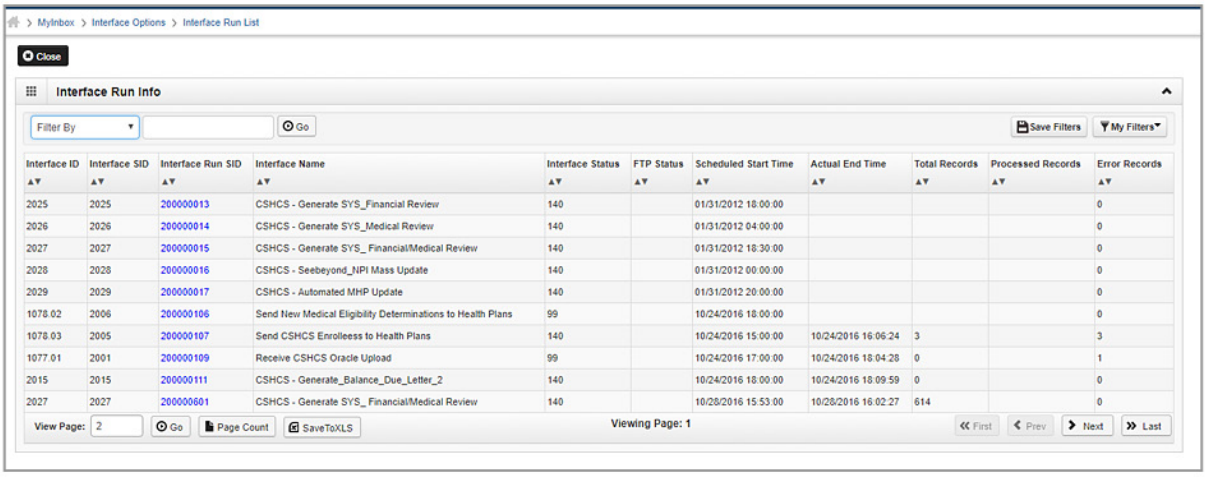


Figure 3.10.1-108. Interface Transport Details Screen. Team CNSI's ISR solution provides configurable screens to view the transport details of an interface to support the exchange of data with external systems within MT DPHHS.



MTPSM-3-424

Figure 3.10.1-109. Interface Run Details Screen. Team CNSI's ISR solution provides configurable screens to view the different interface run details of an interface over a specific period along with the supporting statistics such as the completion status, total records, processed records, and error records.

DM55

The Contractor shall provide a conceptual data model (CDM) that identifies the data elements required for an end-to-end business process execution including the identification of data standards that will reduce future rework to achieve successful data sharing across the enterprise and for intrastate/interstate exchanges. The CDM is required to be used as a reference to provide high-level overview of the data and relationships used by the enterprise and to provide a tool for ensuring the completeness of the business model.

Team CNSI's evoBrix PMIS solution has an established conceptual data model that addresses the data needs of enterprise wide Medicaid operations. The evoBrix solution has the Conceptual Data Model (CDM) for all business areas of a Medicaid System. The model conceptually groups all business areas into one big product. It has evolved over multiple versions and represents universal data needs across multiple States. The CDM is a pictorial representation of various functional requirements independent of database management systems. It provides in-depth details of various entities and how they relate with other entities irrespective of how they are implemented in the backend. Figure 3.10.1-110 shows a sample conceptual data model for a subset of the evoBrix solution's Provider Enrollment business area.

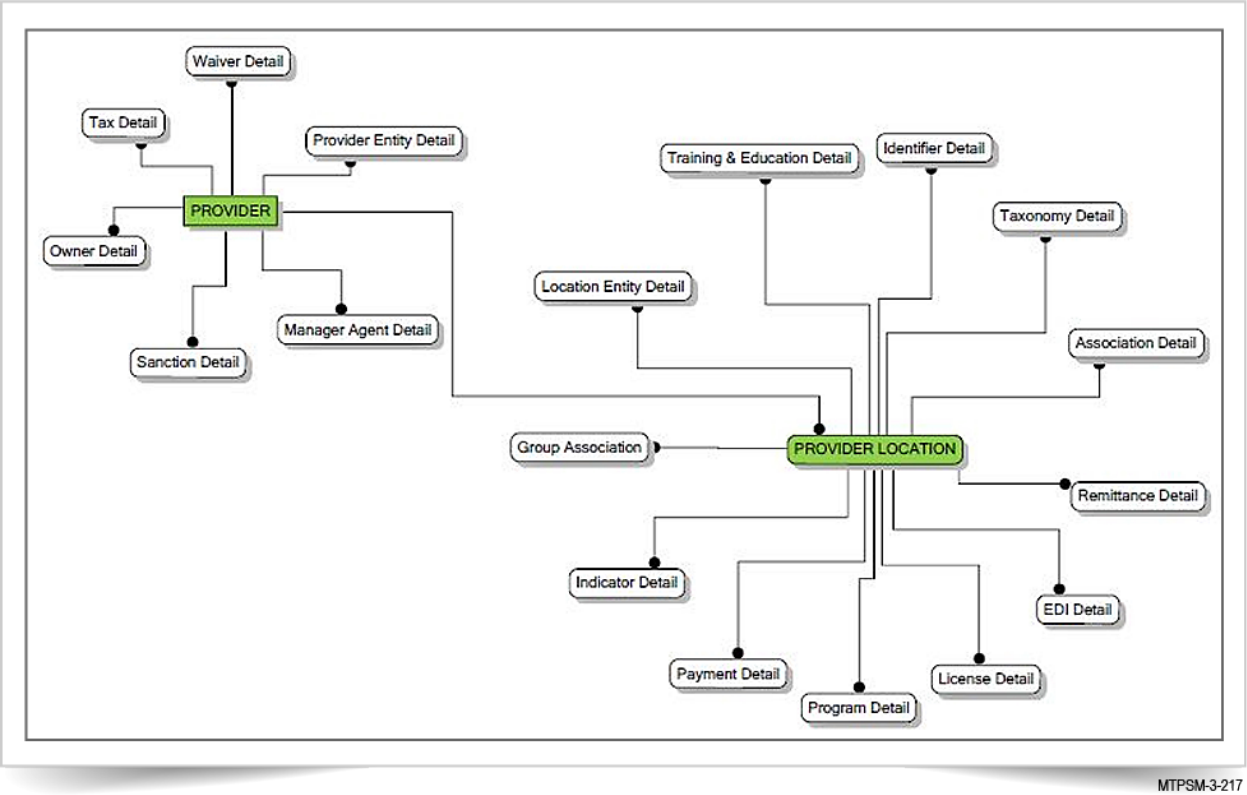


Figure 3.10.1-110. evoBrix Provider Enrollment – Conceptual Data Model. The evoBrix Conceptual data model was designed and refined using the best practices learned from MMIS implementations across multiple tenants.

The evoBrix conceptual data model is designed based upon Object Relational Model (ORM) techniques, i.e., use of types and subtypes to define entities at an abstract level. The model was designed using the following processes based on best practices learned from MMIS implementations across multiple States:

- Define New Entities
- Identify Supertypes and Subtypes
- Define Entity Relationships
- Determine Primary Identifiers

The evoBrix conceptual data model comprises of the following components:

- Subject Area – Conceptual grouping of entities based on functional specifications
- Entity - A thing capable of an independent existence that can be uniquely identified

The evoBrix conceptual data model consists of the following types of entities:

- Master Entity
- Operational Entity
- Transactional Entity
- Relationship – A conceptual connection based on interaction among entities

DM57

The Contractor shall standardize the structure and visibility of data and applications to support automated electronic data exchanges within the State's enterprise to promote interoperability.

Team CNSI's evoBrix Interface framework features an extensive list of interoperability protocols including SOA/Standards-based integration approaches using protocols including REST, SOAP, and commercial off-the-shelf (COTS) Application Programming Interface (API). Team CNSI's evoBrix solution's core architecture leverages the ESB features within the SOA framework to integrate disparate systems effectively. This architecture provides an integration backbone that connects core applications and services without directly accessing the underlying systems and at the same time supports electronic data exchanges within the State's enterprise to promote interoperability.

- Support for standard content formats such as documents, eXtensible Markup Language (XML), JavaScript Object Notation (JSON), EDI for user, and machine-readable and understandable content.
- REST APIs leveraging Swagger specifications for producing, consuming, and visualizing APIs to support service inquiries.
- SOAP APIs leveraging Web Service Definition Language (WSDL) specifications for data exchange with business partners for post services.
- COTS APIs expose COTS functionality as internal and external interfaces through standard APIs. Examples include Document Management API, Workflow API, Correspondence API, and Siebel API.
- EDI gateway support for standards-based information exchange for EDI transactions (e.g., HIPAA ANSI X12 standards). Support for secure FTP gateway and compliance with CORE rules.
- File-based information exchange for standard and non-standard file based integration.
- Secure information exchange using API keys, web service security 1.0 standards, and other security protocols for ensuring data during transit.

Team CNSI's evoBrix PMIS solution's accessor provides user communication through web based and mobile enabled portals such as provider portal, consumer portal and worker portal. The solution is modular by nature and rapid adoption to change is accommodated by versioning through the mediation layer.

DM58

The Contractor's solution shall maintain online access to at least four (4) years of selected management reports and five (5) years of annual reports.

Team CNSI's Reporting solution facilitates archival of pre-built and scheduled report outputs into IBM Cognos BI Content Store. Team CNSI's evoBrix PMIS solution will maintain online access to at least four years of selected management reports and five years of annual reports. The data retention period for the different types of operational, management, and annual reports, as it applies to evoBrix PMIS, can be configured per pre-defined retention policies. Please refer to section 3.10.15 for more details on Team CNSI's Reporting Solution.

DM60

The Contractor shall be responsible for data management including ensuring the architecture addresses data semantics, data harmonization, and shared-data ownership.

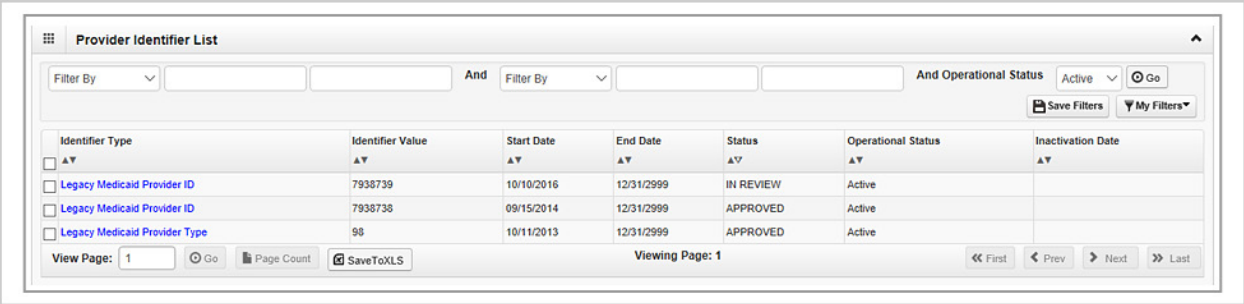
Team CNSI understands the data needs and dependencies of a successful MMIS system based on the experience of designing and operating similar systems for multiple States that are currently operational. Team CNSI's evoBrix PMIS solution is designed with a sound data design and provisioning strategy, as it is not only a key aspect for managing the current and future needs of MT DPHHS, but also one of the vital elements of an extensible, interoperable infrastructure. We understand that the MT DPHHS's MMIS system has a dependency on varying datasets such as Provider, Eligibility, Reference/Lookup, Claims, Payments, and TPL for managing the technical and operational needs of the existing system. Team CNSI's evoBrix PMIS solution has the means to support all dependent datasets, both from internal and external sources, orchestrated through a robust enterprise-grade relational data model, to facilitate a seamless transition of MT DPHHS's existing Provider Enrollment system to the new solution.

Team CNSI's evoBrix platform's underlying data models have evolved over multiple iterations and not only represent a harmonization of data needs across multiple States but are also specifically designed to cater to the data design needs of enterprise-wide Medicaid operations. The solution has taken a layered approach to addressing the process and data needs by balancing the normalization needs of a data model with the performance needs of large-volume transaction processing systems. The data model is layered into the Medicaid foundation entities and transactional entities. This approach allows for a more coherent data management and provides better data integrity handling at the database layer. The data model is very flexible and provides the business agility to accommodate state policy changes, such as supporting different health care programs. The overarching goal of Team CNSI's evoBrix PMIS solution is not only to facilitate smooth exchange of data for day-to-day business operations but also to ensure that the solution does justice as the "system of record" for addressing the operational demands within the MPATH Medicaid enterprise to realize MT DPHHS's vision of shared-data ownership.

DM62

The Contractor's solution will ensure current and historical provider IDs are linked back to one universal/common identifier.

Team CNSI's evoBrix PMIS solution ensures that the provider's historical and current identifiers are linked to a single master record. Even if multiple identifiers are associated with a Provider, Team CNSI's evoBrix PMIS solution retains the information under a single enrollment and a unique Provider Identifier (Provider ID) that is in turn linked to the provider's NPI and TIN. Figure 3.10.1-111 shows the different identifiers that are tied to a unique provider ID that can be tracked through the evoBrix Provider Identifier List screen.



MTPSM-3-388

Figure 3.10.1-111. Support for Multiple Provider Identifiers. Team CNSI's evoBrix PMIS solution supports multiple alternative identifiers, both current and historical, to link all the records related to a provider that is identified via a unique evoBrix Provider ID.

DM63

The Contractor's solution shall assign standardized unique internal identifiers for entities and prevent the creation of duplicate records.

Team CNSI's evoBrix PMIS solution has the ability to identify, track, and report individual providers across multiple application types. When multiple identifiers for the same provider are fed into the system through various sources, the evoBrix PMIS solution identifies the duplicates and ensures that there is always a unique set of active identifiers for a provider stored under a unique Provider Identifier linked with the provider's NPI and TIN.

Team CNSI's evoBrix PMIS solution performs the following validations to ensure data integrity before the provider data can be accepted and stored in the system:

- NPI Validation: The solution verifies the user input NPI against the National Plan and Provider Enumeration System (NPPES) database to make sure the NPI, provider name, and provider entity type entered match the data registered with the NPPES system.
- Duplicate Check: The solution verifies the input against the enrolled providers in the system to ensure that the NPI is not already associated with a previously enrolled provider.
- Duplicate Record Check: The solution has validations in place to restrict modification of the same information, by the provider and authorized State staff, at the same time.

An appropriate error message is displayed to the user during the enrollment process if any of the above validations fail.

DM64

The Contractor shall be responsible for backup and retention of data to include:

1. Daily incremental backups with retention of sixty-one (61) days.
2. Weekly incremental backups with retention of twelve (12) weeks.
3. Monthly full backups with retention of eighteen (18) months.
4. Annual full backups with retention of seven (7) years.

Team CNSI use the latest possible version of Oracle database and associated tools to manage the databases and their backups. Starting with Oracle 11g there are many enhancements for back-up and recovery features available for Oracle databases. RMAN is used to configure and backup the Oracle databases along with third-party tools for placement on external media. Oracle RMAN backup strategy will be incremental in nature thereby saving storage costs without compromising on recovery or recovery timelines. There are many ways Team CNSI employs to perform the backup and recovery.

- Script based backups:
  A backup script is setup and scheduled to run multiple times in a day to maintain consistent backups to be used for recoveries whenever needed.

- OEM based backups:
  Using Oracle Enterprise Manager (OEM), Team CNSI configures RMAN to perform full online backups weekly to external disk-based storage systems (or as per final State requirements, if different). Team CNSI also uses OEM to configure RMAN to perform daily incremental backups to external disk-based storage systems.

Additional features of RMAN help to keep up the backup/restore performance and realize storage savings without compromising on the security by enabling encryption.

- RMAN uses binary compression algorithm as it writes data to backup sets. This binary compression algorithm can greatly reduce the space required for disk backup storage which is typically around 2x to 4x based on the selected compression level that BASIC, LOW, MEDIUM and HIGH.

Team CNSI will maintain the following SLAs, shown in Figure 3.10.1-112, while preparing and executing the backup strategy.

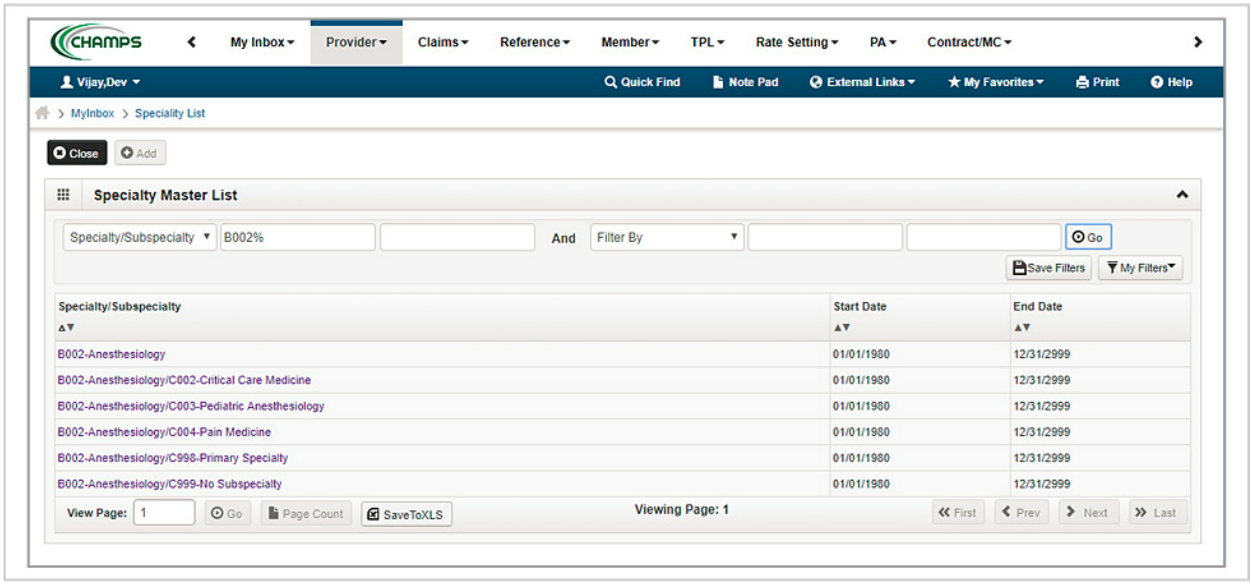
Backup Type	Retention
Daily incremental backups	61 days
Weekly incremental backups	12 weeks
Monthly full backups	18 months
Annual full backups	7 years

Figure 3.10.1-112. Backup and Retention Schedule. Team CNSI's compliance to the State-mandated backup and retention schedule for the evoBrix PMIS solution.

DM69

The Contractor's solution shall maintain online access to all reference tables with an option to search and display by reference data type and code.

Team CNSI's evoBrix PMIS solution provides the ability to maintain master/reference data such as provider types, enrollment types, address types, license certification types, specialties, and subspecialties. An authorized user can search and maintain the master data through interactive, online screens. Figure 3.10.1-113 shows the evoBrix PMIS Specialty Master List application screen that provides support for searching specialties by code.



MTPSM-3-389

Figure 3.10.1-113. Provider Specialty Online Maintenance Screen. Team CNSI's evoBrix PMIS solution supports online access to reference data with the ability to view, search and display data.

DM70

The Contractor's solution shall maintain user controlled parameters for all standards and messages.

Team CNSI's evoBrix PMIS solution uses a generic model framework referred to as Message Management Framework (MMF) to maintain and interact with application to generate messages and correspondences. MMF addresses the need to streamline application and system messaging by following a universal framework across various modules in Team CNSI's evoBrix PMIS solution. This is a multi-tenant, multi-language compliant framework that dynamically builds messages based on configurable pre-defined parameters stored in the MMF configuration data mart. This approach helps messages and parameters to be easily configured without having to alter the program code. Figure 3.10.1-114 shows the nomenclature that is used to drive the configuration of messages in the evoBrix PMIS solution using the Message Management Framework.

Various message categories are handled by MMF including, but not limited to:

- Application Message - Warning/errors related to the application screens or operations
  - Services Validation Message
  - Persistence Validation Message
  - Message Encrypt Validation Message
- Security Message - Authentication/ unauthorized access related messages
  - Authentication Validation Message
  - Application Access Validation Message
  - Unauthorized Access Validation Message

- Validation Message - Any generic validation that doesn't conform to a specific function
  - Tenant Validation Message
  - Login Validation Message
- Other Generic Messages

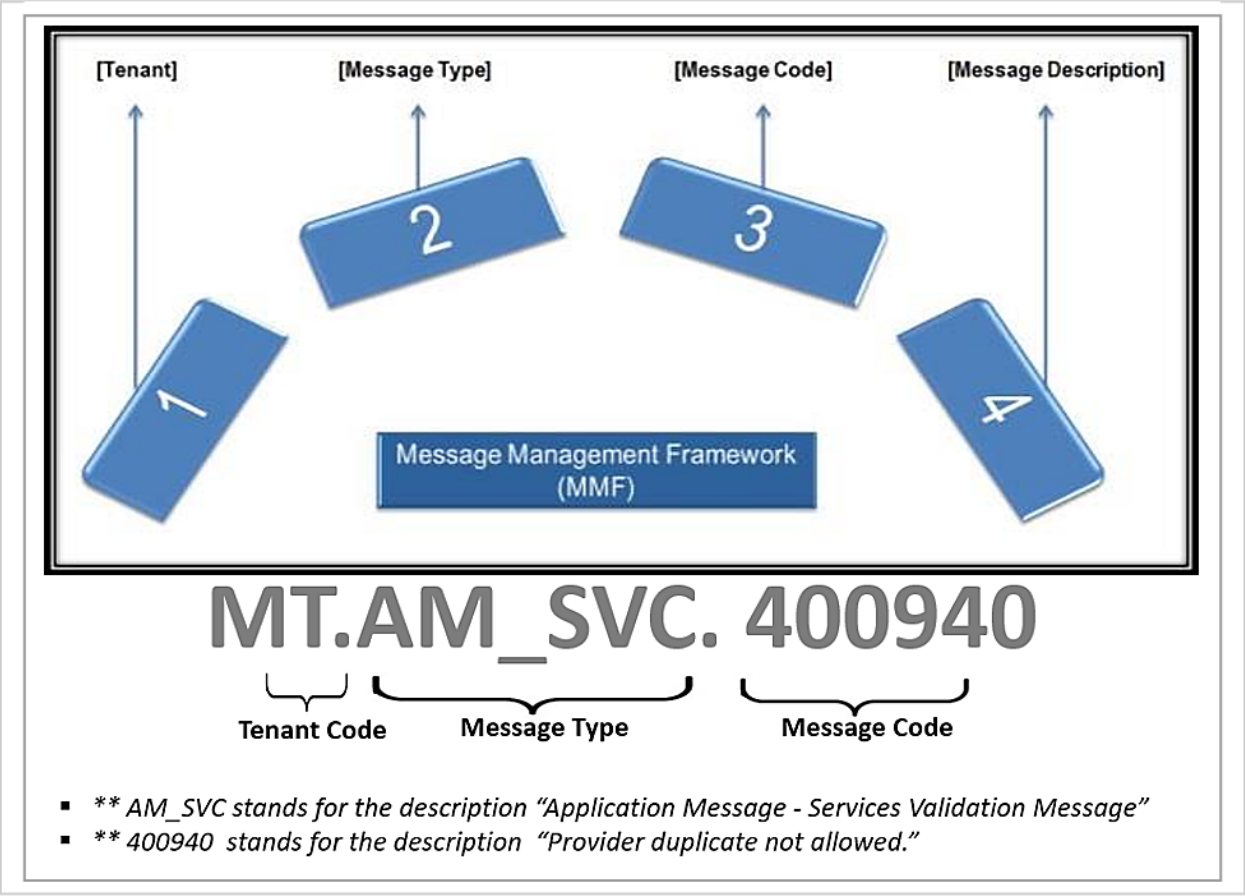


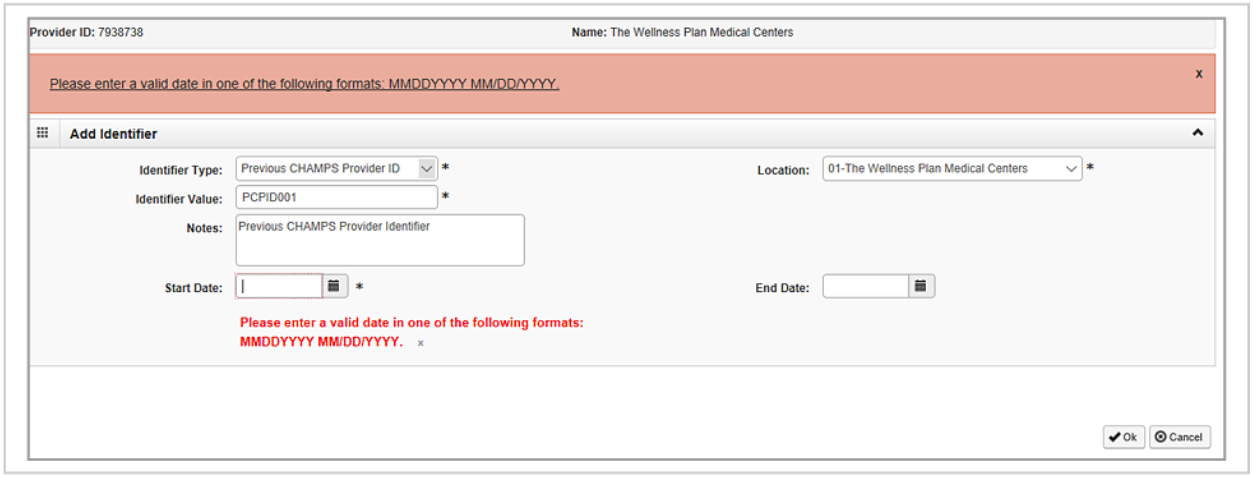
Figure 3.10.1-114. Message Management Framework. Team CNSI evoBrix Message Management Framework (MMF) supports the configuration of messages in the PMIS solution.

DM71

The Contractor's solution shall verify that all dates are valid and reasonable.

Team CNSI's evoBrix PMIS solution provides an application portal to let business operations users manage day-to-day operations. The application screens are powered by a robust framework that ensures that all date values entered by users are validated for correct date formats and values. The date validations consider the business context of the data being keyed in and provide meaningful messages to the user to take corrective actions should it be invalid. For example, should a user enter a date in an invalid format that is not permitted by the solution, the user would be presented with a standardized message to take corrective action before any further actions can be taken on the screen; if the user enters a date that is part of a date range/span, the system will validate whether the begin date is prior to or equal to the end date

and prompt the user for an action should it fail the date range check. Figure 3.10.1-115 shows the evoBrix PMIS application screen that enforces comprehensive validation of date formats/values.



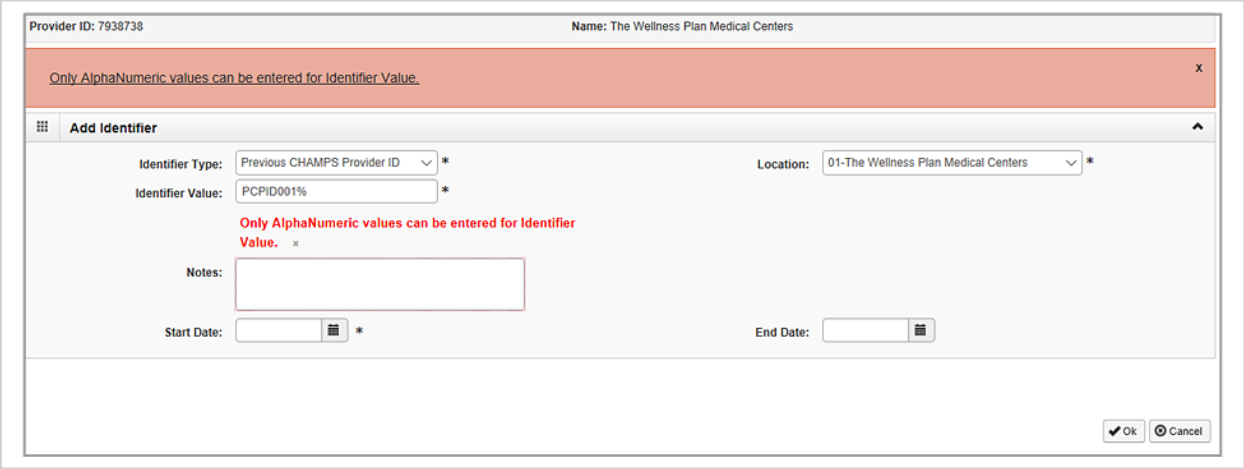
MTPSM-3-392

Figure 3.10.1-115. Validations for Date Format/Value. Team CNSI's evoBrix PMIS solution supports comprehensive validation for date formats and values prompting users to take corrective action on the application screens.

DM72

The Contractor's solution shall provide proper data validation rules (e.g., all fields defined as alphabetic contain only alphabetic data, fields defined as numeric contain only numeric data, items with definitive upper and/or lower bounds are within the proper range).

The application portal for Team CNSI's evoBrix PMIS solution lets business operations users manage day-to-day operations. The robust framework that powers the application screens ensures that all values entered by users are validated for correct data types. The data type validations consider the business context of the data being keyed in and provide meaningful messages to the user to take corrective actions should it be invalid. For example, should a user enter a special character into an alphanumeric field, it is rejected by the screen and the user would be presented with a standardized message to take corrective action before any further actions can be taken. If the user enters a value that is part of a range, the system will validate whether the values fall within the permitted range of upper and lower bounds and the 'From' data value is lesser to or equal to the 'To' data value and prompt the user for an action should it fail the data range check. Figure 3.10.1-116 shows the evoBrix PMIS application screen that enforces comprehensive validation for data fields supporting alphanumeric data.



MTPSM-3-393

Figure 3.10.1-116. Data Validations for Alphanumeric Data Fields. Team CNSI's evoBrix PMIS solution supports comprehensive validation for data fields containing alphanumeric data prompting users to take corrective action on the application screens.

DM73

The Contractor's solution shall capture and maintain the data items needed for State or Federal reporting requirements.

Team CNSI's evoBrix PMIS solution supports State and Federal reporting functions as defined by CMS and the State. The evoBrix solution has a pre-defined set of State specific standard reports as part of the evoBrix PMIS solution. A case in point is Team CNSI's expertise with Transformed Medicaid Statistical Information System (TMSIS) extracts and the related implementations in the states of Utah and Washington that will reduce risks to meet the TMSIS requirements specifically as it applies to the data elements for PMIS that are required for the TMSIS data extracts to be sent to MT DPHHS for submission to CMS. The majority of the TMSIS data elements can be directly mapped from the evoBrix data model and, for any State-specific customizations, through configurable transformation rules that would be leveraged seamlessly while extracting the data.

DM74

The Contractor's solution shall validate calculated data items.

Team CNSI's evoBrix PMIS solution will leverage the generic data validation framework orchestrated through reusable components that applies to the various modes of accessing the data – frontend, backend, interfaces, web services – which ensures that a consistent and streamlined outcome is produced for calculated data items. The evoBrix solution employs different test cases to validate the accuracy of calculated fields. Various levels of testing are performed based on the test cases to make sure the calculations are performed as intended by the business process. The test cases are executed as part of application validation as well as backend code validation processes to make sure all calculated field values are accurate.

Team CNSI's evoBrix PMIS solution ensures that all calculated values are validated. The data validations consider the business context of the data being calculated and provide meaningful error messages to the user to take corrective actions should there be any data issues. For example, should a calculated data

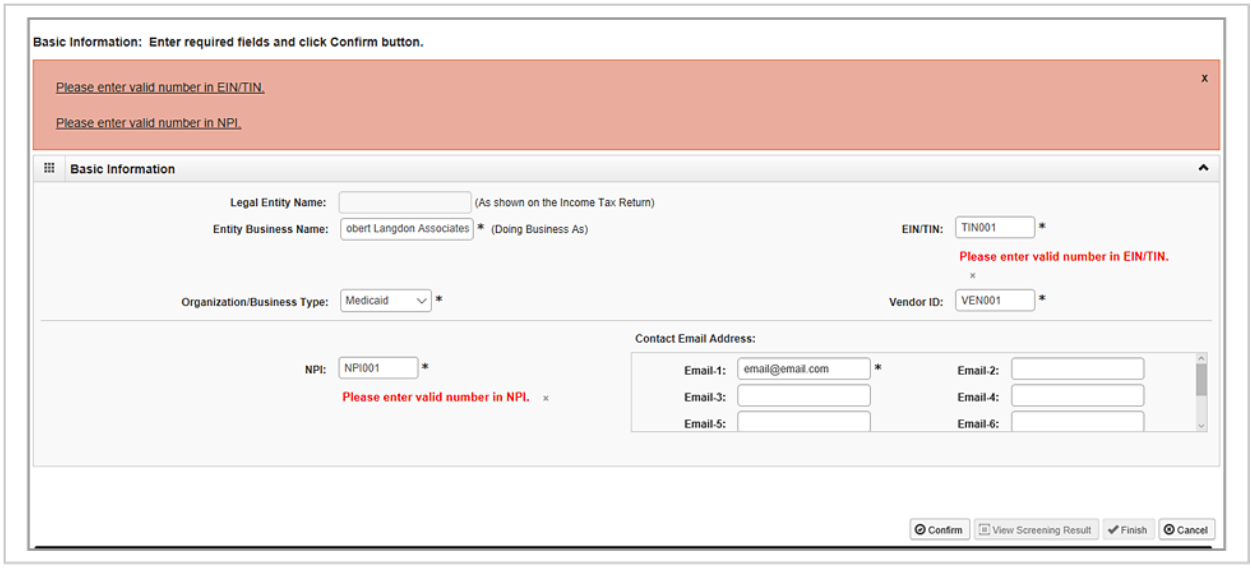
return an invalid value, it is rejected by the screen and the user would be presented with a standardized message to take corrective action before any further calculations can be performed.

DM75

The Contractor's solution shall validate, and/or verify that all data items that contain self-checking digits (e.g., National Provider Identifier) passes a specified check-digit test.

Team CNSI's evoBrix PMIS solution supports an interactive enrollment application that provides structured, online screens with a Business Process Wizard (BPW) for provider enrollment. The wizard guides the provider step-by-step through the enrollment process and provides real-time field level edits, including data format checks such as check-digit test, on each screen that greatly reduces key-in errors. The wizard also displays applicable validation error messages throughout the data entry process. Figure 3.10.1-117 shows the evoBrix PMIS application screen that validates the NPI and prompts the user to correct the value should the keyed in value be of the wrong format that doesn't comply with the check-digit test.

The evoBrix PMIS solution validates and ensures all the required enrollment steps are completed before accepting final submission of the enrollment application. This prevents providers from submitting incomplete applications or applications with incorrect data.



MTPSM-3-397

Figure 3.10.1-117. Validations for Fields with Check-digit Test. Team CNSI's evoBrix PMIS solution supports comprehensive check-digit validation for data fields such as National Provider Identifier prompting users to take corrective action on the application screens.

DM79

The Contractor's solution shall support the Extract, Transform and Load (ETL) processes from real-time web services or batch processes.

Team CNSI understands the need for enabling an efficient, secure, and scalable integration framework, resulting in the consolidation of different disparate systems as required by MT DPHHS business areas. Team CNSI's integration framework is comprised of the below components to integrate the systems with other information systems leveraging the applicable ETL processes, as needed:

- Batch Interfaces via ISR
- Web services via evoBrix integrator

Batch Interfaces via ISR

Team CNSI's evoBrix ISR configurable solution supports automated data exchanges with MT DPHHS and MT DPHHS-approved agencies. The evoBrix ISR solution uses an enterprise class service bus (Oracle SOA Suite) as the core orchestration tool of business processes across the different applications that support Medicaid operations. The framework supports inbound and outbound interfaces and pass-through data exchange within evoBrix and with interface partners. The framework provides features for management of scheduling, auditing, error logging, and escalation along with detailed reporting on interface execution status, combined with notification modules to track execution of the various interface transactions.

Here are the key features of the ISR solution:

- ISR supports the data exchanges between MT DPHHS and MT DPHHS approved trading partners by adding the required configurations.
- ISR solution handles all industry standard file formats.
- Interface schedules, validations, error thresholds, external agency details, email alerts for MT DPHHS interfaces can be configured in ISR.
- This framework can scale for growth in data volumes and transaction volumes seamlessly and take advantage of the rich features of the underlying hardware and software resources.
- ISR solution is built on scalable and high available infrastructure.
- ISR solution has robust error logging and auditing features. When processing MT DPHHS interfaces, errors are logged and the details can be sent to the approved email IDs for further correction.
- ISR supports modular approach by plug and play of generic code. MT DPHHS related interfaces can be configured easily.
- ISR is capable of handling large payloads with failover cluster.
- ISR solution enables seamless and simplified connectivity with external agencies using Secure File Transfer and SSL.

Team CNSI's evoBrix ISR framework can be leveraged to integrate MT DPHHS and the external approved federal and state agencies and other authorized trading partners. Data can be transmitted via batch or real-time web services to exchange license information, Provider Credentialing Service information, Enrollment information from MCOs, and any other required information as part of evoBrix PMIS solution. The ISR solution supports secure data exchanges using available standards in the industry such as SFTP, FTPS, and SSL.

Web Services via evoBrix Integrator

Team CNSI's evoBrix Integrator solution uses ESB features within the SOA framework to integrate disparate systems effectively. This solution provides an integration backbone that connects core applications and services without directly accessing underlying systems. The evoBrix integrator solution is based on leveraging a series of COTS products that use a services-based integration platform. The evoBrix integrator solution leverages Oracle Service Bus for Service mediation for real-time web

services. It supports robust authorization, authentication and validation features using Oracle Service Bus. The solution is capable of handling common industry standard service requests such as SOAP and REST. Also, evoBrix integrator can change the various attributes of the service without impacting existing clients. The solution will allow Core MMIS to avoid point-to-point communication between different system components and will streamline flow of all information throughout the MPATH Medicaid enterprise. The key features of evoBrix Integrator include:

- Leverage light weight Oracle Service Bus built on SOA and SCA principles
- Ability to change the various attributes of the service without impacting existing clients
- Supports multi tenancy with easy configurable modules
- Robust authorization, authentication, and validation features
- Dynamic routing capability
- End-to-end instance tracking with state and error information
- Streamlines business process exception handling
- High availability and scalability of the digitized platform
- Capable of handling common industry standard service requests
- Handles asynchronous callbacks reliably
- Structured conversational interactions with other systems and trading partners

3.10.1.6 Interfaces

This section addresses interface requirements for the Contractor's solution(s) and operations. The Contractor's Application Program Interfaces (APIs) and components must comply with industry standards (e.g., National Information Exchange Model (NIEM), National Institute of Standards and Technology (NIST) and HIPAA compliance standards). In the response, the Offeror must describe current methods of electronic data exchange, detail the industry standard formats currently used and describe any proprietary formats used. The Offer must also describe their approach to meet each of the interface requirements detailed in Attachment F, Requirements Matrix.

Team CNSI understands the need for enabling an efficient, secure, and scalable transmittal of data, and consolidation of different disparate systems as required by MMIS business areas, as the core of Montana Provider Services Module (MT PSM) integration strategy. Team CNSI's evoBrix configurable Interface Service Repository (ISR) solution, as illustrated in Figure 3.10.1-118, can handle MT PSM integration for transmittal of data for different systems via MT PSM System Integration Services. ISR solution will be used to interface with the state and all state approved trading partners including Managed Care Organizations (MCO), integrate with state agency program areas for enrollment process and configure the interface details for any future needs as part of evoBrix Provider Management Information System (PMIS) implementation.

The Team CNSI Advantage

Team CNSI brings our proven evoBrix platform to support the MT PSM solution in handling interface requirements and operations for electronic data exchanges between MT PSM and the approved external agencies.

- Interface Service Repository (ISR) supports data exchanges with agencies and trading partners and supports industry standard file formats
- ISR is facilitated by Oracle SOA Suite and supports modular approach by plug and play of generic code
- Configurable interface schedules, error thresholds, validations, email alerts, and robust error logging and auditing features
- Dynamic routing capability feature supports multi tenancy with easy configurable modules
- Faster integration with code reusability which results in increased productivity
- Capable of handling large payloads with failover cluster and end-to-end instance tracking with state and error information

MTPSM-3-251



Team CNSI's evoBrix ISR solution uses an enterprise class service bus (Oracle SOA Suite) as the core orchestration tool of business processes across the different applications that support Medicaid operations. Here are the key features of evoBrix ISR solution.

Managing File Exchanges through Configurations:

Team CNSI's evoBrix ISR solution was developed from the ground up to manage numerous types of data exchanges typical of every MMIS implementation. The framework supports inbound and outbound interfaces, service mediation, and pass-through data exchanges within evoBrix PMIS and DPHHS approved agencies. To facilitate administration, the solution provides features for management of scheduling, auditing, error logging, and escalation along with detailed reporting on interface execution status, combined with notification modules to track execution of the various interface transactions. The current ISR solution is based on a modular and scalable framework, and will allow for any new interfaces within evoBrix PMIS.

Alignment to Industry Standards:

Team CNSI continues to participate in MITA, HL7 standards, and other standards-related forums to promote and adopt standards. The evoBrix platform is aligned to industry standards, including the following key components:

- Data Standards
  - HIPAA X12 standards for EDI transactions and code sets such as ICD10
  - Compliance to CORE Rules and NCPDP data standards

- Interoperability Standards
  - Swagger and WSDL SOAP specifications for web services
  - SOA architecture standards
  - Web service security standards (1.0) for web services security
- Web/Usability Standards
  - W3C Standards
  - ADA guidelines
- Compliance to security, privacy, and data standards
- Alignment to MITA standards
- Adherence to CMS' Seven Standards and Conditions

Monitoring and Alerting:

Team CNSI's evoBrix ISR solution also implements a comprehensive escalation feature to alert multiple levels of event subscribers. For example, if an inbound interface file related to licensing is arriving late, the system will alert the system operations staff and if subsequently the file never arrives, the system will alert business users. The system will also report unsuccessful file transfers and uploads to the DPHHS approved agencies, and confirm successful file transfers and uploads. The solution also provides configurable screens to administer the various aspects of the MT PSM interface operations and provides a dashboard for reporting the status of all the scheduled interfaces. After processing credentialing information, provider data and license information with approved agencies, email notifications will be sent to the configured personnel on the status of the interfaces, including audit details of the interface.

File Transfers and Security:

Team CNSI's evoBrix ISR solution is architected using secure transport methods to provide secure and protected data communication that maintains confidentiality and integrity of data within MMIS systems. Extract files will be produced using the ISR solution powered by Oracle SOA Suite. File layout will be defined during the design session with inputs from DPHHS, based on vendor requirements, in the adhered standard. Data exchange and file transmission is handled by ISR in a secure manner with external entities using secure file transfer protocol (SFTP), FTPS, or SSL. The solution can support other types of file transfers available in the industry. File transfer status (successfully transferred or failed) is available in the email notification generated after the completion of an interface by ISR solution. Team CNSI evoBrix solution supports EDI files, flat file with fixed length, flat files with delimiters, XLS, and other proprietary file formats.

Team CNSI's ISR solution is built on a multi-layered security approach that protects the backend client data from unauthorized access. Team CNSI perform annual audits to comply and achieve certification with Statements on Standards for Attestation Engagements/Service Organization Control (SSAE/SOC) and HIPAA standards. All these certifications will remain in place for the duration of the contract and Team CNSI can provide most recent version of compliance certificates and audit reports. The following certifications are in place to provide for the confidentiality, integrity, and availability of the information systems:

- SSAE 16 SOC 1 Type II
- SSAE 16 SOC 2 Type II
- HIPAA/HITECH/FedRAMP

Additionally, Team CNSI's evoBrix ISR solution includes security and privacy controls that are compliant with the most current version of the CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E) and National Institute of Standards and Technology (NIST) standards. Team CNSI's evoBrix PMIS solution adheres to the following security standards:

- Federal Information Security Management Act (FISMA)
- Internal Revenue System (IRS) Publication 1075
- Patient Protection and Affordable Care Act (PPACA) or (ACA)
- NIST Special Publication 800-66 Revision 1
- NIST Special Publications 800-53 and 800-53A
- NIST Special Publication 800-47
- NIST Special Publication 800-88 Revision 1
- NIST Special Publication 800-111

Multi-tenancy:

Team CNSI's evoBrix ISR framework supports multi-tenancy with easily configurable modules. The existing solution can be configured to support processing of MT PSM interfaces. The extendable ISR framework is based on a modular approach, enabling plug and play of generic solution components. Because of the multi-tenancy feature, the existing ISR solution with minimal configuration can be leveraged and reused for common interfaces from federal agencies and for credentialing. Figure 3.10.1-119 is the list of interface services that the current ISR solution is supporting for the provider module. These interfaces can be reused and any new interfaces as part of evoBrix PMIS implementation can be processed by configuring the details through the ISR solution.

Interface	Type	Source	Destination
Send Approved Provider Information to Legacy MMIS	Batch	PMIS	Legacy System
Receive NPPES (National Plan and Provider Enumeration) File from DCH	Batch	Federal Agency	PMIS
Receive Taxonomy Data from Edifecs	Batch	Federal Agency	PMIS
Receive Federal CLIA (Clinical Laboratory Improvement Amendments) from DCH	Batch	Federal Agency	PMIS
Receive Federal DEA (Drug Enforcement Agency) Active Records from DEA	Batch	Federal Agency	PMIS
Receive Home Help Authorization, Task and Case Worker Information from ASCAP/ASAP	Batch	State Agency	PMIS
Provider Search/Inquiry Service	Web Service	PMIS	External Entities
Send NCPDP (National Council for Prescription and Drugs Program) Service Provider Panel File to Magellan	Batch	State Agency	External Entities
Send Daily Provider Enrollment Update to LN (Lexis Nexis)	Batch	PMIS	Provider Credentialing Agency
Send State Professional License Information to LN	Batch	PMIS	Provider Credentialing Agency
Send State Vital Information to LN	Batch	PMIS	Provider Credentialing Agency
Send NCPDP Provider Information to LN	Batch	PMIS	Provider Credentialing Agency
Receive State Vital Screening Results from LN	Batch	Provider Credentialing Agency	PMIS

Interface	Type	Source	Destination
Receive State Professional License Screening Results from LN	Batch	Provider Credentialing Agency	PMIS
Receive CLIA Screening Results from LN	Batch	Provider Credentialing Agency	PMIS
Receive Criminal Screening Results from LN	Batch	Provider Credentialing Agency	PMIS
Receive DEA Screening Results from LN	Batch	Provider Credentialing Agency	PMIS
Receive Federal Vital Deceased Screening Results from LN	Batch	Provider Credentialing Agency	PMIS
Receive Discipline Screening Results from LN	Batch	Provider Credentialing Agency	PMIS
Receive Out of State Medical License Screening Results from LN	Batch	Provider Credentialing Agency	PMIS
Receive Sex Offense Screening Results from LN	Batch	Provider Credentialing Agency	PMIS
Receive NPI Screening Results from LN	Batch	Provider Credentialing Agency	PMIS
Receive ABMS (American Board of Medical Specialties) Screening Results from LN	Batch	Provider Credentialing Agency	PMIS
Receive NCPDP Screening from LN	Batch	Provider Credentialing Agency	PMIS
Send Provider Enrollment Update	Batch	PMIS	External Entities

Figure 3.10.1-119. Interface Services. List of interfaces supported by Team CNSI's current evoBrix ISR solution.

Scalability:

Team CNSI's evoBrix ISR solution can scale seamlessly for growth in data and transaction volumes, and can utilize the rich features of the underlying hardware and software resources. ISR currently scales and handles high volume interfaces from federal agencies, MCOs or credentialing services and any other external agencies for Michigan, Illinois, and Utah.

High Availability:

To ensure a high availability, Team CNSI's evoBrix ISR infrastructure will be implemented with fault tolerance capabilities that will allow it to continue to operate despite failure or unavailability of individual technology components such as a server platform or network connection. ISR solution components are deployed in an oracle cluster environment with high availability features. This proposed solution is capable of handling large payloads with failover cluster.

Interoperability:

The evoBrix ISR core architecture leverages ESB features within the SOA framework to integrate disparate systems effectively. This architecture provides an integration backbone that connects core applications and services without directly accessing underlying systems. The evoBrix architecture is based on leveraging a series of COTS products that use a services-based integration platform.

evoBrix relies on open standards and standard application program interfaces (API), such as the Java Business Integration (JBI) standard, for plug-ability of third-party communities. The evoBrix architecture uses an enterprise class service bus (Oracle Fusion SOA) as the core orchestration tool of business processes across the different applications that support Medicaid operations. evoBrix supports robust

authorization, authentication and validation fe0atures using Oracle Service Bus. The proposed solution is capable of handling common industry standard service requests such as SOAP and REST. Also, evoBrix has the ability to change the various attributes of the service without impacting existing clients. ESB infrastructure will allow Core MMIS to avoid point-to-point communication between different system components and will streamline flow of all information throughout the evoBrix PMIS implementation.

INR01

The Contractor's solution must ensure that all data exchanges including inbound and outbound interfaces shall comply with industry standards (e.g., National Information Exchange Model (NIEM), National Institute of Standards and Technology (NIST), HIPAA-compliance standards, Health level 7 (HL7), Fast Healthcare Interoperability Resources (FHIR)).

Team CNSI's evoBrix solution complies with HIPAA compliance standard for all data exchanges including inbound and outbound interfaces. The data exchange with external vendors is handled via managed file transfer using secure file transfer protocol. Team CNSI's ISR solution leverages Oracle SOA suite built in adapters that comply with industry standards (HL7, NIEM) to process inbound and outbound interfaces.

Team CNSI has extensive experience in implementing X12 version 5010 and interacting with providers, clearing houses and third-party vendors using the following HIPAA transactions as required by 45 CFR Parts 160 and 162.

- 276 – Electronic Claim Submission System Request
- 277 – Electronic Claim Submission System Response
- 277RQ – Health Care Claims Request for Additional Information
- 277CA – Health Care Claim Acknowledgement Report
- 835 – Healthcare Claim Payment Advice
- 837D – Healthcare Claim – Dental
- 837I – Healthcare Claim – Institutional
- 837P – Healthcare Claim – Professional
- 999 – Functional Acknowledgment
- TA1 – Interchange Acknowledgment
- 278 – Prior Authorization Request
- 278 – Prior Authorization Response

Team CNSI's evoBrix PMIS solution includes security and privacy controls that are compliant with the most current version of the CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E) and NIST standards. Team CNSI's evoBrix PMIS solution adheres to the following security standards

- Federal Information Security Management Act (FISMA)
- Internal Revenue System (IRS) Publication 1075
- Patient Protection and Affordable Care Act (PPACA) or (ACA)
- NIST Special Publication 800-66 Revision 1
- NIST Special Publications 800-53 and 800-53A
- NIST Special Publication 800-47
- NIST Special Publication 800-88 Revision 1
- NIST Special Publication 800-111

INR02

The Contractor shall support the exchange of data between the System and the systems with which it interfaces (including external entities) to facilitate business functions that meet the requirements of Department policy, and federal and State rules and regulations.

Team CNSI's evoBrix ISR solution will be used to interface with the State agencies and all approved trading partners. It offers a robust and comprehensive framework to interface with all State-approved trading partners and federal provider-related data sources using a secure connection to facilitate business functions to meet the requirements of department policy, and federal/state rules and regulations. The evoBrix ISR solution supports scheduling, audit, error logging, and escalation features along with detailed reporting on interface execution status, combined with notification modules to track execution of the various interface transactions, thus ensuring processing of MT PSM interfaces within timeframes. The evoBrix ISR solution was built for scalability by design.

Team CNSI's evoBrix ISR will be running multiple levels of validations before and after file processing and will notify all stakeholders of any issues during the process. File format, data type, and record length are few examples of validation run during the time of file processing. However, if there were any errors, notification emails will be sent out to the business users containing details of the error, which helps in isolating the root cause enabling corrective actions to be taken by the business user according to the business timeframe.

INR04

The system shall send and receive real-time discrete transactions between modules and the State's integration platform to reduce the need for bulk data transfers.

In addition to batch mode of data trading, the Team CNSI ISR solution supports real-time data trading of interfaces based on the business/operations need between modules and the State's integration platform. CNSI's evoBrix ISR solution supports data trading in near real-time via evoBrix OSB web services. The evoBrix architecture uses an enterprise class service bus (Oracle Fusion SOA) as the core orchestration tool of business processes across the different applications that support Medicaid operations. CNSI's evoBrix Integrator's configurable ISR solution can handle MT PSM integration for transmittal of data for different systems to align with the conceptual solution architecture. This solution provides an integration backbone that connects core applications and services without directly accessing the underlying systems. evoBrix supports robust authorization, authentication, and validation features using Oracle Service Bus. The solution is capable of handling common industry standard service requests such as SOAP and REST. Also, evoBrix can change the various attributes of the service without impacting existing clients. The Oracle Fusion SOA infrastructure will avoid point-to-point communication between different system components and will streamline the flow of all information.

INR05

The Contractor's solution shall provide the ability to view raw daily interface files for up to sixty (60) calendar days. Archive raw daily interface files after sixty (60) calendar days and maintain for up to six (6) months.

Team CNSI's evoBrix ISR solution provides a custom archival solution for the interface files depending on DPHHS requirements. The ISR solution manages multiple directories such as working, temporary, error, and completion. Files will be moved to the completion directory upon successful execution; if there are any errors, files will be moved to the error directory. Interface files can be viewed from this directory for a configurable period depending on the retention policies defined by DPHHS. The ISR archival process can be configured to keep raw daily files for 60 days. The files can be archived, with the vendor determined retention period, to the secure location. The archived files can be maintained up to 6 months. Team CNSI will work with DPHHS on the archival intervals to view the raw data and archive the raw files to secure location for future review.

INR06

The Contractor's solution shall provide the ability to view raw monthly and quarterly interface files for up to one year (365) calendar days. Archive raw monthly and quarterly interface files for two years (730) calendar days and maintain for up to two (2) years.

Team CNSI evoBrix ISR solution provides custom archival solution for the interface files depending on the DPHHS requirements. The ISR solution manages multiple directories such as working, temporary, error, and completion. Files will be moved to the completion directory upon successful execution; if there are any errors, files will be moved to the error directory. Team CNSI will configure the solution to provide ability to view raw monthly and quarterly interface files for up to one year (365 calendar days), archive raw monthly and quarterly interface files for two years (730 calendar days), and maintain for up to two years.

INR07

The Contractor shall document all interfaces in an Interface Control Document (ICD) which will include data layout documentation, data mapping crosswalk, inbound/outbound capability and frequency of all interfaces.

Team CNSI will work with MT DPHHS to create the Interface Control Documents (ICDs) for the third-party interfaces. Team CNSI converts ICDs to Detail System Design Document (DSDD). The DSDD contains interface specifics such as file format, file structure, third-party system details, and inbound/outbound details along with interface schedule frequency, detailed business rules, and any other required information. Team CNSI maintains required information related to integration with MT DPHHS external agencies in the DSDD.

INR08

The Contractor's solution shall include a process and toolset to maintain interfaces, code, and data models.

Team CNSI maintains SharePoint as the online repository in which to store all the interface-related ICD templates and design documents (DSDD) containing the interface layouts including field definitions, descriptions, purpose of the interface, and schedule information. Any change logs after the approval from the State team will be stored in the online portal/SharePoint.

Team CNSI uses a robust version control mechanism to store the code and any data objects related to the data model. Team CNSI uses ClearCase and Subversion as the version control tools for the code and data model changes. Team CNSI has proven expertise in maintaining different code bases and maintaining multiple environments to support different system/application testing needs.

INR11

The Contractor shall design, develop and maintain interfaces. Each Application Program Interface (API) and components that will interface with the Systems Integration Services Integration Platform will be documented using a mutually agreed upon ICD template. This effort is performed in collaboration with other stakeholders in the State's healthcare programs enterprise.

Team CNSI understands the need for enabling efficient and scalable transmittal of data, and consolidation of different disparate systems as required by various business areas, as the core of MT PSM integration strategy.

Team CNSI will work closely with the MT DPHHS to implement data trading with the Medicaid Enterprise through the System Integration Services. During the design phase, Team CNSI will work with MT DPHHS to create ICD template and CNSI converts ICD templates to the DSDD for the third-party interfaces. The DSDD contains interface specifics such as file format, file structure, third-party system details, detailed business rules, and any other required information. Team CNSI maintains required information related to integration with MT DPHHS external agencies in the DSDD.

INR12

The Contractor shall ensure proprietary interfaces and protocols between modules are not used.

Team CNSI adheres to industry standard file formats in its current implementation with states of Michigan, Illinois, and Utah, and does not have any proprietary interfaces. Also, the ISR framework is implemented through industry standard transport methods/protocols and security framework for the Core MMIS. Exchanges are architected to provide secure and protected data communications that maintain confidentiality and integrity of the data. Data exchange from evoBrix PMIS to external systems will be handled by evoBrix ISR framework by leveraging Oracle SOA suite File transfer features that supports secure data exchanges using available standards in the industry such as SFTP, FTPS, and SSL.

3.10.1.7 Business Rule

This section addresses Business Rule requirements for the Contractor's solution(s) and operations. The Contractor shall describe the proposed solution's capacity to configure, support and maintain business rules (i.e., add, modify, or remove/retire rules) and the type of resource and necessary skill set(s) required for business rule configuration. Describe the change management processes associated with business rule configuration. In addition, the Offeror must describe their approach to meet each of the Business Rules requirements detailed in Attachment F, Requirements Matrix.

The evoBrix PMIS solution addresses the business rule requirements through a combination of tools and frameworks that allow authorized users to configure, define, and maintain the business rules required for provider enrollment, disenrollment, re-enrollment, and maintenance activities as required by State policy. As a part of the implementation of the MT PSM, Team CNSI will train authorized State business operations staff to add, modify or remove/retire configurable enrollment rules. The evoBrix PMIS leverages:

- RuleIT, a rules engine based on industry standards and built specifically to address Medicaid programs
- evoBrix PMIS Permission Matrix, a table-driven approach to configuring license/certification rules based on Provider type and Specialty within the application itself

The Team CNSI Advantage

The evoBrix PMIS leverages a decision management framework that is a combination of RuleIT, an industry-standard rules engine built specifically to address the Medicaid program, and Permissions Matrix to address the business rule requirements.

- RuleIT provides out of the box CMS–mandated policy rules for Medicaid
- RuleIT supports the use of English-like syntax, a predefined Medicaid dictionary, and standard Medicaid edits and processing flows
- Permission Matrix provides a table-driven approach to configuring license/certification rules based on Provider type and Specialty
- The evoBrix PMIS provides a balanced approach between configuration-driven changes and code changes that allows non-technical subject matter experts to update or change business decisions and policies

MTPSM-3-288

RuleIT

Team CNSI has implemented RuleIT to support provider enrollment and maintenance management for our implementations in Washington, Michigan, Illinois, and Utah. RuleIT has been engineered from the ground up to meet the high demands of the Medicaid enterprise. Through our previous implementations, RuleIT has been refined and optimized to support provider enrollment, management, and maintenance.

RuleIT was developed on the Java 2 Enterprise Edition (J2EE) platform architecture, making it portable across many hardware and software platforms. The use of English-like syntax, a predefined Medicaid dictionary, and standard Medicaid edits and processing flows make RuleIT easy to deploy and implement. RuleIT acts as a business rules repository for various business scenarios, and accumulates business knowledge in small, manageable pieces. RuleIT uses a sequential process algorithm, in which the business scenario evaluation is controlled by the rule, its conditions, and any associated branching. Its flexible architecture lets a business analyst determine the sequence of rule evaluation, which simplifies setting up the processing chain more manageably. RuleIT facilitates the execution of a single rule or a series of complex process flow rules.

RuleIT consists of the following major components:

- RuleIT Composer is a user interface for creating, editing, exporting, and importing rules to the Rules Repository. RuleIT Composer, built on the Java platform, is easy to use and navigate. It provides a debugging mode that displays results of rule execution and can be installed on all major operating systems that support Java.
- RuleIT Configurator is used to define and create variables, constants, and methods. It uses a web-based interface and permits more flexibility in managing and administering the application. It provides the ability to configure the engine, create the English-like syntax, add business definitions, and maintain users and permissions, among other things.
- RuleIT Processor is an Enterprise Java Bean (EJB) that is the runtime rule evaluator or executor for rules defined in the RuleIT Repository. RuleIT Processor can be deployed on most application servers, and provides a public interface that integrates easily with other J2EE-compliant applications. RuleIT Processor is currently tested and certified on WebLogic, WebSphere, and JBoss application servers.
- RuleIT Evaluator is used to test rules for the various scenarios by providing the inputs. This testing aids in better understanding of the business and significantly reduces the delay between writing rules and running it in production.

- RuleIT Repository is the centralized store for all rules defined within RuleIT and can store rules for multiple applications. The rules can be segregated into knowledge bases and rule groups, which allows for greater flexibility and control. The RuleIT Repository can be hosted on an Oracle or MySQL database.

The flexible and comprehensive RuleIT Rule Composer allows authorized users to define the enrollment rules for each provider enrollment type and specialty. An enrollment type is a predefined general category of provider. Authorized users will use the Rules Composer to define each step of the enrollment process and the data elements required to complete that step for each enrollment type. The business rules developed using RuleIT are deployed to providers and business operations staff in the form of Business Process Wizards (BPWs) that govern the enrollment and maintenance activities for each type of enrollment. Once all the business rules are defined, the authorized State user will use the Rules Composer to organize the enrollment path for each type of enrollment.

The BPWs guide providers through the enrollment and maintenance processes. The BPW uses State-specific rules configured using the RuleIT rules engine to designate steps as required or optional, dynamically, depending on data entered by the provider for a given enrollment type, as shown in Figure 3.10.1-120 and Figure 3.10.1-121. Figure 3.10.1-120 shows the BPW for an individual billing provider. Figure 3.10.1-121 shows the BPW as configured for an individual atypical provider. The BPW validation rules, controlled by RuleIT, are based on the State policies for enrollment type and include validation of data, such as NPI.

Using RuleIT to configure the BPW's pre-defined business rules prevents submission of an enrollment application until the information content and validity have been verified to meet State standards. Use of RuleIT also facilitates easy modification when State policy changes are necessary.

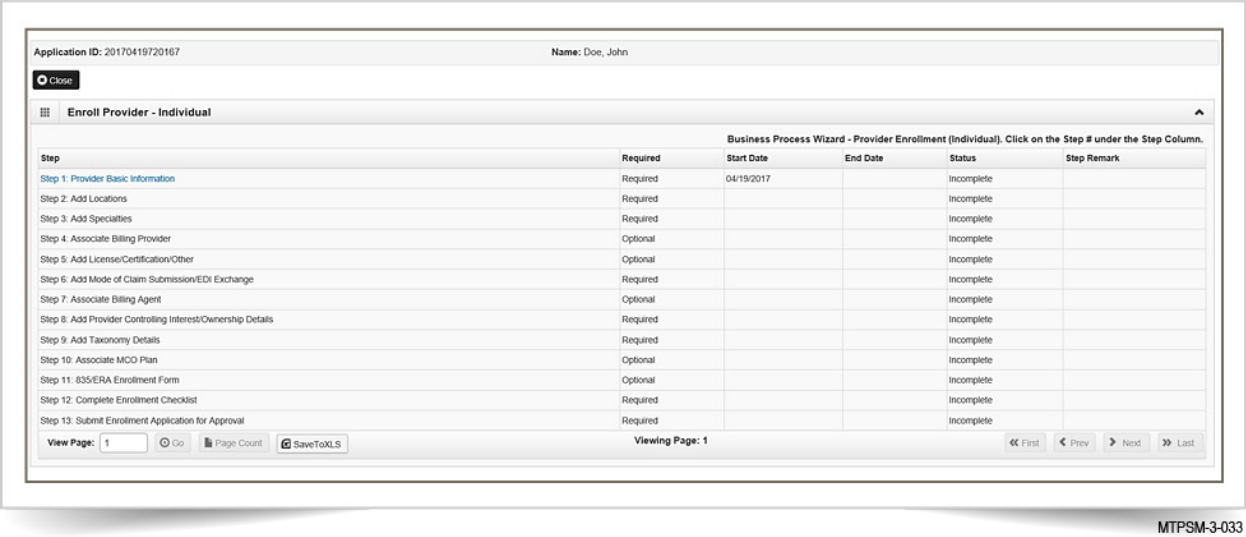
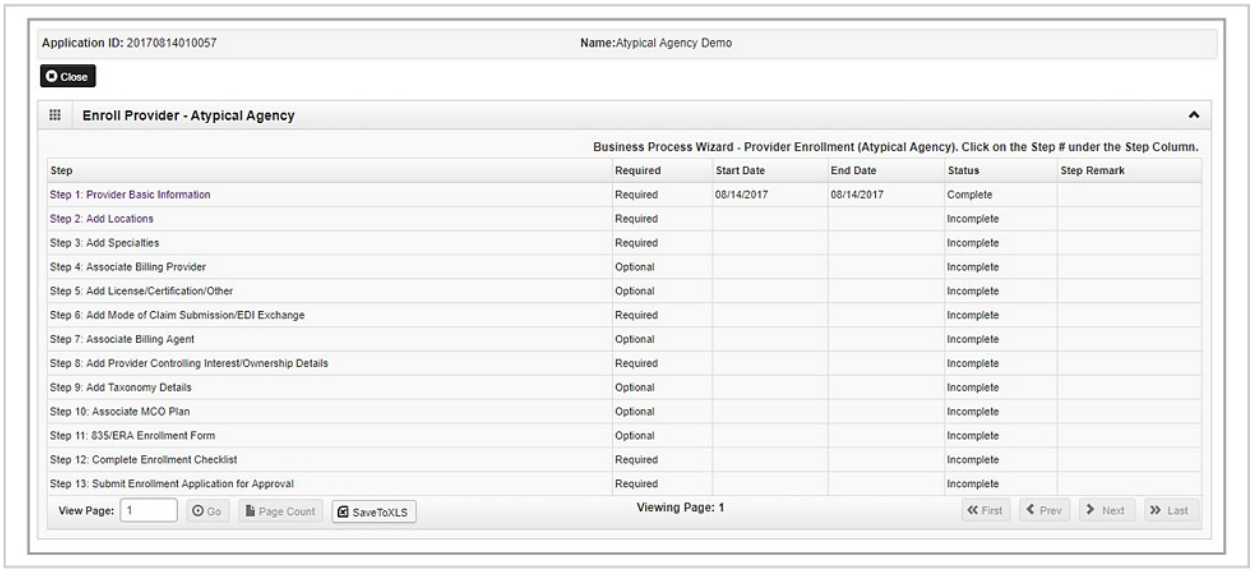


Figure 3.10.1-120. The evoBrix PMIS Individual Enrollment BPW. The BPW guides the enrolling provider through all steps of the enrollment process.



MTPSM-3-441

Figure 3.10.1-121. The evoBrix PMIS Atypical Agency Enrollment BPW. The BPW guides the enrolling provider through all steps of the enrollment process.

Permissions Matrix

The second major component of business rules management is the evoBrix PMIS Permission Matrix. The Permissions Matrix defines the provider types and specialties supported by the State's Medicaid and Waiver programs. This includes specific credentials, such as licensing, required of successful applicants for each defined provider type/specialty combination. The Permissions Matrix helps to:

- Define State-specific specialty combinations and risk category (High, Moderate, and Low)
- Configure mandatory, optional, and conditionally mandatory enrollment and re-enrollment data requirements by provider type and specialty combination
- Define and configure credentialing and re-credentialing rules for each unique provider type and specialty combination.

Prior to enrollment approval, the BPW applies the credentialing policy based on the Permissions Matrix in real time as the provider enters enrollment information. Once the required credentials are entered, the application is submitted and if any credentials are missing, the BPW notifies the provider accordingly for proper action as required for enrollment to be completed. Once the provider's enrollment is approved, the credentialing policy is applied each time a change is requested. The provider maintenance BPW provides the same functions as the provider enrollment BPW, advising the provider of missing information in real time.

Using the Permission Matrix configurations, evoBrix PMIS' nightly batch process generates warning notices to providers in advance of the expiration of a required credential. This allows the provider to update the credential and avoid any lapse in Medicaid eligibility. On a nightly basis, provider records are reviewed against the credentialing policy. When missing or expired credentials are found, the provider's records are marked as inactive.

Using the Permissions Matrix, authorized State users have the ability to implement new or revised credentialing requirements through a simple table change. The new credentialing requirement becomes effective as soon as the update is made. The enrollment unit begins by generating a communication that

alerts affected providers of the new requirement and its effective date. The communication specifies the date by when the credential must be provided if their enrollment is to remain valid. The evoBrix PMIS automatically changes the status to "inactive" for providers who do not comply. This method limits inactivation to specific specialties and programs for which the credential change is applicable. Other provider type/specialty combinations for the provider remain active.

Figure 3.10.1-122 shows the provider types that are associated with specialty/subspecialty combinations.

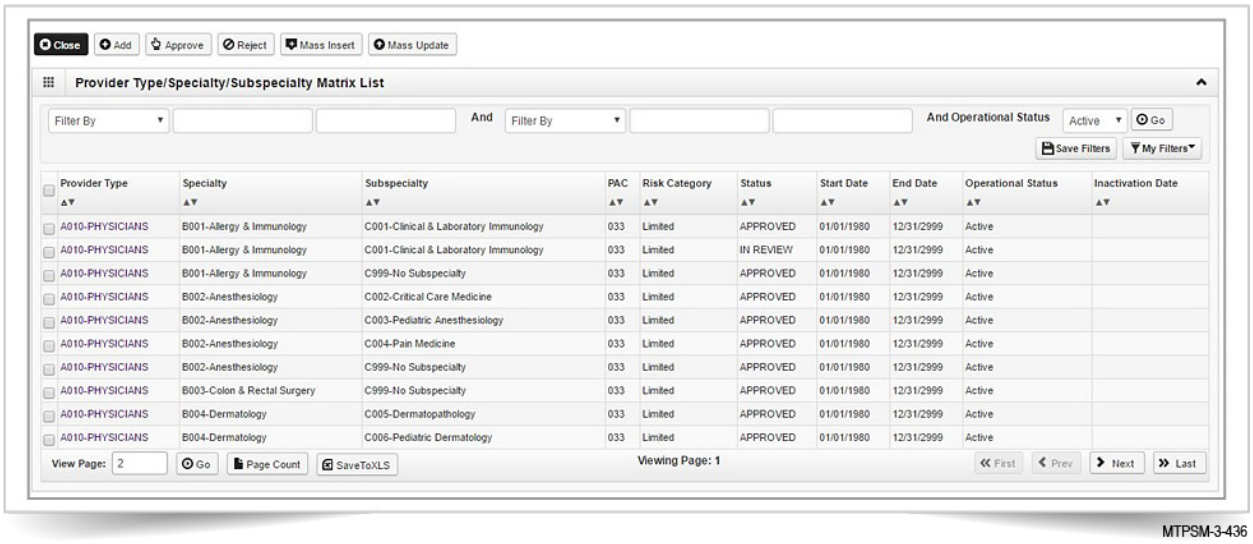


Figure 3.10.1-122. Provider Type/Specialty/Sub-Specialty Combinations Configured in evoBrix PMIS. PMIS provides flexibility in configuring provider types, specialties, and sub-specialties.

Figure 3.10.1-123 shows the screen through which new combinations of provider type/specialty/sub-specialty combinations are added to the matrix.

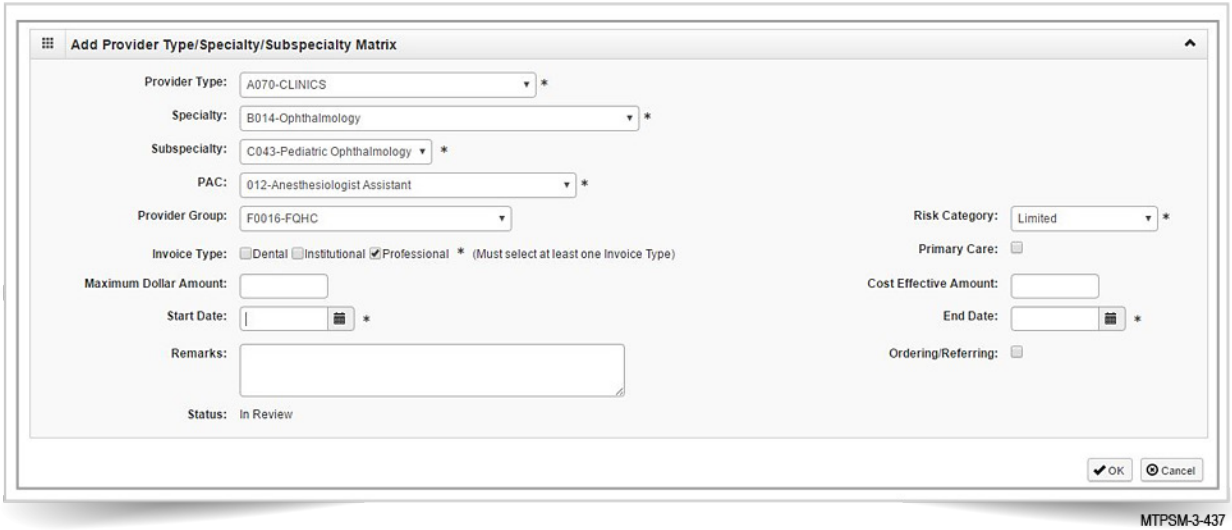


Figure 3.10.1-123. Add Provider Type/Specialty/Sub-Specialty Combination. Screen through which business operations staff can add provider type/specialty/sub-specialty combinations within the evoBrix PMIS.

Figure 3.10.1-124 shows the screen through which an existing provider type/specialty/sub-specialty combination can be modified. This screen also gives additional menu options to make changes to the Licenses, Claim Type, and Bill Type associated with the combination.

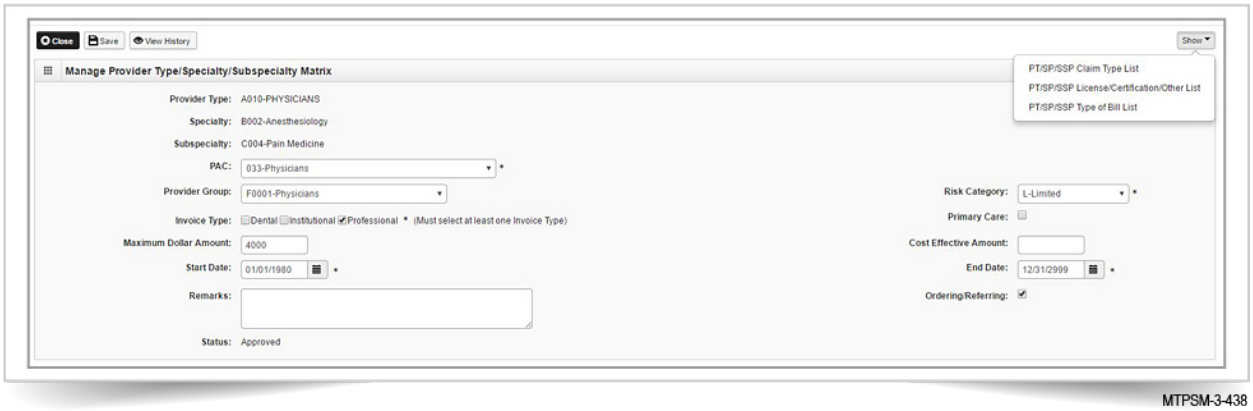


Figure 3.10.1-124. Manage Provider Type/Specialty/Sub-Specialty Matrix. Screen through which the business operations staff maintain the provider type/specialty/sub-specialty combinations within evoBrix PMIS.

Figure 3.10.1-125 shows the list of licenses configured for a specific provider type/specialty/sub-specialty combination.

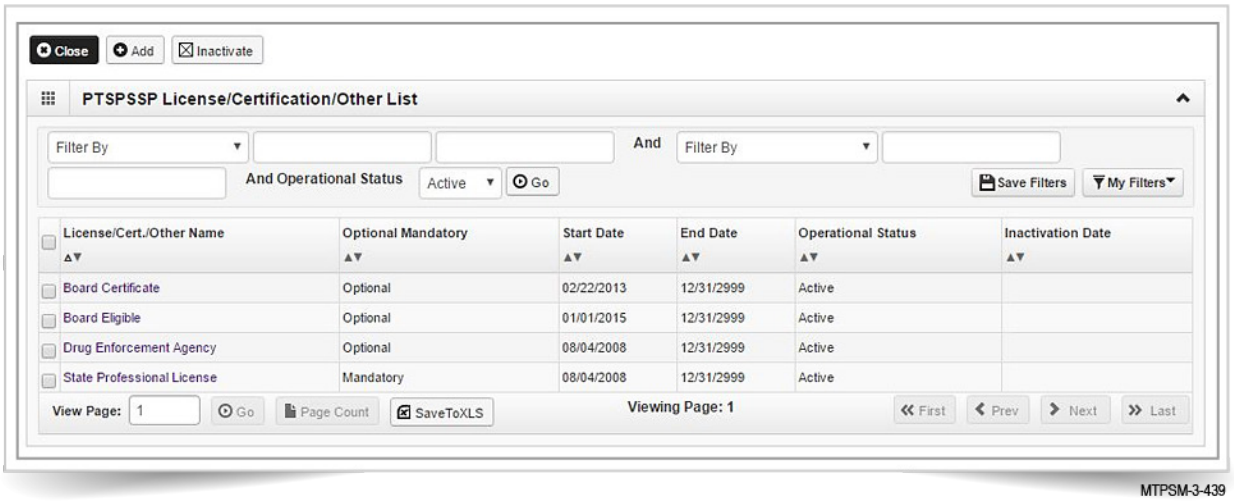


Figure 3.10.1-125. License/Certification List Screen. Screen displaying the list of licenses/certifications for a specific provider type/specialty/sub-specialty combination.

Figure 3.10.1-126 shows the screen through which a license can be configured for a provider type/specialty/ sub-specialty combination. Marking a license mandatory will force the provider to enter a license when the combination of provider type/specialty/sub-specialty is selected during the enrollment process, thus driving business rules.

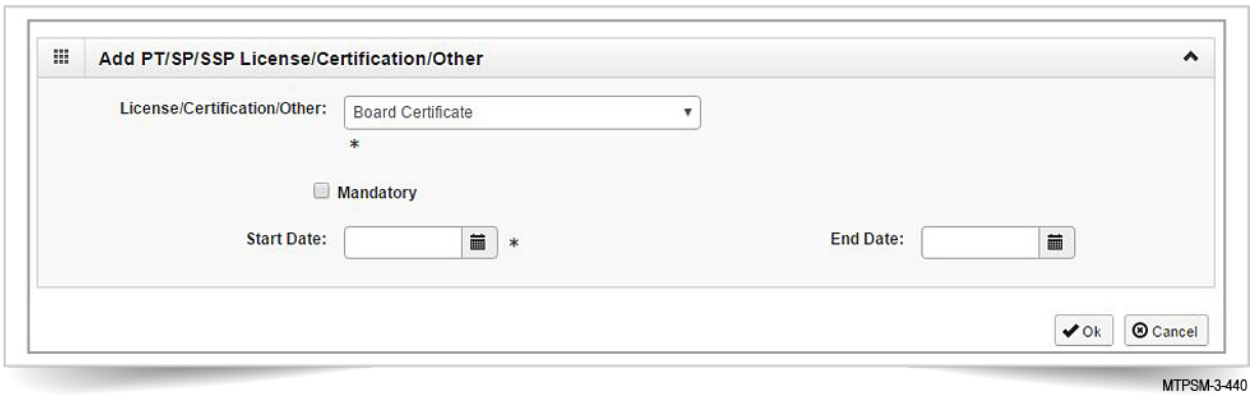


Figure 3.10.1-126. Add Provider Type/Specialty/Sub-Specialty License/Certification/Other Combination. The business operations staff maintain provider type/specialty/sub-specialty license/certification combinations through online screens.

BR01

The Contractor shall configure, support and maintain a business rules engine (e.g., add, modify, or remove/retire rules) based on the Service Architecture (SOA).

The evoBrix PMIS leverages RuleIT, a rules engine based on industry standards and built specifically to address the Medicaid program. The RuleIT Composer shown in Figure 3.10.1-127 is the component of RuleIT used to add, modify, or remove/retire rules in the rules engine repository. The exhibit highlights some of the key features of this tool and shows a sample rule syntax.

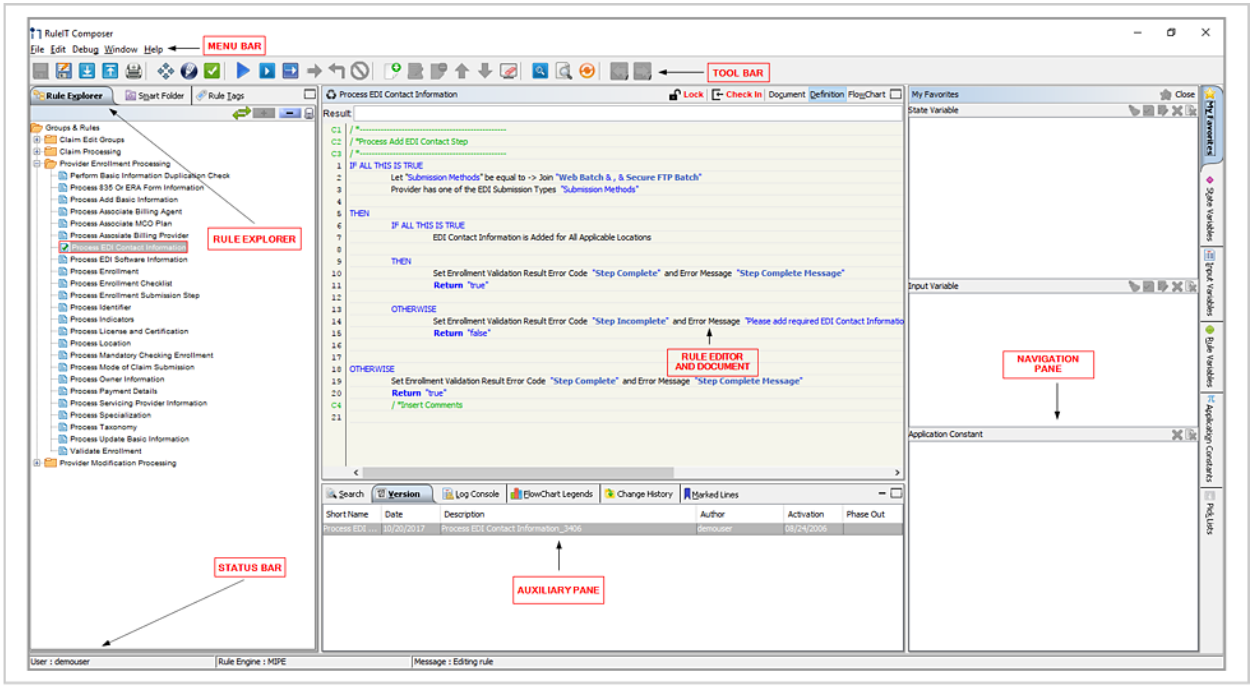
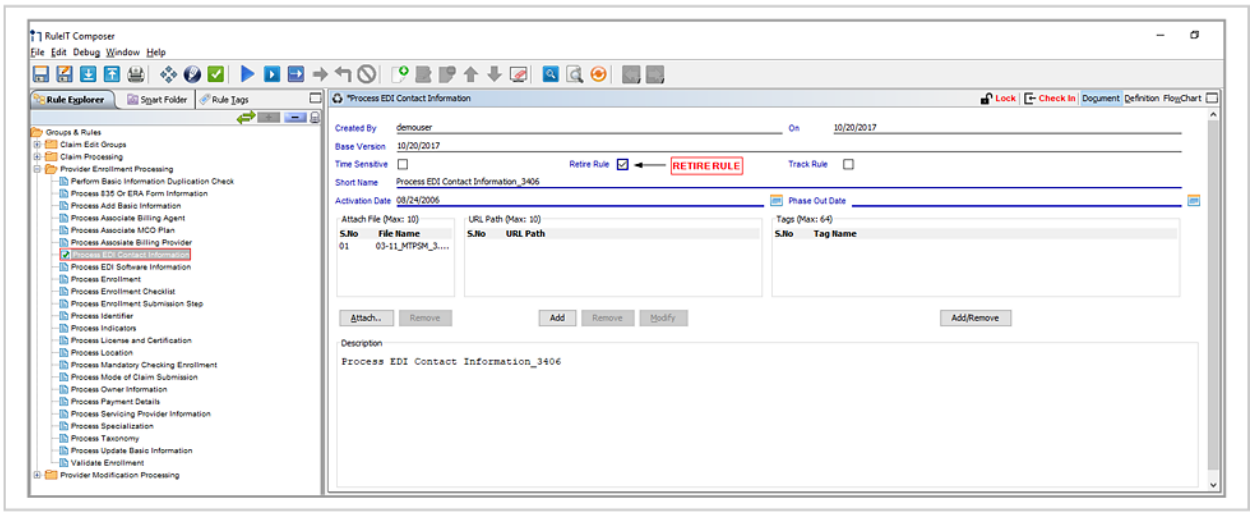


Figure 3.10.1-127. RuleIT Composer. RuleIT Composer has a user-friendly interface that makes it easy to use.

RuleIT offers the flexibility to create and integrate customized rules specific to the Department's needs and can accommodate changes to existing rules. The flexibility and increased productivity that RuleIT offers will reduce the time it takes to build, test, and implement complex rules. RuleIT Composer provides the option to retire rules, which can be useful when rules must be retired based on policy changes. Figure 3.10.1-128 shows the screen used for retiring a rule.



MTPSM-3-443

Figure 3.10.1-128. RuleIT Composer Retire Rule Configuration Screen. RuleIT supports retiring rules through an easy configuration screen.

Team CNSI uses the Web services framework to integrate with other components. The architecture provides for a set of tools and infrastructure services to support the management of integration with other components in the enterprise using SOA principles. RuleIT Processor can be exposed as a service to external components using a Web services wrapper. When exposed as a webservice, the rules can be consumed by external enterprise application using SOA integration methodologies.

BR02

The Business Rules Engine (BRE) shall allow authorized system users including Department resources, the ability to create, configure and maintain rules for business functions in a user-friendly graphical user interface (GUI) that facilitates rules maintenance without coding changes.

RuleIT Composer provides a user name and password screen to authenticate users before they are allowed access to the application. Administration of RuleIT users is available to authorized security administrators through online screens. Users can be added and removed and their appropriate privileges can be assigned through this interface, so it does not pose a risk of unauthorized data access.

Figure 3.10.1-129 shows the Rule IT Composer login screen.

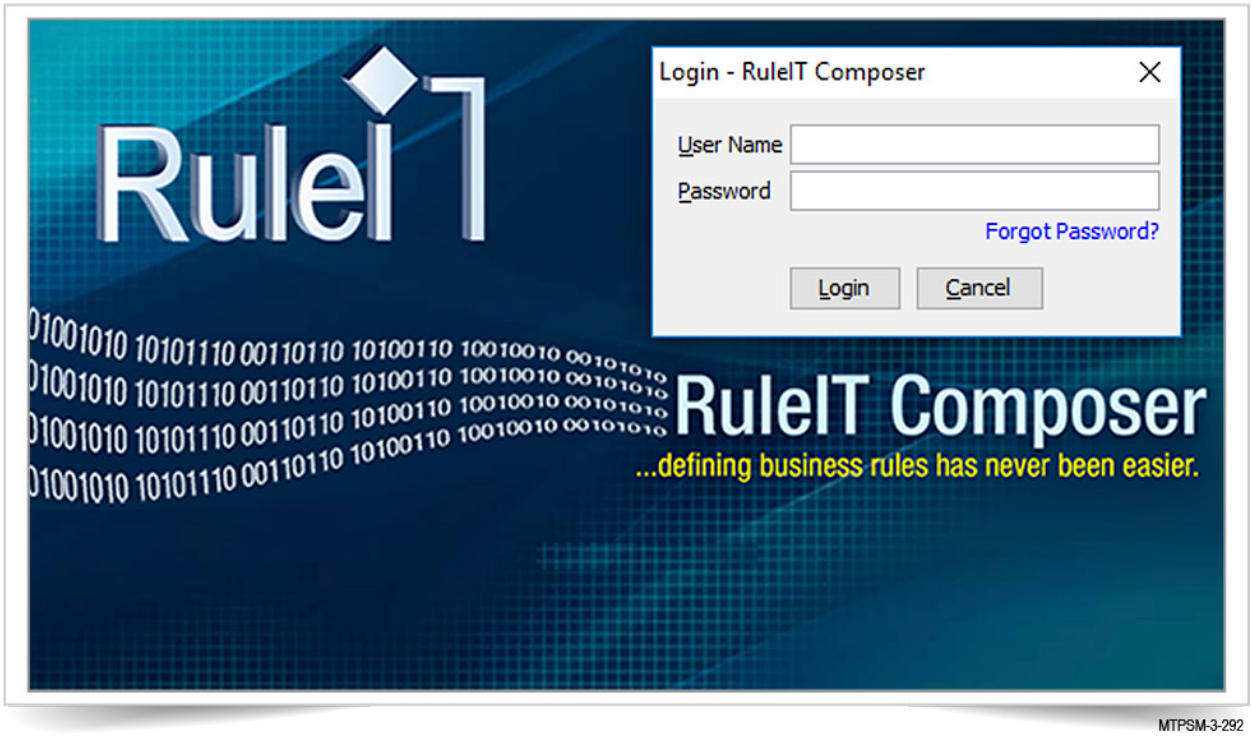
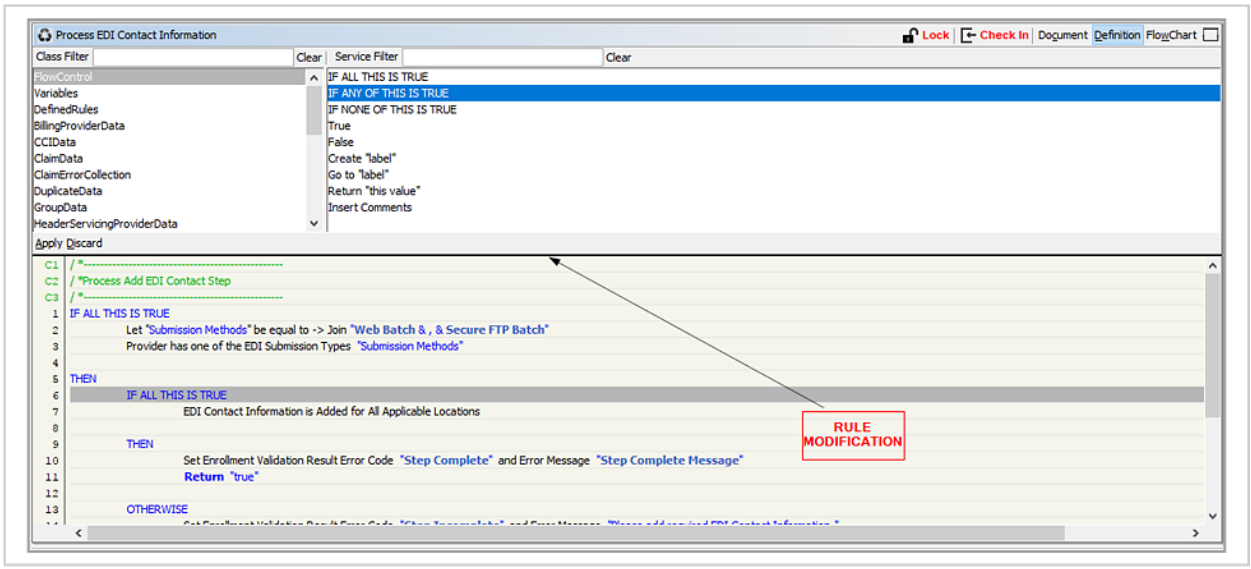


Figure 3.10.1-129. RuleIT Composer Login Screen. RuleIT supports well-tested and audited authentication and authorization security measures.

The RuleIT Composer component is built on the Java platform, and is a graphical user interface (GUI) used for creating, editing, exporting, importing, and searching rules in a repository, as shown Figure 3.10.1-130. It also provides the capability to document the rule and the option to make the rule change time-sensitive for claim processing. RuleIT Composer also allows users to navigate all the rules and search within the rules based on user-selected criteria. These features enable designated Department users to apply or disable rules quickly and without programmer intervention.



MTPSM-3-444

Figure 3.10.1-130. RuleIT Composer Rules Editing Screen. RuleIT's user-friendly GUI facilitates rules maintenance without coding changes.

BR03

The Contractor shall provide real time access to a Business Rules Catalog, in an electronic format approved by the State, that documents all business rule logic used by the solution.

Team CNSI will provide real-time access to a Business Rules Catalog that documents all business logic used by the evoBrix PMIS solution and provides the framework necessary to support State approval for business rule management activity. Authorized users will have the ability to access the Business Rules Catalog in real-time.

The evoBrix PMIS leverages a decision management framework that is a combination of RuleIT, an industry-standard rules engine built specifically to address the Medicaid program, and Permissions Matrix to address the business rule requirements. Therefore, the business rules implemented in the solution not only use the rules engine repository but also the Permissions Matrix stored within the application itself. The Permission Matrix configuration changes can be made through the evoBrix PMIS screens.

Team CNSI will work with the State to publish a Business Rules Catalog that documents the business rules used by RuleIT and the Permissions Matrix. Authorized users will have the ability to access the Business Rules Catalog in real-time.

BR04

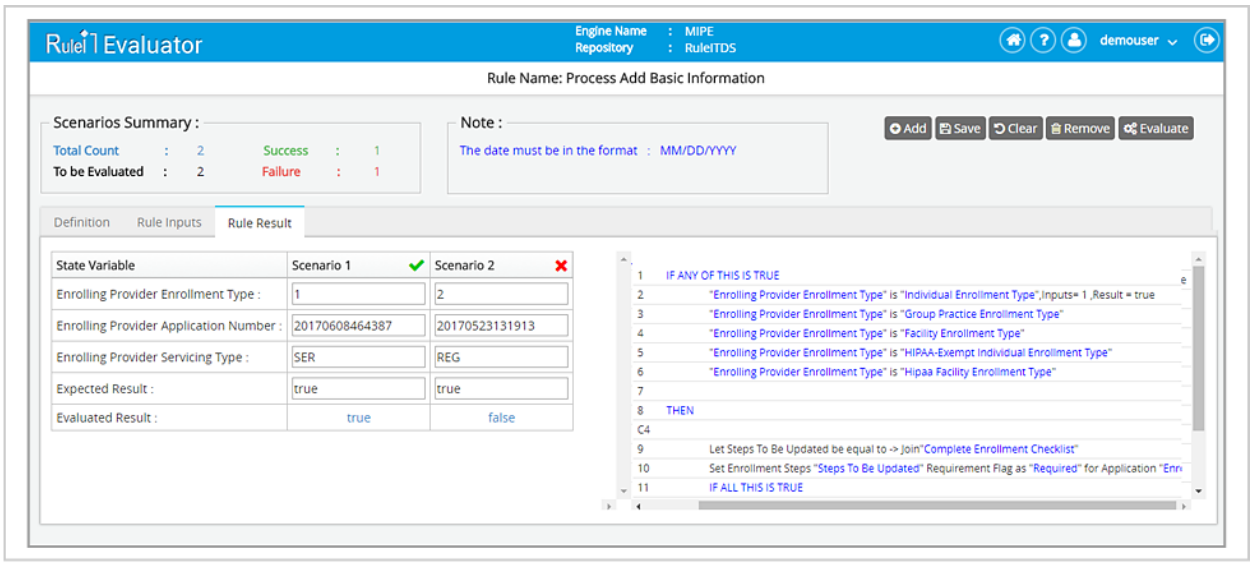
The Contractor shall update the Business Rules Catalog with all additions or changes.

Team CNSI will maintain the Business Rules Catalog to reflect all additions or changes to the business rules implemented in the solution. The additions and changes will be published to the users through the real-time access to the online Business Rules Catalog.

BR05

The Contractor's Business Rules Engine shall be integrated into a testing environment that contains production data to allow users to perform "what if testing" and compare the before and after outcomes. The Contractor will provide Department staff and designated project resources, support and access to reports or reporting tools to evaluate the impact analysis.

Team CNSI maintains a fully-integrated testing environment that contains production data to allow authorized users to perform "what-if testing." This environment will mimic the production setup and can be refreshed with the current production data to support impact analysis of "what-if" scenarios. The before and after outcomes can be compared and results of the comparison can be published to State staff and designated project resources. Further, RuleIT Evaluator, a component of RuleIT, enables users to test business rules by creating scenarios based on various rules inputs and perform "what-if testing," which aids in understanding the impact and analyzing outcomes of the changes. This is illustrated in Figure 3.10.1-131.



MTPSM-3-447

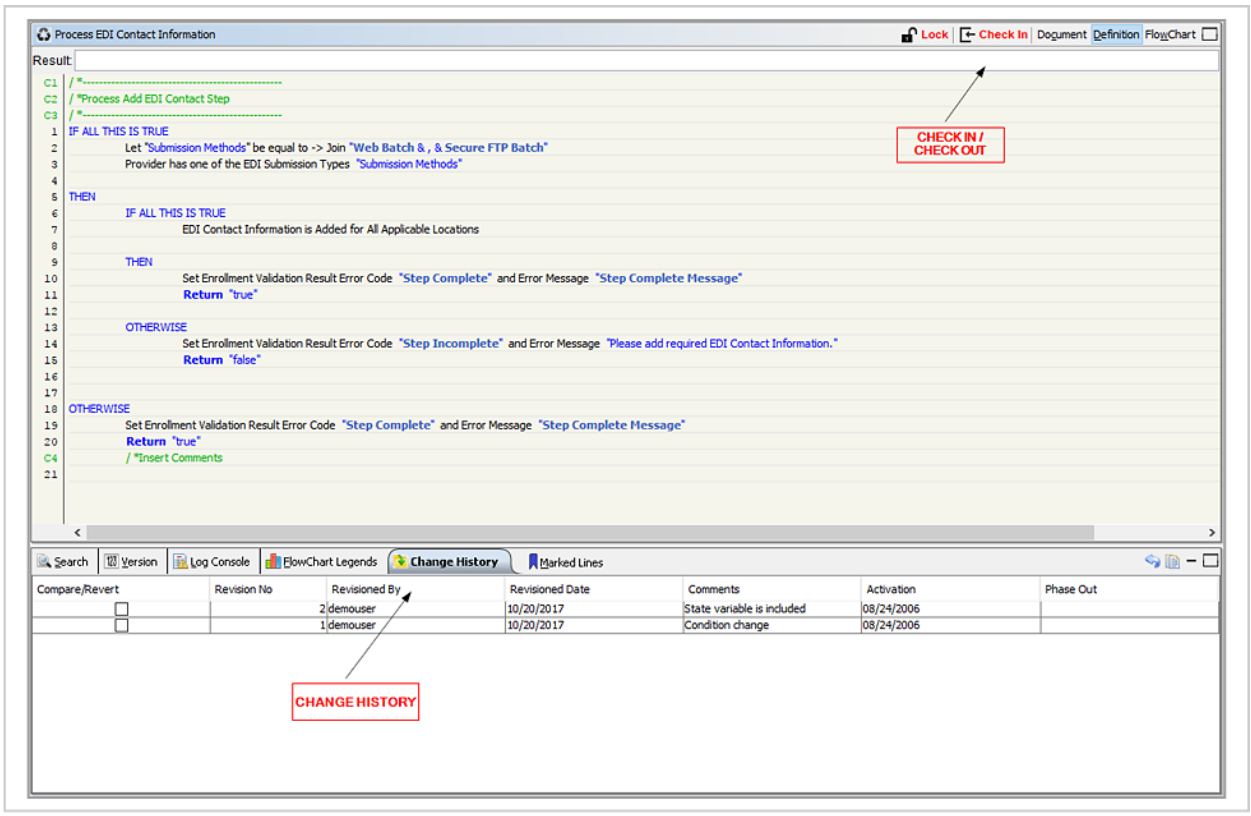
Figure 3.10.1-131. RuleIT Evaluator screen. RuleIT Evaluator performs rules testing to understand the before and after outcomes and supports what-if scenario testing.

The same environment can be used to test Permission Matrix changes as well. The table-driven configuration changes can be made through the evoBrix PMIS screens and assessed as part of the overall "what-if" analysis.

BR06

The Contractor's Business Rules Catalog shall include granular check-out and check-in rules and an audit trail of business rules changes.

RuleIT Composer includes checks and validations to support multiple users' rules configurations. It maintains a check-out/check-in feature so that a user can reserve a particular rule before making any changes. Figure 3.10.1-132 shows the Check In button on the RuleIT Composer screen.



MTPSM-3-448

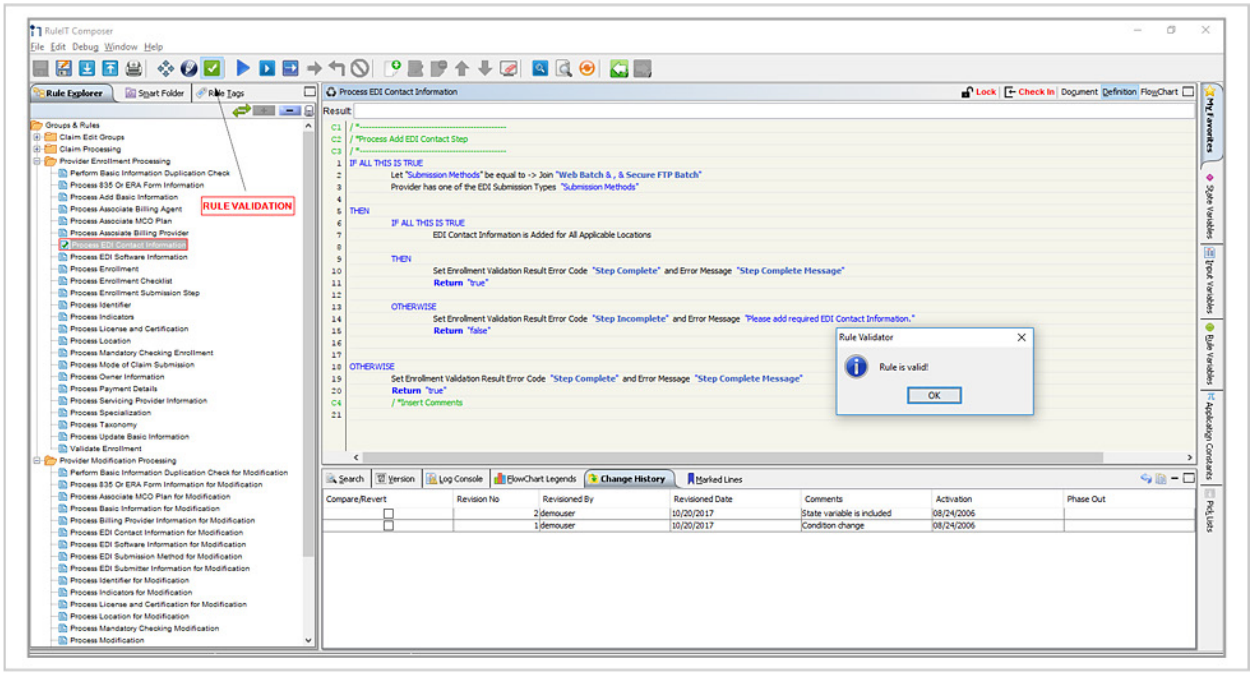
Figure 3.10.1-132. RuleIT Composer Version History Screen. RuleIT allows users to check-out and check-in rules changes with detailed audit trails.

The table-driven Permissions Matrix changes are performed through the evoBrix PMIS screens. The application has validations in place to prevent multiple users from modifying the same record at the same time. The ability to maintain the Permissions Matrix is granted only to specific users. Also, the Permissions Matrix changes go through an approval process and can be approved or rejected by an authorized approver.

BR08

The Business Rules Engine shall allow changes to be made to valid values without impacting production rules engine availability and operations.

In RuleIT Composer, users can modify the rules for the change in business variable values and application constants. After the rule modification, rule validation can be checked as shown in Figure 3.10.1-133. Rules are developed in the development environment and promoted to higher environments such as test, user acceptance, and production using the RuleIT Migrator. The rules migration process is performed during the scheduled deployment window and will not impact production rules engine availability and operations.



MTPSM-3-449

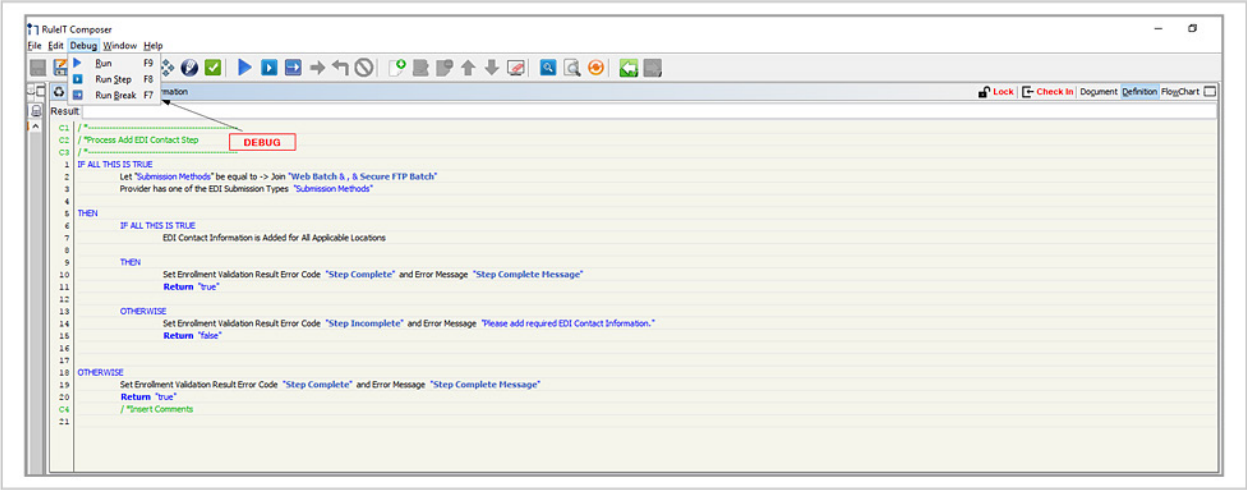
Figure 3.10.1-133. RuleIT Composer Rules Validation Screen. RuleIT allows users to easy access to validate the rules.

The table-driven Permissions Matrix changes are tied to effective date ranges and will not disrupt the rules implementation in production. Authorized State staff can use an evoBrix PMIS feature called “Mass Update” to apply the Permission Matrix changes to all impacted providers at the same time.

BR09

The Business Rules Engine shall include the ability to debug business rules at rule execution.

RuleIT Composer provides a debugging mode that displays the results of rule execution, which allows users to quickly view logical errors. Figure 3.10.1-134 shows the debugging screen, with RuleIT Composer’s various debug options.



MTPSM-3-450

Figure 3.10.1-134. RuleIT Composer Debugging Options. RuleIT provides elaborate debugging options to support developing and verifying the rules quickly.

BR10

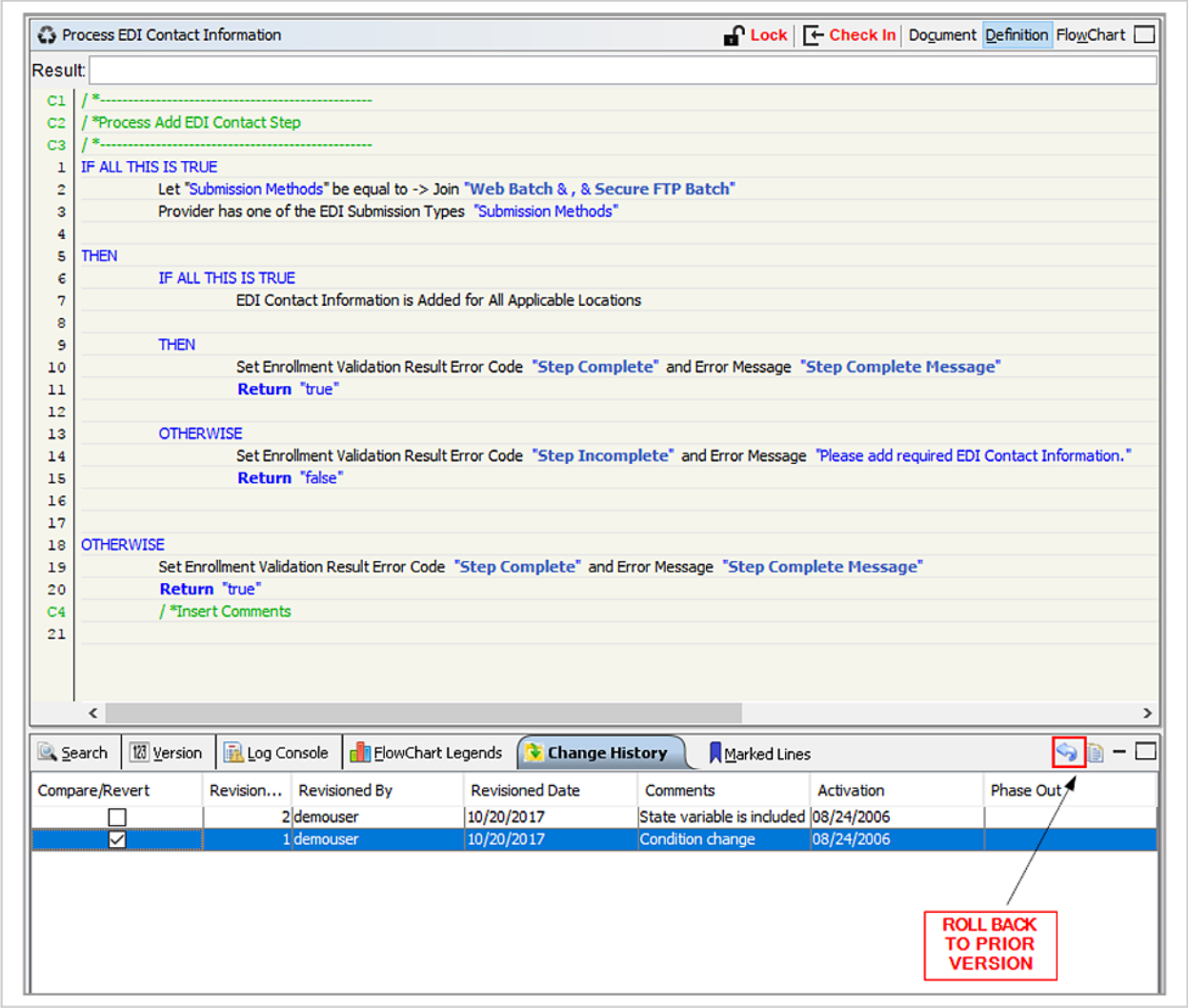
The Contractor shall provide the ability to allow multiple users to work concurrently on different parts of the same rule base.

RuleIT Composer is a multi-user client server application available to all users who need to work on the rule base. The application provides the ability to allow multiple users to work concurrently on different parts of the same rule base. Users will check-out an individual rule while making changes and check-in once they are done with the updates. Rules checked out will not be available for editing by other users. This prevents version issues and ensure integrity of the rules.

BR11

The Business Rules Engine shall have the ability to rollback to prior versions of rules without impacting production rules engine availability and operations.

Rules change history is maintained and the users would be able to roll back to the previous versions when required, as shown in Figure 3.10.1-135. Rules are developed in the development environment and promoted to higher environments such as test, user acceptance, and production using the RuleIT Migrator. The rules migration process is performed during the scheduled deployment window and will not impact production rules engine availability and operations.



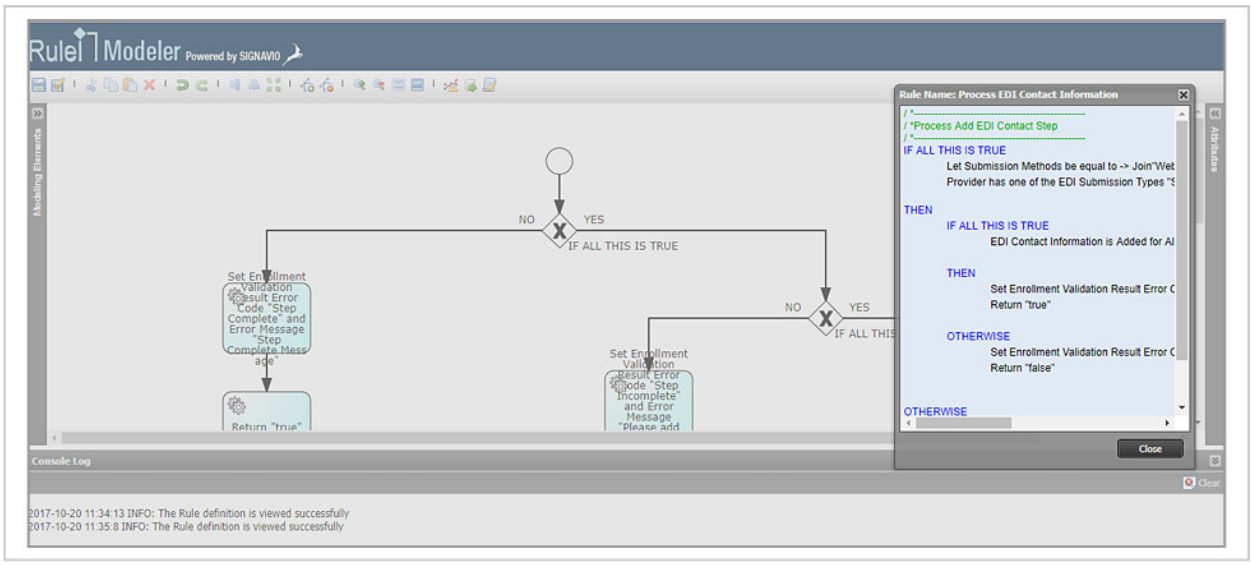
MTPSM-3-451

Figure 3.10.1-135. RuleIT Composer Change History Screen. RuleIT allows users to roll back changes and retrieve older versions of the rule.

BR12

The Contractor shall provide and maintain a graphical representation of business rule flow(s) and orchestration for all business rules

The graphical representation of the business rules flow is presented using the RuleIT Modeler is shown in Figure 3.10.1-136. The business rules flow could be altered using the modeling elements, and the user would be able to publish the rule and view the rule definition as English-like syntax.



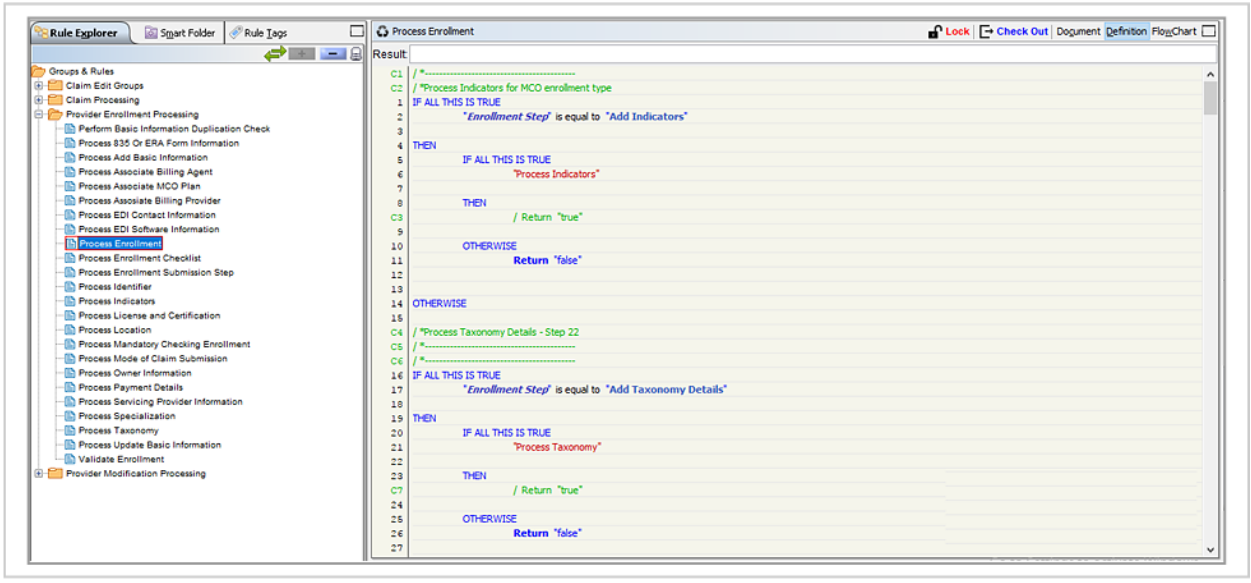
MTPSM-3-452

Figure 3.10.1-136. RuleIT Modeler Screen. RuleIT Modeler provides a graphical representation of the rules flows.

BR13

The Business Rules Engine shall have mechanisms to identify which rules are executed for each specific business process.

RuleIT uses a "sequential process" algorithm, in which the rule flow and the evaluation is controlled by the rule, its conditions, and the associated branching. This provides the user to identify and foresee the rule execution flow for the various business process as shown in Figure 3.10.1-137.



MTPSM-3-453

Figure 3.10.1-137. Rules Sequential Flow. Complex rule flows can be identified and implemented quickly and these rule flow are simple to read and edit.

BR14

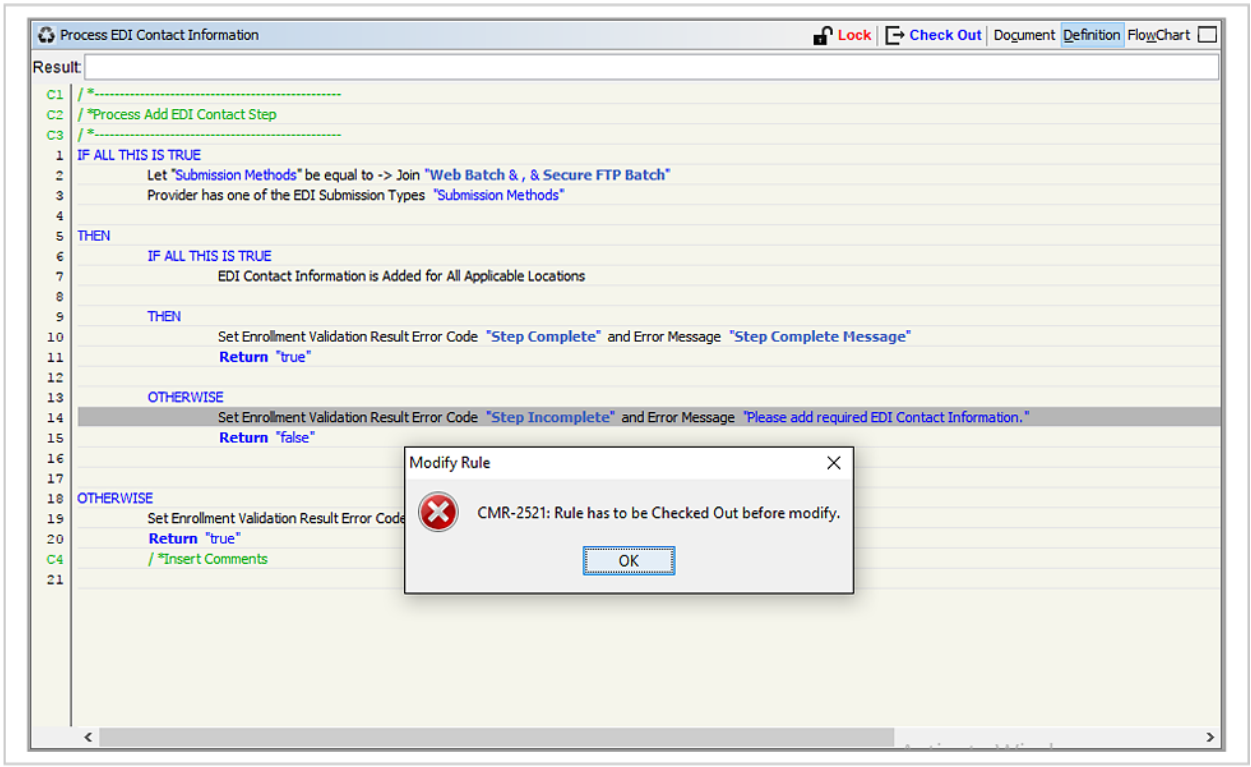
The Business Rules Engine shall be able to produce a report on rules passed or failed for all transactions.

RuleIT Processor has detailed logging capabilities built using the Log4j logging framework. The rules executed and details of whether they passed or failed during the transaction flow are logged using this framework. The logging levels can be easily configured during the deployment of the application. The logging level can be set to “INFO” level to track detailed rules execution flow; this level is recommended to be enabled during development and testing phases. In production environments, the level is set to “ERROR” level which disables detailed logging and improves performance of the application.

BR15

The Business Rules Engine shall send alerts to the appropriate resource for issues identified in the rules engine. The Contractor will take appropriate action to address any alerts or rule failures.

The user with the appropriate error codes is notified of RuleIT issues. These error codes are sent or shared, which helps the support team to take the appropriate action for quick resolution of the reported issues. Figure 3.10.1-138 shows the application alert messages along with the error code.



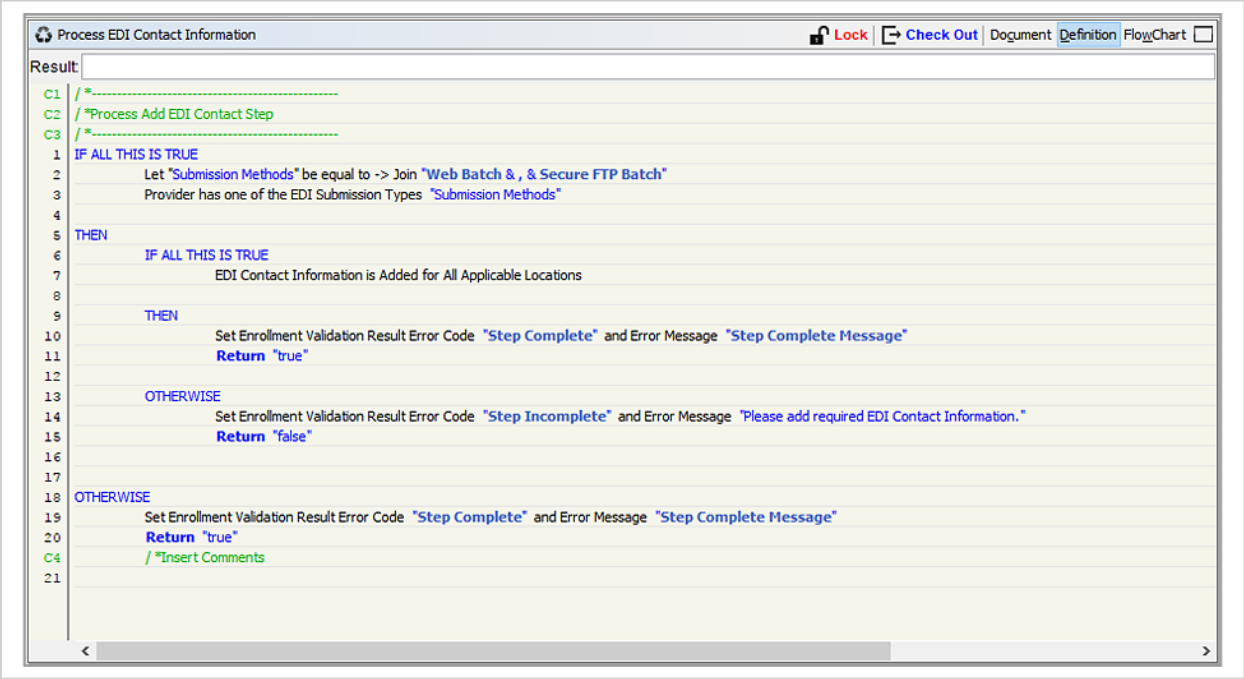
MTPSM-3-454

Figure 3.10.1-138. RuleIT Composer Alerts Screen. RuleIT issues are shown to the users with details of the errors.

BR16

The Business Rules Engine rules editor shall allow subject matter experts or technical resources to write natural language business rules (i.e. human readable).

Team CNSI has honed a balanced approach to manage the implementation of business rules via online configuration-driven tables and declarative English-like rules syntax in the rules engine. RuleIT Composer allows subject matter experts or technical resources to write natural language business rules. These rules are human-readable, as shown in Figure 3.10.1-139.



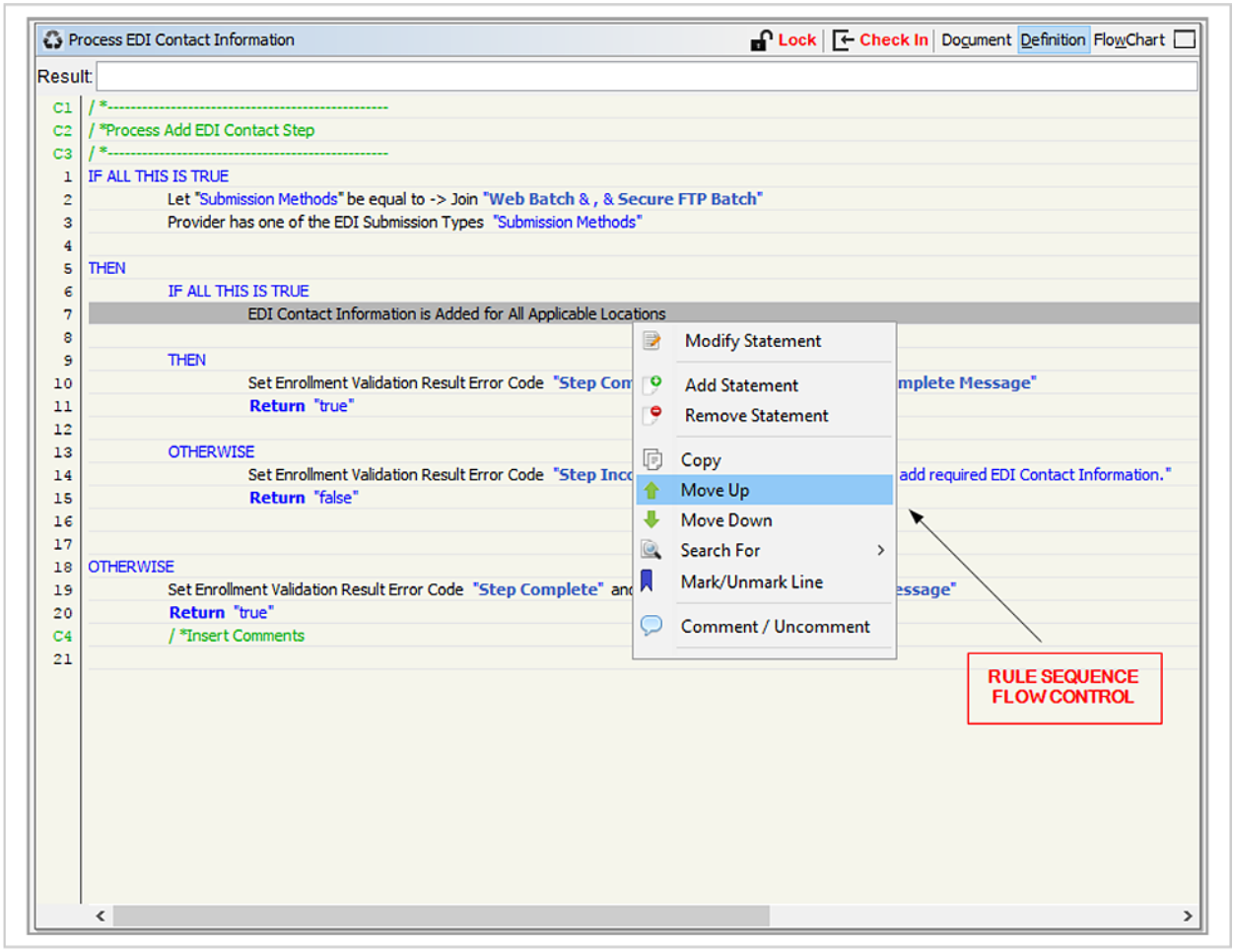
MTPSM-3-455

Figure 3.10.1-139. RuleIT Composer Rules Screen. RuleIT provides an intuitive English-like user interface and a decision tree model of implementation.

BR17

The Business Rules Engine shall provide the ability to prioritize, sequence, and allow administrators to control processing.

Unlike other rules engines, RuleIT uses a "sequential process" algorithm, in which the evaluation is controlled by the rule, its conditions, and the associated branching. Its flexible architecture lets a business analyst determine the sequence of rule evaluation, which simplifies setting up the processing chain more manageably. This is illustrated in Figure 3.10.1-140.



MTPSM-3-456

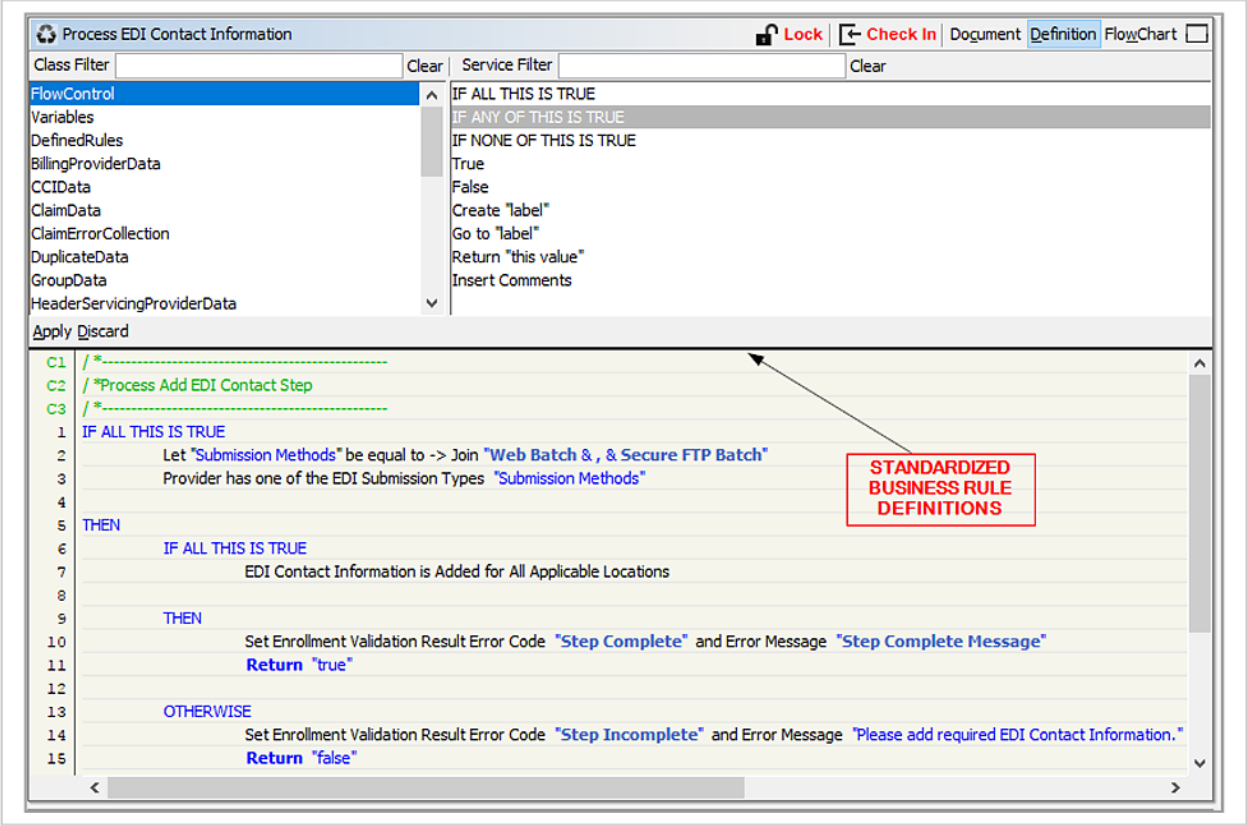
Figure 3.10.1-140. RuleIT Composer Rule Flow Configuration Screen. Users can author the flow and sequence of the rules using the rules composer.

The RuleIT Processor supports the ability to prioritize, sequence, and allow application administrators to control processing of rules engines resources. This is possible because the RuleIT Processor gets invoked from within the application as an Enterprise Java Bean (EJB) component.

BR20

Where applicable, the business rules engine shall use standardized business rules definitions.

RuleIT Composer provides comprehensive authoring capabilities that support standardization of the business rules definitions. The standardized business rules are available as a library of resources as internal services for users who are developing the rules. This is illustrated in Figure 3.10.1-141.



MTPSM-3-457

Figure 3.10.1-141. RuleIT Internal Services Screen. Users can search and use standardized business rule definitions while authoring the rules.

BR21

The Contractor's business rules shall execute in a runtime environment.

RuleIT was developed on the Java 2 Enterprise Edition (J2EE) platform architecture, making it portable across many hardware and software platforms. RuleIT Processor is the runtime rule evaluator or executor for rules defined in the RuleIT Repository. RuleIT Processor can be deployed on most Java application servers, and provides interfaces that integrates easily with other J2EE-compliant applications. RuleIT Processor is currently tested and certified on WebLogic, WebSphere, and JBoss runtime environments.

3.10.1.8 Enterprise Content Management

This section addresses Enterprise Content Management requirements for the Contractor's solution(s) and operations. The MPATH Integration Platform will include a centralized enterprise content management solution. The Contractor's solution will be required to send all documentation to the MPATH Integration Platform for storage in the centralized enterprise content management solution. The Contractor shall describe the proposed solution's capacity to configure, support and maintain an enterprise content management solution and the type of resource and necessary skill set(s) required for enterprise content management and configuration. Describe the change management processes associated with enterprise content management. In addition, the Offeror must describe their approach to meet each of the Enterprise Content Management requirements detailed in Attachment F, Requirements Matrix.

Team CNSI brings state-of-the-art technology and health care expertise to the MPATH document and content management implementation. Team CNSI understands the need for a comprehensive document management system that is configurable, centralized, integrated, and secure, and provides the agility required to adapt to change while assuring accuracy and timeliness of information. The tool chosen must support all facets of document management including common and generic features like ingestion, storage, retrieval, filing, and retention. Integrated security features must ensure that documents are accessible and distributed only to authorized users. It must also include a workflow feature that can handle a complex review and approval process for document and/or template creation by the Department.

The Team CNSI Advantage

Team CNSI's evoBrix PMIS solution uses IBM FileNet as the Content Management solution, which will be the single repository for all system documents, system generated correspondences, and provider support materials.

- It supports high-speed ingestion and retrieval of imaged and non-imaged content
- Electronic documents are stored in their native formats which reduces errors in transformation, and supports future accessibility and migration to other platforms
- It supports all facets of document management, including ingestion, storage, retrieval, filing, and retention. The integrated security features ensure that documents are accessible and distributed only to authorized users

MTPSM-3-023

The evoBrix Provider Management Information System (PMIS) seamlessly integrates with the FileNet content management solution by IBM, which is Team CNSI's Document Management System (DMS) and will serve as our Enterprise Content Management (ECM) tool. The evoBrix DMS solution will send all documentation to the MPATH Integration Platform for storage in the State's centralized ECM solution. The evoBrix DMS platform has integrated technology frameworks atop FileNet to provide advanced document management features and functionality that meet DPHHS requirements. The evoBrix DMS will be the repository for all system documents and provider support materials, and supports high-speed ingestion of imaged and non-imaged content through a series of tuned processes. Unlike other document management solutions, electronic documents are stored in their native formats. This reduces errors in transformation and supports future accessibility and migration to other platforms. The evoBrix DMS is a configurable, integrated, and secure solution that provides the agility required to adapt to change, while assuring accuracy and timeliness of information. The evoBrix DMS supports all facets of document management, including common and generic features like ingestion, storage, retrieval, filing, and retention. The integrated security features ensure that documents are accessible and distributed only to authorized users.

FileNet Security

Content Platform Engine is the core component of IBM FileNet, using which an administrator can create and manage document classes, properties, storage, and metadata that form the foundation of the FileNet ECM solution. Content Engine does not implement its own authentication module but uses the application server's authentication mechanism. Before clients can log in to a Content Engine server, the application server's authentication providers must be configured to point to specified directory servers where security objects, such as realms, groups, and users, are stored.

A directory server is divided into partitions, each of which is called a naming context (or namespace). There are different types of naming contexts, such as the configuration naming context, which holds configuration information, and data naming contexts, which contain all directory data. Each data naming context is defined as a Content Engine realm and each realm contains groups and users.

A User object exists in the Content Engine Realm as part of the security interface that allows a user access to a specific Content Engine resource. A Group object maps to a set of users and access rights

(permissions) are assigned to individual users and/or groups. FileNet implements role based security by mapping permissions to groups as opposed to individual users.

DMS Usage

The evoBrix PMIS letters and provider supporting documents will be archived in the evoBrix DMS and accessed through the evoBrix PMIS module's web interface or printed on demand. The flexibility of the evoBrix DMS allows seamless integration with MPATH Integration Platform. A copy of the enterprise content will be sent for storage in the centralized enterprise content management solution, in addition to FileNet. Figure 3.10.1-142 illustrates the usage of FileNet for archival, storage, and search of user supplied documents and system generated letters.

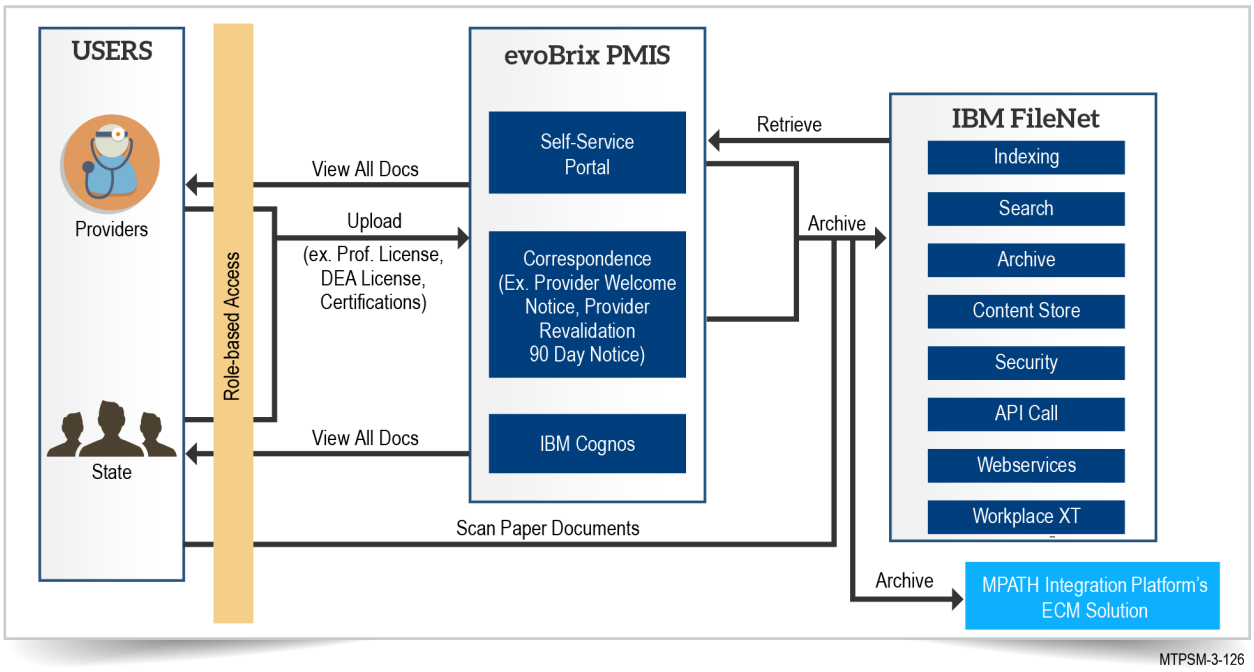


Figure 3.10.1-142. evoBrix PMIS Enterprise Content Management. This diagram shows how users interact with the evoBrix PMIS and directly with FileNet to archive and retrieve correspondences.

Providers upload documentation in support of their enrollment application, such as a copy of their license and of any certifications. State staff also upload documentation on behalf of the providers. The evoBrix PMIS allows the providers to submit the enrollment application through multiple channels, including the secure web portal, email, traditional mail, phone, or fax. Applications received as an email attachment, by fax, or by traditional mail will be scanned or manually entered into the system by the business operation staff. The image of the paper application will be uploaded to the system and linked to the application record. When the user(s) invoke the upload functionality, the evoBrix PMIS internally calls the FileNet API to archive the uploaded document within the DMS and index the document based on pre-configured parameters, to aid in document retrieval later. The evoBrix PMIS-generated correspondence letters are also archived within the DMS by default.

The FileNet Java API is an interface-based API that provides access to the full capabilities of the Content Engine. The FileNet P8 Platform also includes web services for the Content Engine, which are compliant with WS-I Basic Profile 1.0 and WS-Security. The evoBrix DMS platform is built on these features to optimally leverage the functionality of Content Engine APIs for effective document management.

Resource Support

Following are the necessary skillsets that are required to configure, support, and maintain an enterprise content management solution:

- Extensive experience in FileNet Core Component installation and configuration
- Experience performing administrative tasks including
  - Configuration of Content Engine (Content retrieval / Contact Search Service / Content Collector), Application Engine, Enterprise Manager, Content Navigator
  - Creation and maintenance of Object Stores
  - Workflow management
  - Security enablement
- Perform deployments to QA and Production Environments

Team CNSI will utilize resources for the above skillsets to effectively manage the setup, configuration, administration, and maintenance of the evoBrix DMS solution.

Change Management

Team CNSI will follow the standard Change Management process for Enterprise Content Management area. Our change management process includes methods for communicating, evaluating, and approving or rejecting changes throughout the project. This process ensures that proposed changes are evaluated for impact to system, schedule, scope, cost, and resources. This facilitates informed decision-making by all parties involved in the change. As a part of our Change Management process, a log of changes is maintained in the project repository and indicates the disposition and status of all change requests. A similar process is instituted to handle changes post-implementation. For more details on change management, please refer to Section 3.10.2.1 Project Management.

ECM02

The Contractor's ECM solution must be able to support all common document types (i.e., Word, PDF, Visio, Excel, PowerPoint, TIFF, and JPEG) and must integrate seamlessly with the most common document viewing and editing tools used by the Department.

The evoBrix PMIS DMS solution supports the storage of a wide variety of document formats including but not limited to Word, PDF, Visio, Excel, PowerPoint, TIFF, and JPEG. The documents are downloaded directly on to user machines. Alternately, users also utilize the document viewing capabilities of IBM Content Navigator to view the documents.

Users access, manage, and use the downloaded documents from desktop and mobile devices, anytime and from anywhere across the enterprise. Users edit documents using standard document viewing and editing tools used across various enterprises such as PDF and Microsoft Office tools, create new documents using document templates, and rotate, cut, or split documents and check in changes back to the repository.

ECM03

The Contractor's ECM solution must allow users to access documents from any platform with all core features available across platforms (desktop, web, mobile). The ECM must allow users to view all

documents and images without the use of plug-ins.

IBM FileNet comes with a Content Navigator tool that enables users to access, manage and use enterprise content across platforms including desktop, web, and mobile using a standard web browser, without requiring the use of a plugin. Documents can also be downloaded using Content Navigator based on individual needs.

ECM04

The Contractor's ECM solution must support role-based control and access of documents, as well as including the following:

a. Granular authorizations for access, preview, editing and sharing.

b. Automatic access expirations for documents deemed sensitive by the Department.

c. Content security policy enforcement, such as unusual document access activity and sharing of documents with sensitive information of uploads/downloads of prohibitive data.

The evoBrix PMIS DMS solution supports defining role based access using the concept of Groups or Business Areas. Only authorized staff members will be allowed to upload, access, and view documents through evoBrix PMIS screens relevant to their Business Area. Access can also be customized and controlled at the data element/field level to meet federal and state security requirements.

Users attempting to access documents, including shared documents, are subject to access restrictions and policies specific to the document being accessed, based on roles and privileges.

Auditing is supported at various levels of granularity, including object stores, document types, and document properties, to track critical activities on custom or system events that occur for objects. Team CNSI will work with DPHHS to create an auditing framework, and track events pertaining to security, content management, and business transactions, to enforce security policies and track unusual activity.

The evoBrix DMS solution will enforce automatic document expirations in conjunction with document retention policies as defined by State. Team CNSI will work DPHHS in identifying the content deemed sensitive and setup document expiration and removal.

This comprehensive solution enables PMIS to streamline records-based activities, help enforce compliance with retention policies and track unusual activity. Using FileNet, the evoBrix PMIS solution captures, classifies, stores, and disposes of electronic records according to regulatory requirements.

ECM05

The Contractor's ECM solution must include a flexible search engine, including document and content search capabilities.

The IBM Content Navigator is equipped with several content search options for users, including text search and property search using the indexed parameters. The searches are performed against one or more Document Classes and can include or exclude certain terms, match terms exactly, or search within a specific proximity of words.

Documents are stored in the evoBrix DMS solution and tagged with appropriate metadata or document properties, that serve as index parameters. These are used to search for and retrieve specific documents later. Document Classes are entities (or document types) that are predefined with a set of index parameters at the time of creation, to store specific metadata, along with any constraints that apply to the index parameters.

Figure 3.10.1-143 shows the landing page of the IBM Content Navigator, which is customizable by user, and Figure 3.10.1-144 shows the search screen, which users can use to search for specific documents.

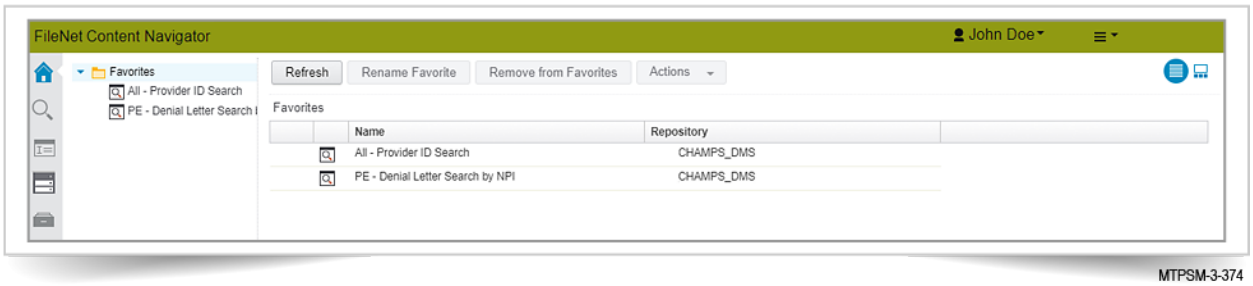


Figure 3.10.1-143. evoBrix DMS Solution - IBM Content Navigator. The IBM Content Navigator Home page view.

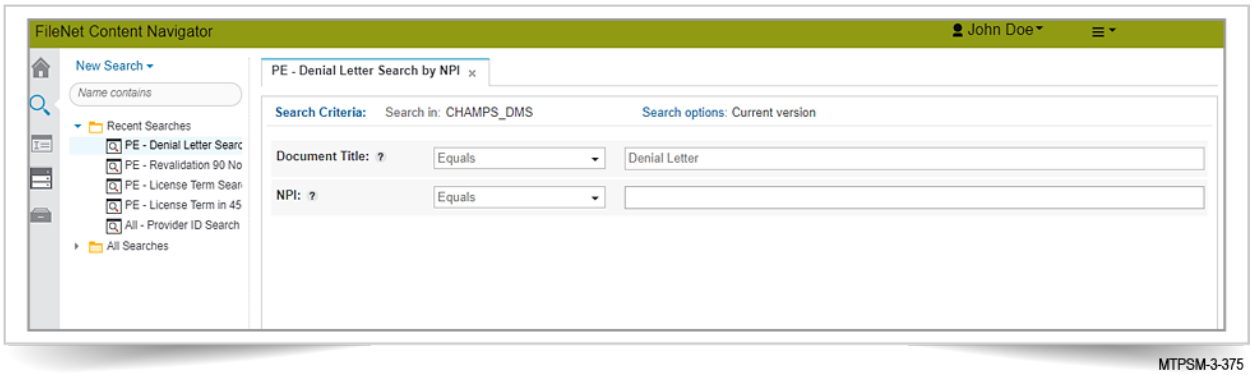


Figure 3.10.1-144. evoBrix DMS Solution - IBM Content Navigator. Search screen that allows users to search for specific documents.

ECM06

The Contractor's ECM solution must allow users to associate metadata with documents.

All enterprise content is indexed and stored with associated metadata as part of the evoBrix PMIS DMS solution. The solution supports a wide range of metadata, including character metadata and dates. These metadata are leveraged during searches and will be indexed for enhanced performance. Associating metadata and indexing are key features in evoBrix PMIS DMS solution's ability to scale and handle large volumes of documents in a growing enterprise.

ECM07

The Contractor's ECM solution must support simple integration with scanning solutions (support for bulk-scanning).

The evoBrix DMS solution integrates with fax/scanning solutions and processes bulk documents based on State requirements. The solution scans bar codes, associates metadata to scanned documents, and stores them in ECM.

The evoBrix DMS solution integrates with most fax/scanning hardware and derives index parameters based on barcodes and coversheets. Team CNSI has extensive expertise in fax and scanner integration, including with our current client, State of Michigan MDHHS, which uses RightFax and high-speed scanners for document intake.

ECM08

The Contractor's ECM solution must support version control.

The evoBrix DMS solution supports maintaining the history of changes to a document and controls the access users have to change the content of a document at a particular point in time. The set of versions for a single document is maintained as a version series. Users have the capability to check-out documents, perform revisions, and check them in, and the changes are maintained through version history.

Figure 3.10.1-145 shows the version history of a sample document.

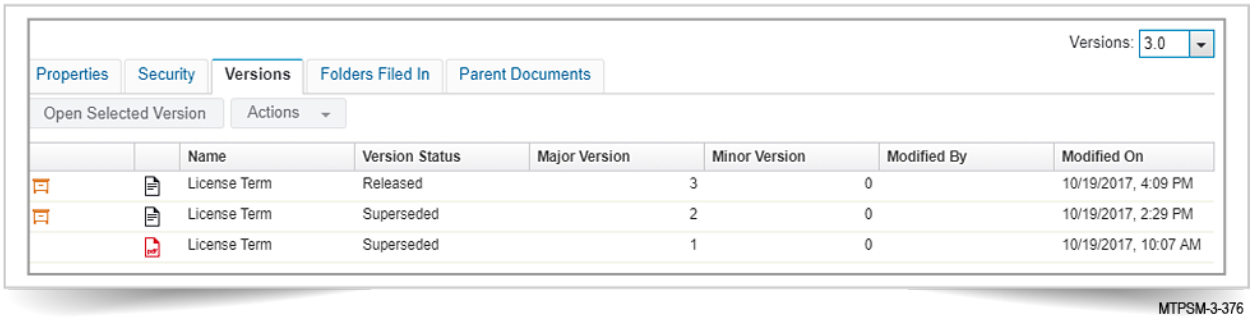


Figure 3.10.1-145. evoBrix DMS Solution. This screenshot shows the version history of a document.

Figure 3.10.1-146 and Figure 3.10.1-147 highlight the check-out and check-in functions that can be performed against a document.

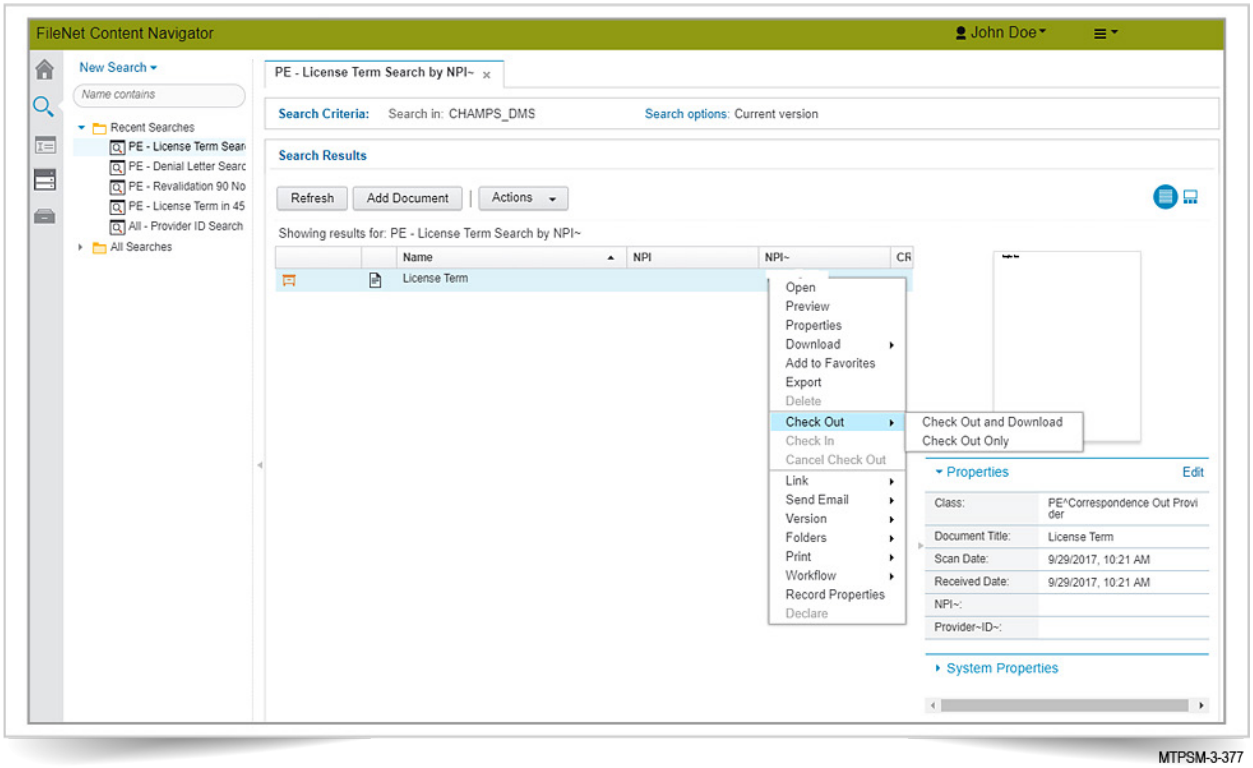


Figure 3.10.1-146. evoBrix DMS Solution. This screenshot shows the permissible actions against a document, including the check-out action.

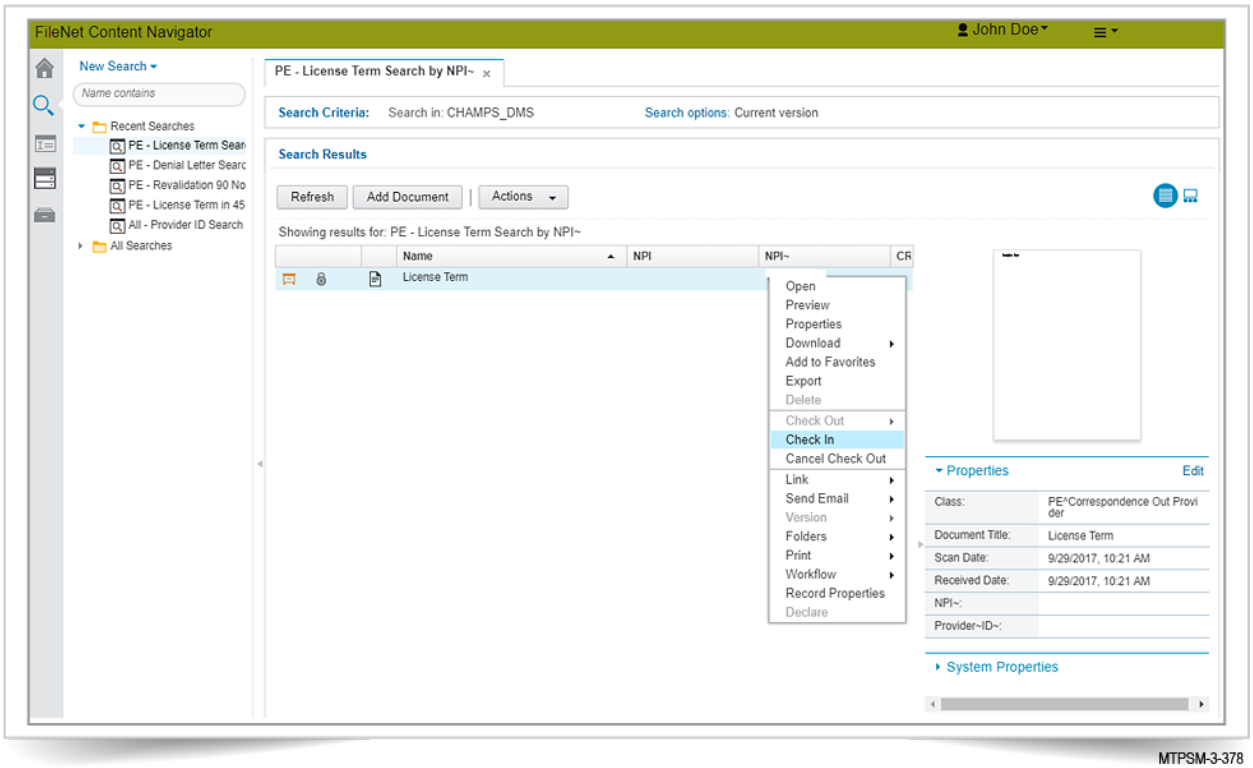


Figure 3.10.1-147. evoBrix DMS Solution. This screenshot shows the option to check-in a document.

ECM09

The Contractor's ECM solution must be configurable to comply with the Department's document retention policies.

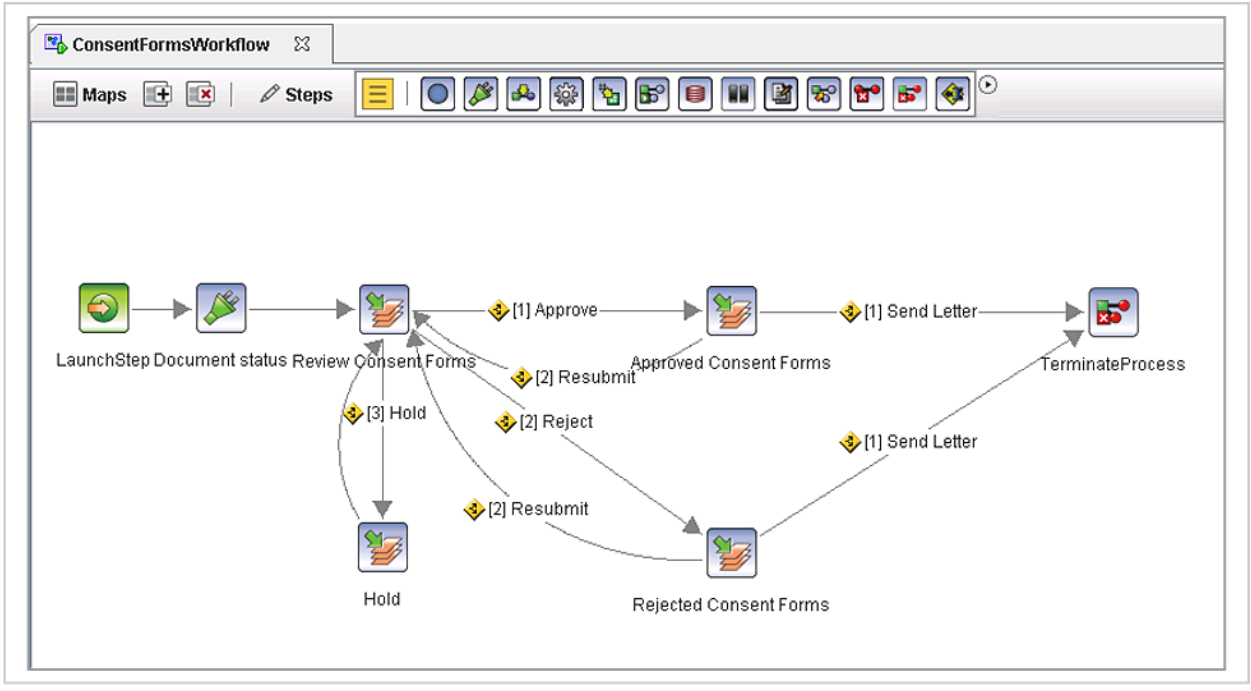
The evoBrix PMIS DMS solution supports configuring and streamlining records-based activities and enforces compliance with retention policies in accordance with State and Federal regulatory requirements.

Team CNSI will work with DPHHS to determine the appropriate retention policies and configure the evoBrix DMS platform to support the same.

ECM10

The Contractor's ECM solution must support document workflows with review/approval ability with digital signature support (e.g., scan notifications).

The evoBrix PMIS DMS solution provides the ability to create, modify, manage, analyze, and simulate business processes, or workflows, that are performed by applications, enterprise users, and external users such as partners and customers. Figure 3.10.1-148 illustrates a sample workflow configuration. Complex business rules can be created with various routes between workflow steps. Work is managed in several types of queues, where users are provided with a set of tasks they need to perform.



MTPSM-3-419

Figure 3.10.1-148. evoBrix PMIS DMS Workflow Configuration. This figure shows a sample workflow configuration.

The evoBrix PMIS DMS solution can leverage IBM Signature Foundation for FileNet Content Manager, which provides a toolbox to create a solution for storing digitally signed documents.

ECM11

The Contractor's ECM solution must scan all uploaded documents for viruses prior to storage.

The evoBrix PMIS DMS solution offers support for scanning the uploaded documents for viruses based on State requirements, by integrating with Symantec Protection Engine 7.8 software through API calls. User uploaded documents will be scanned prior to being archived to the document repository, thereby ensuring the safety and security of the documents.

ECM12

The Contractor's solution shall be able to index, link and display incoming correspondence or uploaded documentation with the entity record.

The evoBrix DMS solution has the capability to integrate with a fax/scanning solution, read barcodes, and store the incoming correspondence or uploaded documentation into FileNet, along with index parameters corresponding with the documents. The documents can be linked to the corresponding business entities based on the index parameters.

Team CNSI will work with DPHHS to determine the integration points for State fax and scanner hardware, and establish processes to archive the incoming correspondences and documentation to the evoBrix DMS.

ECM13

The Contractor's solution shall send all documentation to the Systems Integration Services module for storage in the centralized ECM.

In addition to utilizing FileNet, the evoBrix PMIS DMS solution comes with the capability to interface with additional storage and content management systems, including the centralized ECM solution that is part of MPATH Integration Platform.

The evoBrix PMIS DMS solution will send a copy of all document and image content that is uploaded and scanned, and a copy of evoBrix PMIS generated correspondences, to MPATH Integration Platform's centralized content management system.

ECM14

The Contractor's solution shall have an integrated electronic document management solution to meet the business needs of the State's enterprise.

The evoBrix PMIS DMS solution provides an integrated electronic document management solution, that uses IBM FileNet in the backend, to support the business needs of the State's enterprise, as outlined against specific content management requirements.

ECM15

The Contractor's solution shall accept, record, store, and retrieve freeform or HIPAA attachment documents submitted with or in reference to claim submission activity (e.g. operative reports, occupational, physical, and speech therapy reports, durable medical equipment and warranty data, manufacture's tracking data for implants, waivers and demonstration specific requirements).

The evoBrix PMIS DMS solution has ability to accept, record, store, and retrieve attachments during enrollment process.

The evoBrix DMS solution is optimized towards document types and index parameters related to the provider enrollment process, utilizing index parameters such as NPI and Taxonomy. The evoBrix DMS is flexible and can be customized to support multiple document types and their associated index parameters. This is leveraged to define Claim specific document types and index parameters such as Transaction Control Number (TCN) and Beneficiary information, to hold claim-specific documents. A wide variety of file types and content is supported by evoBrix DMS thereby enabling the support for freeform data or attachments containing supporting documents.

ECM16

The Contractor will configure, support and maintain Enterprise Content Management (ECM) functionality (including Document Management and Workflow) to meet the business needs of the State's enterprise.

Team CNSI will configure, support, and maintain the evoBrix DMS solution that serves as our ECM tool. The evoBrix DMS solution has integrated technology frameworks atop FileNet that provide advanced document management features and functionality to meet the business needs of the State. It provides the ability to create, modify, manage, analyze, and simulate business processes, or workflows within document management.

The key features of the evoBrix PMIS DMS solution are high-lighted below:

- The evoBrix DMS supports all facets of document management, including common and generic features like ingestion, storage, retrieval, filing, and retention
- The evoBrix DMS will be the repository for all system documents and provider support materials
- It supports high-speed ingestion of imaged and non-imaged content
- All electronic documents are stored in their native formats, thereby reducing errors in transformation
- The integrated security features ensure that documents are accessible and distributed only to authorized users

3.10.1.9 Workflow

This section addresses Workflow requirements for the Contractor's solution(s) and operations. The MPATH Integration Platform will exchange data with all MPATH components to support enterprise wide automated business process orchestration. The Contractor's solution shall include a configurable workflow solution for process definition, execution, monitoring, and management. The Contractor shall describe the proposed solution's capacity to configure, support and maintain a workflow solution (i.e., add, modify, or remove/retire existing workflow configurations) and the type of resource and necessary skill set(s) required for workflow management. Describe the change management processes associated with workflow management. In addition, the Offeror must describe their approach to meet each of the Workflow requirements detailed in Attachment F, Requirements Matrix.

Team CNSI's integrated workflow management solution supports the State's desire for improved automation, reduced manual intervention, configurable work routing, and task management. The evoBrix Provider Management Information System (PMIS) delivers a proven workflow solution with table-driven configurable rules, task routing, assignment, and tracking capabilities.

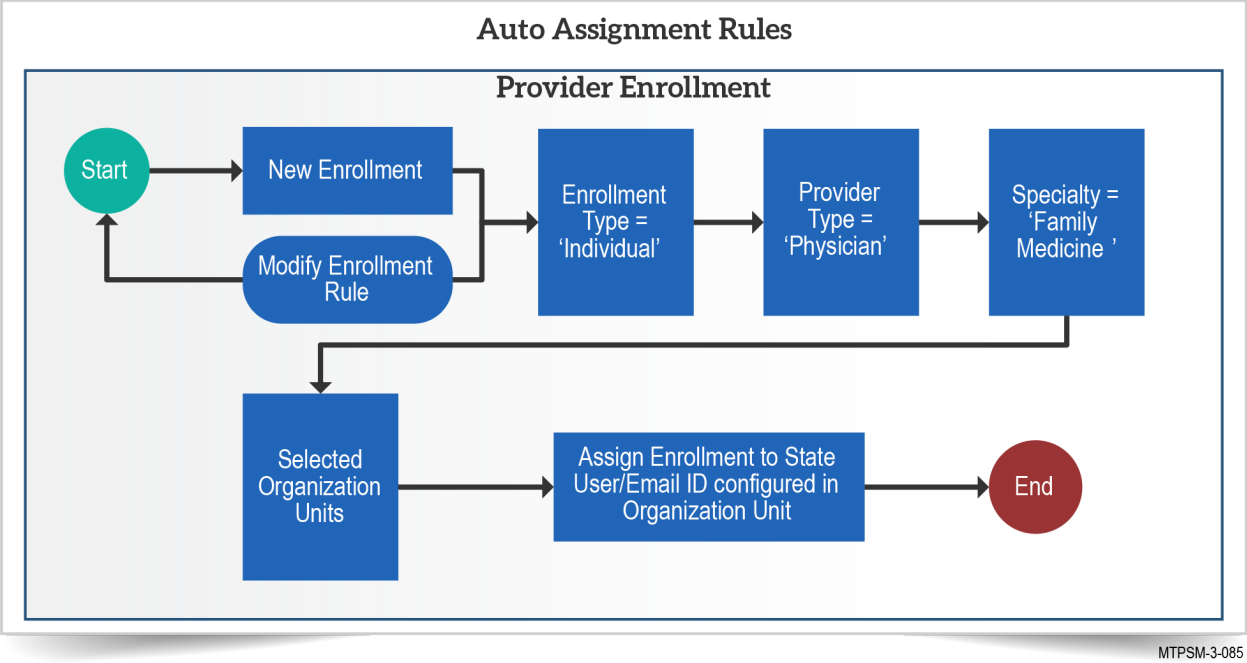
Team CNSI's evoBrix PMIS solution includes a configurable workflow process that provides the flexibility to define State-specific business process rules, as shown in Figure 3.10.1-149. Provider Enrollment applications can be forwarded to specific Business Organization Units and to a specific user within a group. Different combinations of Enrollment Types/Provider Types and Specialties can be configured to route the applications to departments specialized in that area.

The Team CNSI Advantage

Team CNSI's integrated workflow management solution supports improved automation, reduced manual intervention, configurable work routing, and task management. The workflow models are designed and developed in accordance with industry best practices for workflow process modeling.

- Workflow Management solution provides configurable work distribution and re-distribution based on work type, worker skill, priority, and age of work
- It comes packaged with run-time control functions for managing the workflow process in the operational environment
- It supports the generation of alerts and notifications to system users
- The workflow engine processes work queues in real time, assigns tasks, sends notifications, and provides escalation to management and/or supervisors

MTPSM-3-024



MTPSM-3-085

Figure 3.10.1-149. evoBrix Configurable Workflow Process. evoBrix PMIS Workflow solution provides the flexibility to configure and automate business processes.

Workflow Features

Real-time Configuration

The evoBrix PMIS workflow engine processes work queues in real time, assigns tasks, sends notifications, and provides escalation to management and/or supervisors. State-authorized users will receive notification messages to their "My Inbox" section and will be able to navigate directly to the applications that need action. evoBrix PMIS online screens provide users the ability to modify any

existing rule and allow applications to be routed to another business unit/owner. New rules can be defined at any point, allowing additional enrollments to be assigned to the right business units or owners.

User Notifications

User tasks and to-do lists are accessible via the online screen "My Inbox." Users will be able to see if any applications (New, Modification, and Revalidation) are available and need any action. Users have the option to click on the appropriate section and navigate directly to the details. Access to the content can be configured using the evoBrix Role Based Access Control (RBAC) security framework that allows or restricts access to specific screens within evoBrix PMIS.

The user will be able to view task items in the task list page in evoBrix PMIS and act upon the queued task. When the user completes the task, the system will generate notification that will trigger the completion of the step. The evoBrix workflow framework supports coordination of the interactions between State staff to manage the work required to execute a process including:

- Work queues for each participating staff member
- Alerts to the presence of work
- Status indicators to mark work in progress or completed
- Provide a task-reminder and/or To-Do-List function
- Log all instances of workflows that are executed

Reporting

The evoBrix PMIS reporting framework houses various Provider Enrollment reports that provide statistics of New Provider Enrollment and Enrollment Modifications on a daily, weekly, and yearly timeframe. Reports are scheduled and are available for State-authorized users through online screens.

Online Screens

The evoBrix PMIS workflow rules can be configured using online screens as shown in Figure 3.10.1-150 and Figure 3.10.1-151. State-authorized users are able to maintain and modify rules based on business process requirements. The evoBrix PMIS screens present users with a visual representation of all workflow rules and how they are being used throughout the system. Using online screens, State-authorized users are also able to view pending applications and re-route them to another business unit or owner.

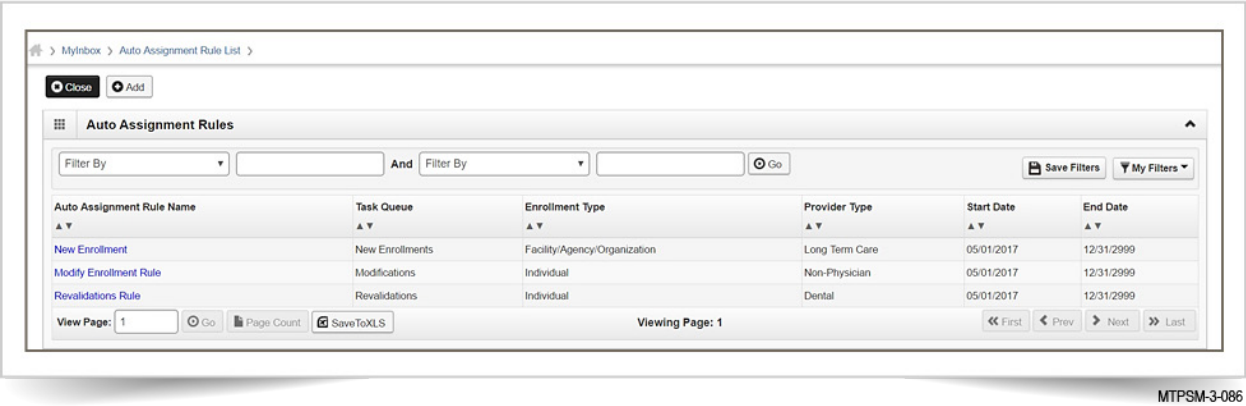


Figure 3.10.1-150. Auto Assignment Rules Screen. This screen allows business users to define/modify the workflow process for New Provider Enrollment applications.

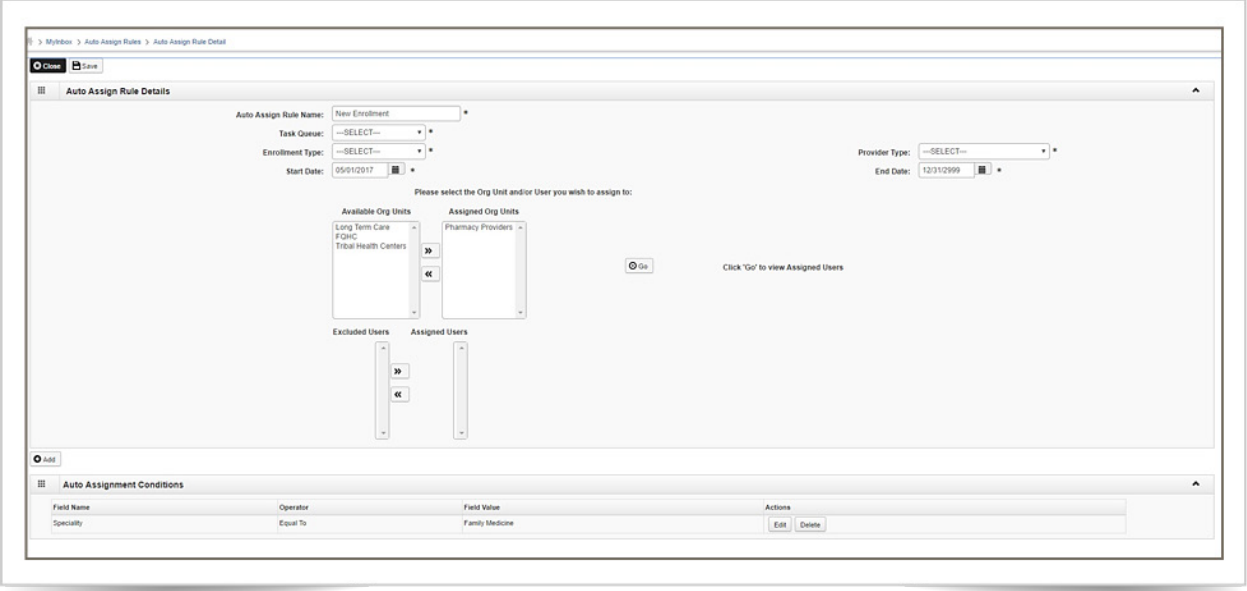


Figure 3.10.1-151. Auto Assignment Rule Details Screen. This screen allows business users to assign Organization Units to a workflow process.

Resource Support

Team CNSI will utilize resources with the following skill sets to effectively manage the configuration, administration, and maintenance of the evoBrix Workflow solution.

- State staff who will define the process flows and workflow rules will need training on the evoBrix Workflow solution to ensure they are conversant with the system capabilities
- Familiarity with BPMN 2.0 notation is helpful but not required

Change Management

Team CNSI follows the standard Change Management process for the evoBrix Workflow. Our change management process includes methods for communicating, evaluating, and approving or rejecting changes throughout the project. This process ensures that proposed changes are evaluated for impact to system, schedule, scope, cost, and resources. This facilitates informed decision-making by all parties involved in the change. As a part of our Change Management process, a log of changes is maintained in the project repository and indicates the disposition and status of all change requests. A similar process is instituted to handle changes post-implementation. For more details on change management, please refer to Section 3.10.2.1, Project Management.

WKF01

The Contractor's workflow solution shall provide a runtime engine that facilitates process events throughout the work type lifecycle.

The evoBrix PMIS workflow engine processes work queues in real-time, assigns tasks, sends notifications, and provides escalation to management and/or supervisors. Authorized users can view their task item in the task list page within evoBrix PMIS and act upon the task. When the user completes the

task, the system generates a notification that triggers the completion of the step. The evoBrix PMIS workflow framework supports coordinating the interactions between State staff to manage the work required to execute a process. Workflow runtime engine automatically sets the state of the work item as configured.

WKF02

The Contractor's workflow solution shall provide configurable work distribution and redistribution based on work type, worker skill, priority, and age of work which can be configured by the State.

Team CNSI's workflow engine processes work queues in real-time, assigns tasks, sends notifications, and provides escalation to management and/or supervisors. Provider Enrollment staff receive notification messages in their "My Inbox" section and can navigate directly to the applications requiring action. evoBrix PMIS online screens provide authorized users the ability to modify any existing rule and allow applications to be routed to another business unit/owner. New rules can be defined at any point in time allowing subsequent enrollments to be assigned to the right business units or owners.

The evoBrix PMIS Workflow screens allow configuration of user assignments to work queues/locations based on attributes such as Enrollment Type, Provider Type, Specialties, as shown in Figure 3.10.1-151. These configurable screens support the business logic embedded in the rules. These can be maintained by the administrator in real time and support distributions of work based on workloads. evoBrix work management configuration screens support supervisory operations for the management of workflow including:

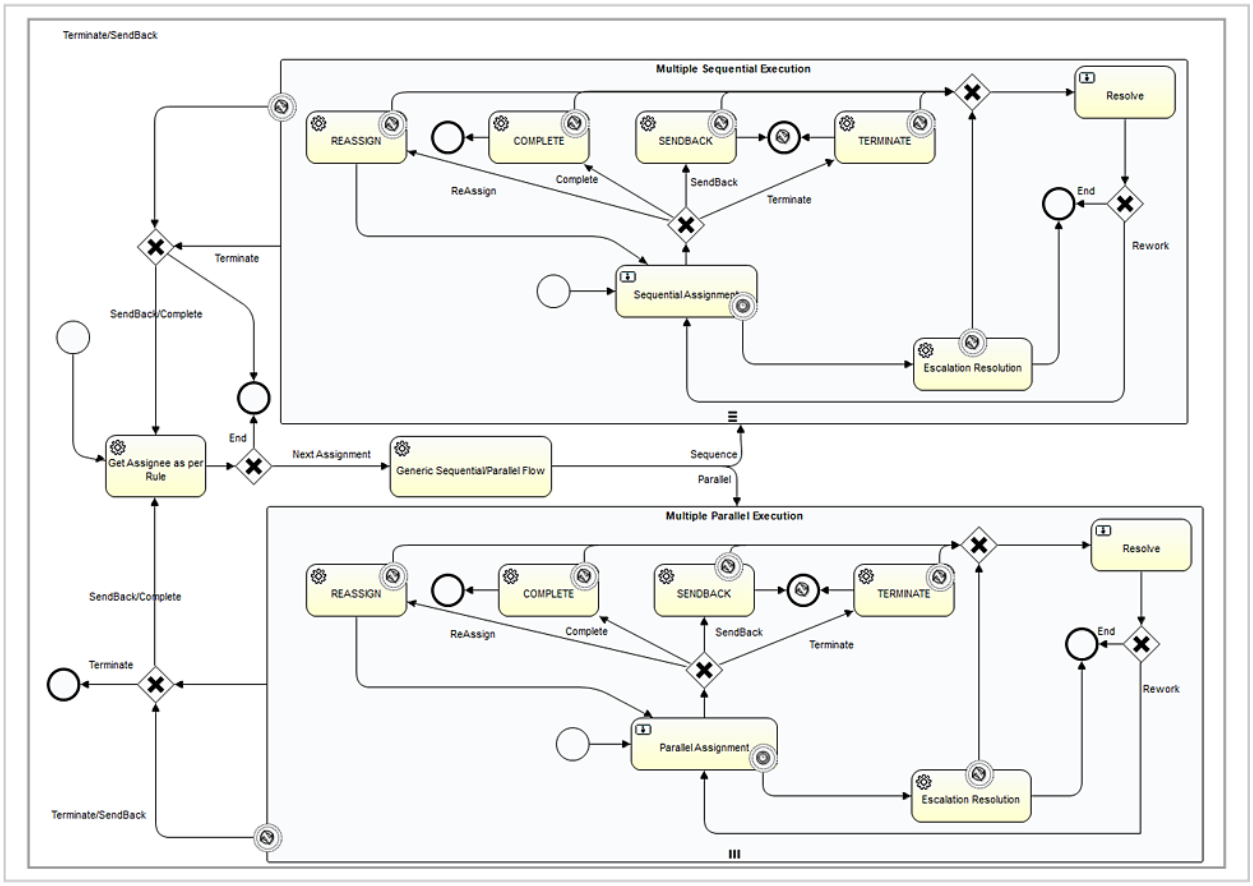
- Assignments/re-assignments
- Work allocation and load balancing
- Approval for work assignments and work deliverables via a tiered approach
- Ability to take necessary action or provide notification when corrective action is needed
- Intelligent work distribution and re-distribution based on work type, worker skill, priority, and age of work

WKF03

The Contractor's workflow solution shall provide a user-friendly Graphical User Interface (GUI) for process definition, execution, monitoring, and management. Support a role-based interface for process definition that leads the user through the steps of defining the workflow associated with a business process including processes that are managed by Department staff only, and that captures all the information needed by the workflow engine to execute that process.

The evoBrix PMIS workflow rules are configured using online screens. Authorized Provider Enrollment Staff are able to maintain rules based on business process requirements. The evoBrix PMIS Workflow screens present users with a visual representation of all workflow rules and how they are used throughout the system. Using online screens, Provider Enrollment staff can also view pending applications and re-route them to another business unit or owner.

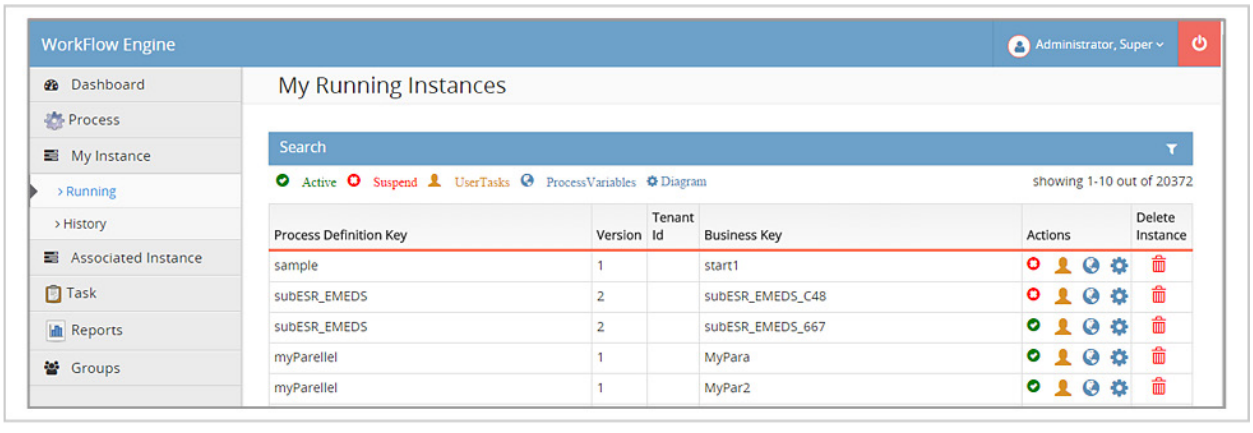
Figure 3.10.1-152 below shows a sample process definition as seen through the GUI by authorized users.



MTPSM-3-407

Figure 3.10.1-152. Sample Process Flow Definition. This screen provides a visual representation of a process flow definition using BPMN notation.

Figure 3.10.1-153 shows the screen through which administrative users can monitor and manage runtime workflow process executions.



MTPSM-3-408

Figure 3.10.1-153. Process Flow Monitoring. This screen allows administrative users to monitor and manage runtime executions of process flows.

WKF04

The Contractor shall support and assist the Department in mapping all business processes and subprocesses to the workflow application and in transitioning from manual to automated process execution.

Team CNSI will support DPHHS in mapping all business processes and sub-processes to evoBrix PMIS Workflow solution during the solutioning phase. A design artifact called Detailed System Design Document (DSDD) is produced as a result of the solutioning activities and will outline the solution for each business process in detail.

WKF05

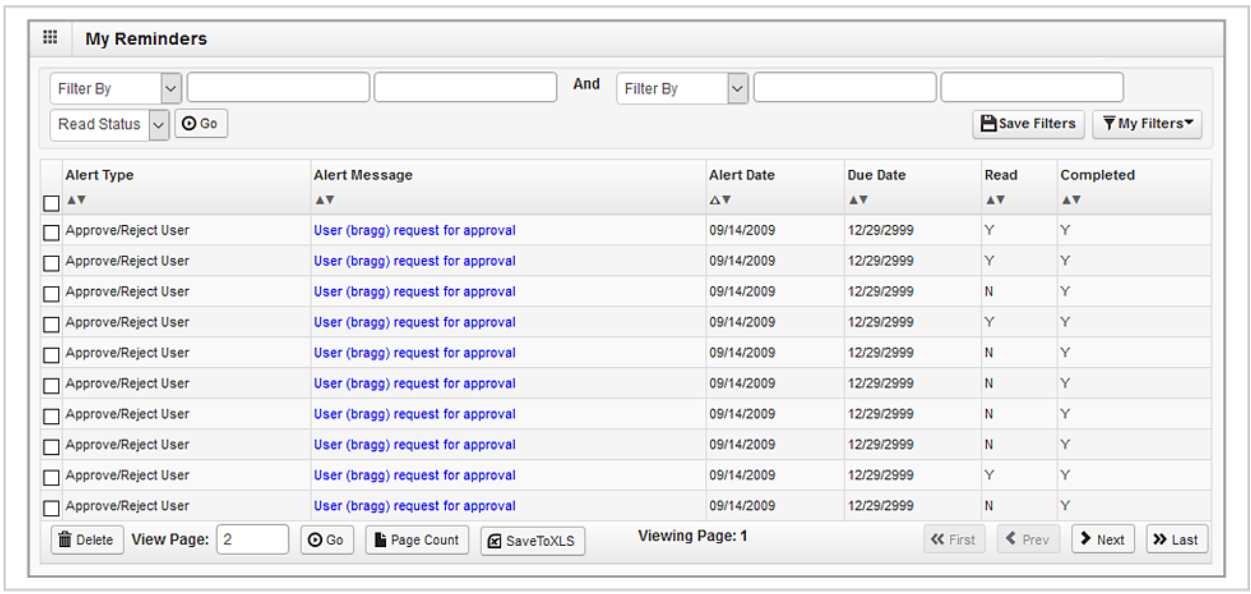
The Contractor's workflow solution shall support work-type processing that includes internal and external dependencies.

Team CNSI's workflow solution makes the business processes efficient, agile, and visible by ensuring that every process step is explicitly defined, monitored over time, and optimized for maximum productivity. Work flows can be configured to have internal and/or external dependencies. Each workflow can be comprised of one or more steps and dependencies can be defined at the task or workflow level.

WKF06

The Contractor's workflow solution shall provide the ability to view alerts and/or reminders by user, by work-type.

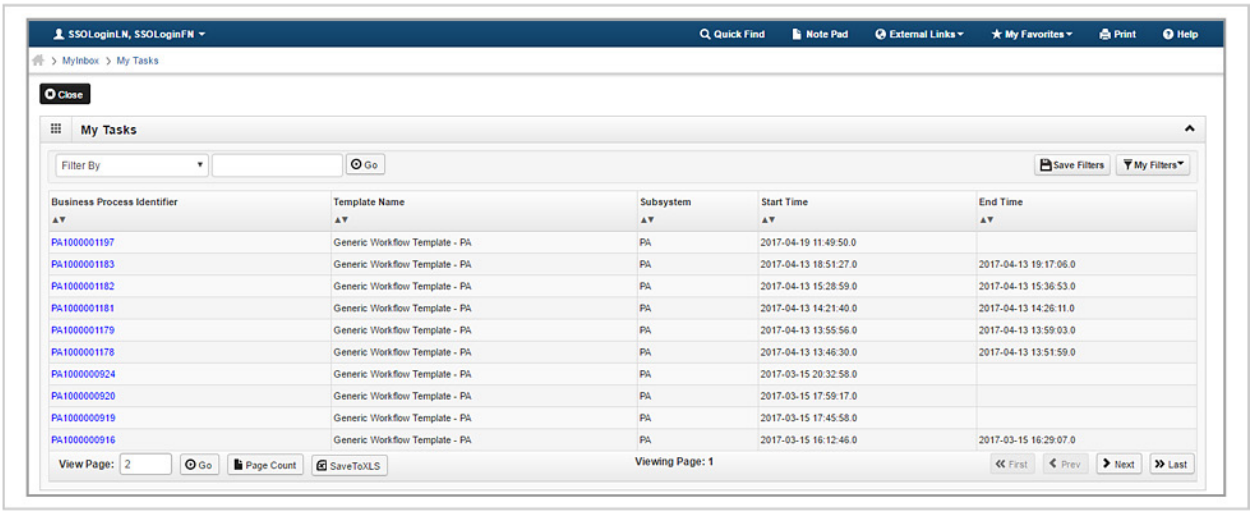
Team CNSI's workflow solution provides the ability to view alerts and/or reminders by user and by work-type. State staff receive notification messages in their "My Reminders" section, as shown in Figure 3.10.1-154, and can navigate directly to the item that needs action. The access to the content can be configured using evoBrix PMIS RBAC security.



MTPSM-3-409

Figure 3.10.1-154. Inbox View. This panel presents a list of alerts or messages for a specific user.

Figure 3.10.1-155 shows the view of the task list assigned to a user for their action.



MTPSM-3-410

Figure 3.10.1-155. Tasks View. This panel presents a list of tasks that are assigned to a specific user.

WKF07

The Contractor's workflow solution shall provide the ability to set alerts and or reminders by user, by work-type.

Team CNSI's workflow solution supports setting up alerts and reminders. Authorized users can view the alerts and reminders configuration and modify it by the work-types. The access to the content can be configured using evoBrix PMIS RBAC security framework.

WKF08

The Contractor's workflow solution shall automatically set the state of the work item, based on the processing steps when completed to provide transparent, accurate status of the work at all times.

Team CNSI's workflow runtime engine automatically sets the state of the work item as configured and automatically generates a notification that triggers the completion of the step.

WKF09

The Contractor's workflow solution shall provide supervisors access and control of work by type and by user.

Team CNSI's workflow solution is configurable through the backend to provide access to supervisors by users and by work-types through the evoBrix PMIS RBAC security framework.

WKF11

The workflow engine shall be configured to support capturing business processes using Business Process Model and Notation (BPMN) 2.0 or later, even if the engine uses a separate coding of the rules for execution.

Team CNSI's workflow solution runtime engine uses industry standard Business Process Model and Notation (BPMN) 2.0 for configuring workflow. Figure 3.10.1-156 shows a sample process flow depicted using BPMN.

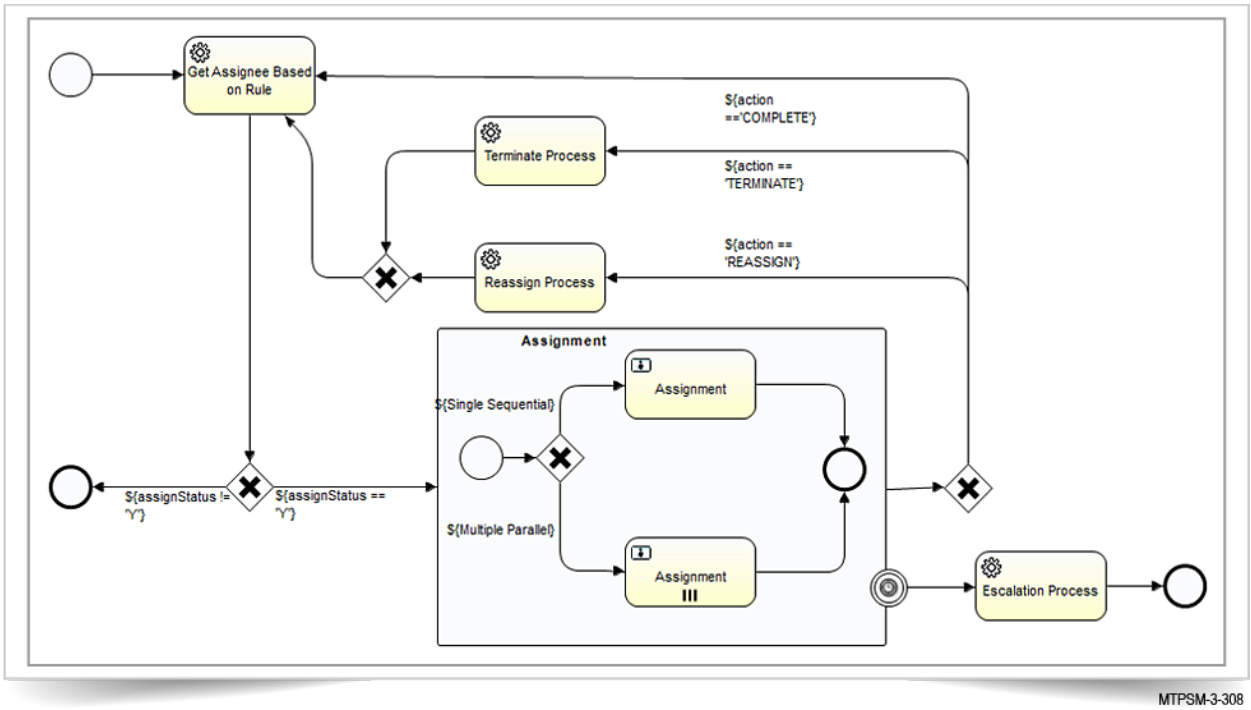


Figure 3.10.1-156. BPMN Notation Usage. A sample process flow using BPMN.

WKF12

The workflow engine shall be configured to support the establishment of work queues allowing in-process knowledge, data, and documentation to flow from one-solution to another solution.

Team CNSI's workflow solution supports work queues. Data and documents can be routed across work queues and through web services across different applications.

WKF13

The workflow engine shall be configured to support workflow access, assignments, and execution for all essential aspects of the business processes (e.g., provider enrollment, provider screening, client communications).

Team CNSI's integrated workflow management solution supports the State's goals of improved automation, reduced manual intervention, configurable work routing, and task management across different business processes. The evoBrix PMIS delivers a proven workflow solution with table-driven configurable rules, task routing, assignment, and tracking capabilities. With these features, evoBrix PMIS handles all aspects of workflow access, assignments, and execution of business processes, such as provider enrollment and provider screening.

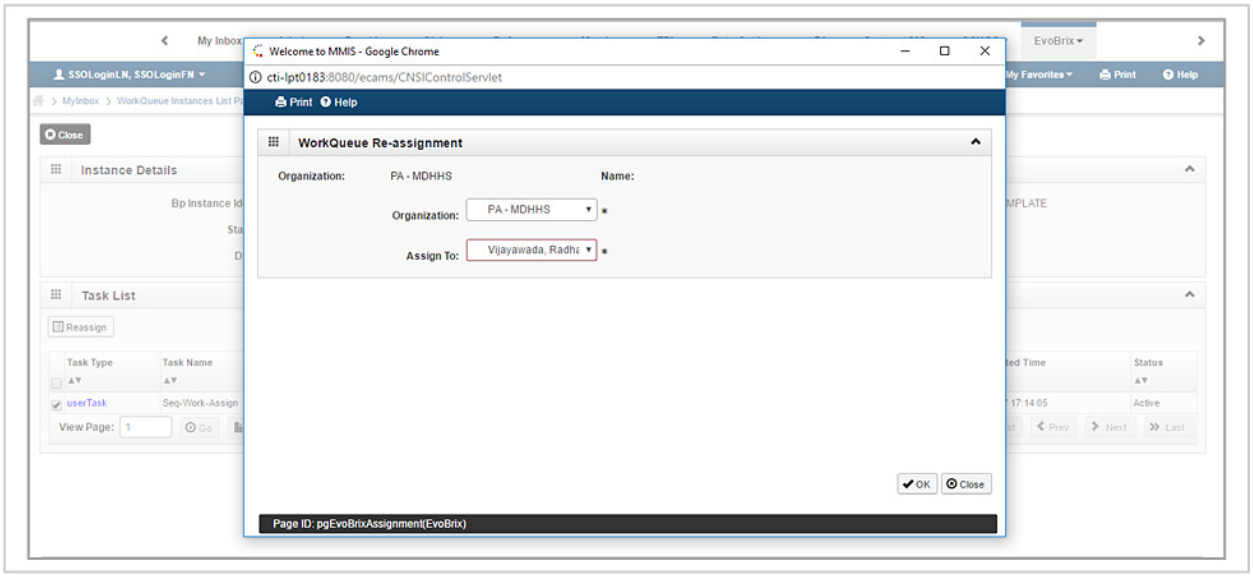
For instance, provider enrollment applications can be forwarded to specific Organization Units or to a specific user within a group. Different combinations of enrollment types/provider types and specialties can be configured to route the enrollment applications to departments specialized in that area.

WKF16

The Contractor's solution shall deliver automated business process/workflow management to support the establishment of work queues via an assigned worker portal allowing in-process knowledge, data, and documentation to route from one worker's queue to another as well as across solutions. The Contractor's solution shall ensure compliance with defined processes.

Team CNSI's workflow solution supports work queues. Data and documents can be routed across worker's queue and through web services across different solutions or applications.

Figure 3.10.1-157 shows a reassignment of an open task from one worker's queue to another.



MTPSM-3-411

Figure 3.10.1-157. The evoBrix Workflow - Task Reassignment Screen. Tasks can be reassigned from one worker queue to another through this screen.

Team CNSI's integrated workflow management solution supports the State desire for improved automation, reduced manual intervention, configurable work routing, and task management. This helps reduce time for the overall completion of a process as well as reducing potential errors caused by human interaction. The evoBrix PMIS Workflow solution comes with table-driven configurable rules, task routing, assignment, and tracking capabilities. This makes processes more efficient, compliant, agile, and visible by ensuring that every process step is explicitly defined, monitored over time, and optimized for maximum productivity. Team CNSI's workflow solution will ensure compliance with state defined processes.

WKF17

The Contractor shall configure, support and maintain a configurable document management and workflow solution that meets the State's requirements.

The evoBrix PMIS seamlessly integrates with IBM FileNet content management solution which is Team CNSI's Document Management System (DMS). FileNet provides advanced document management features and technology frameworks that meet DPHHS requirements. FileNet will be the repository for all system documents and provider support materials, and supports high-speed ingestion of imaged and non-imaged content through a series of tuned processes. The evoBrix PMIS DMS solution will send all documents to State's centralized ECM solution.

Unlike other document management solutions, electronic documents are stored in their native formats. This reduces errors in transformation and supports future accessibility and migration to other platforms. DMS is a configurable, integrated, and secure solution that provides the agility required to adapt to change, while assuring accuracy and timeliness of information. DMS supports all facets of document management, including common and generic features like ingestion, storage, retrieval, filing, and retention. The integrated security features ensure that documents are accessible and distributed only to authorized users.

The FileNet document management system provides a user portal for users to access the document management functions and features such as search, retrieval and viewing of documents.

The users will be able to access the documents in the following two ways:

- By directly accessing the document management system's portal
- Through the evoBrix PMIS Screens

Figure 3.10.1-158 illustrates the usage of Team CNSI's Document Management System.

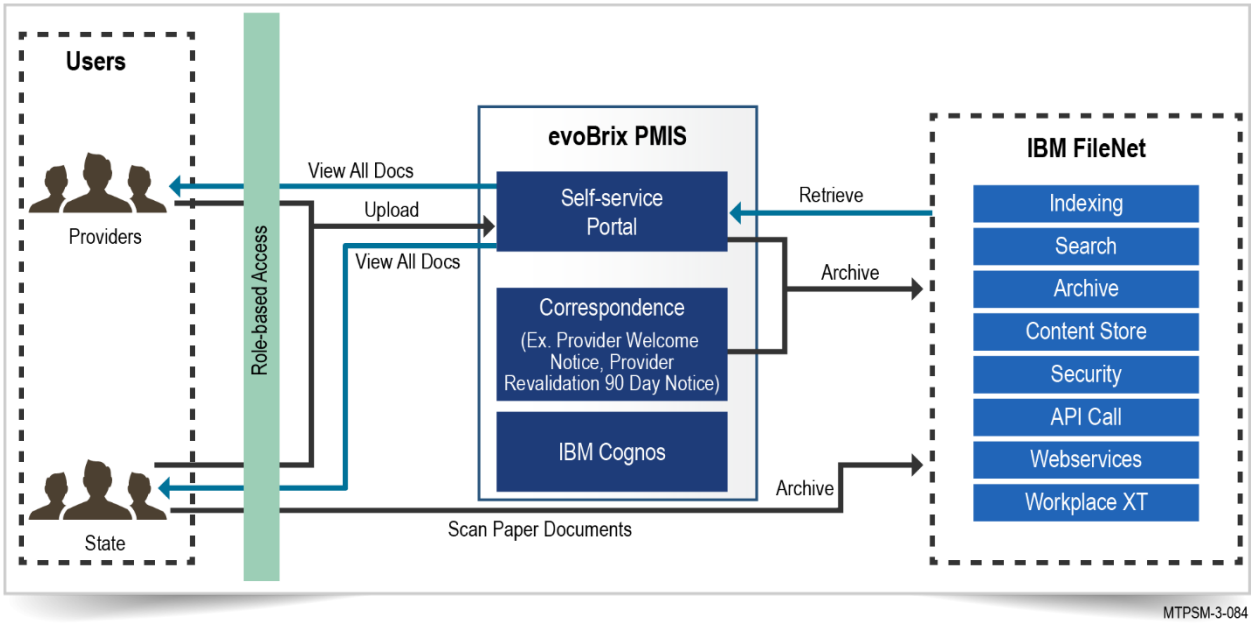


Figure 3.10.1-158. Team CNSI's Document Management System. Documents are archived to IBM FileNet.

Document Handling Work Flow

Documents received for processing by Team CNSI operations team will go through the steps listed below:

- Document Submission – The system allows providers to submit documents using one of the below modes of submission.
    - Mail – Documents that are submitted through mail are sent to the mail room where technicians open the documents, classify and batch the documents, and send them for scanning and document processing.
    - Fax – Documents that are sent through fax are sent to the mail room. The technicians in the mail room take the faxed documents along with the cover sheet, classify and batch the documents, and send them for scanning and document processing.
    - Email – If the provider chooses to email documents, they are required to compose an email with the prescribed metadata elements and attach a scanned copy of the document to a predefined email address. The email is then received by the email servers in the mail room, where the document and metadata information is extracted from the email and are sent for document processing.

- Screen Upload – The provider can also upload any supporting documents through the evoBrix Screens. In this case the provider needs to enter the appropriate metadata in the screens and attach the document.

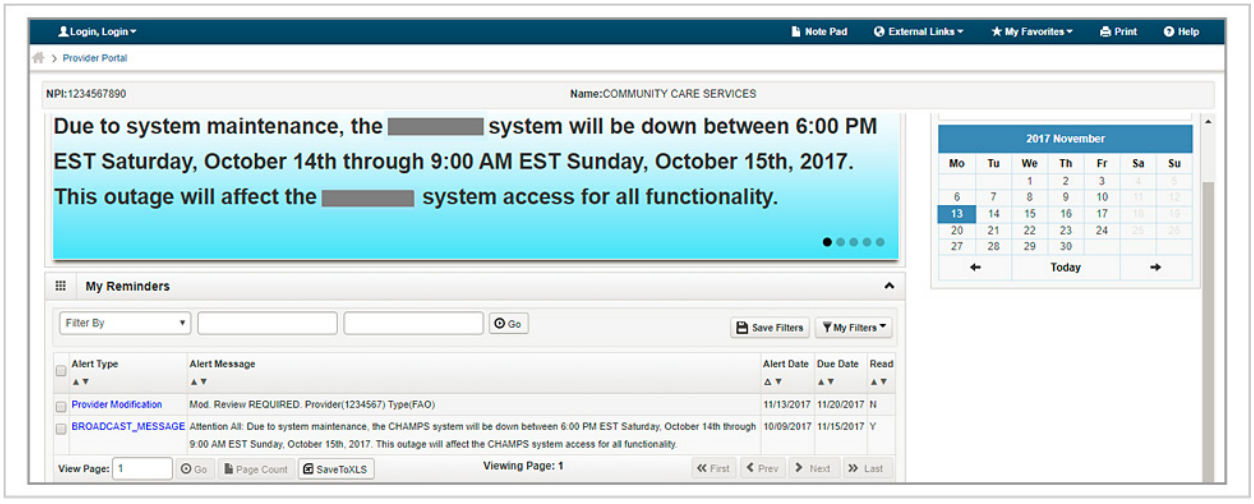
- Error Handling – In case the system encounters any exceptions or errors while processing the document, it is placed in an error queue which is constantly monitored by technicians. These documents then undergo manual review to correct the issue and then reprocessed.
- Transaction Processing – Once the documents successfully go through processing, they are associated with the relevant transaction or record within the system. At this point they are available for review through evoBrix screens and enables DPHHS personnel to process the transaction.

WKF18

The Contractor shall have configurable workflow processes to support auto notifications to providers for specific events (e.g., license expiration, revalidation).

Team CNSI's workflow engine processes are configurable and support sending automated notifications to providers and other State staff (to provide escalation to management and/or supervisors). Providers and State staff receive notification messages in their "My Inbox" section and can navigate directly to the applications that need action. For instance, providers can be notified when their license is about to expire or when their enrollment eligibility needs to be revalidated.

Figure 3.10.1-159 shows the providers' view of their inbox within the evoBrix PMIS portal.



MTPSM-3-412

Figure 3.10.1-159. Inbox View. This screen shows the providers' view of their inbox within the evoBrix PMIS portal.

Providers also receive mail correspondence upon the occurrence of specific events such as license expiration and revalidation.

WKF19

The Contractor shall provide links to screening and monitoring databases in the workflow tool if the data isn't available via an automated interface.

The evoBrix Provider Credentialing Solution (PCS), in partnership with LexisNexis, supports the screening of providers against the Federal Databases like Office of Inspector General (OIG) (for List of Excluded Individuals/Entities (LEIE), Excluded Parties List System (EPLS) from System for Award Management (SAM)) and other State agencies for any exclusions at these sources. Additional data sources can also be linked to the system (e.g., MCSIS, CMS-MED sanction files). PCS also includes monthly batch screening of providers against these databases. This comprehensive screening of providers meets pre-enrollment and post-enrollment screening criteria per the CMS guidelines. When a provider enrollment application or enrollment modification request gets routed for review, the enrollment specialist can also choose to perform an on-demand screening of the provider.

In the event a data source is not available for a screening requirement, the system provides an external link for manual review by the State staff.

WKF20

The Contractor's solution shall have configurable workflow to present for validation, updates submitted online/electronically by specific criteria (e.g., program type, data type, risk level).

Team CNSI's integrated workflow management solution supports the State's goals of improved automation, reduced manual intervention, configurable work routing, and task management. evoBrix PMIS Workflow solution is table-driven with configurable rules, task routing, assignment, and tracking capabilities. The configuration can be driven by specific criteria such as program type, data type, or risk level.

3.10.1.10 Correspondence Management

This section addresses Correspondence Management requirements for the Contractor's solution(s) and operations. The Contractor's correspondence engine shall be configured to generate enterprise correspondence and coordinate the print and distribution through a State approved print and mail service. The Contractor must describe the proposed solution's capacity to configure, support and maintain correspondence management functionality (i.e., add, modify, or remove correspondence) and the type of resource and necessary skill set(s) required for correspondence management functions. Describe the change management processes associated with correspondence management. In addition, the Offeror must describe their approach to meet each of the Correspondence Management requirements detailed in Attachment F, Requirements Matrix.

Team CNSI offers a robust solution to create, manage, and deliver customer communications. Correspondence is a critical part of an organization's day to day activities and business processes. The evoBrix PMIS correspondence module has a highly scalable framework for managing and producing large numbers of personalized communications as well as ad hoc correspondences. It has built-in support for document composition and delivery through multiple channels. Industry standard output formats such as PDF and PostScript are supported, in addition to email.

The evoBrix PMIS correspondence module is highly flexible, can meet the demands of a dynamic organization, and can accommodate changes in an agile manner. It has powerful configuration features that lend themselves for integration with Print and Mail facility's stringent print requirements, including requirements related to margins, address positioning, cover sheets, page counts, and barcodes to help with automated sorting and mailing.

The Team CNSI Advantage

Team CNSI's correspondence solution uses industry proven Pitney Bowes EngageOne Designer and EngageOne Generate for design and generation of outbound letters, both on-demand and in an automated fashion for individual and mass mailing requirements, that are compliant with state and postal guidelines.

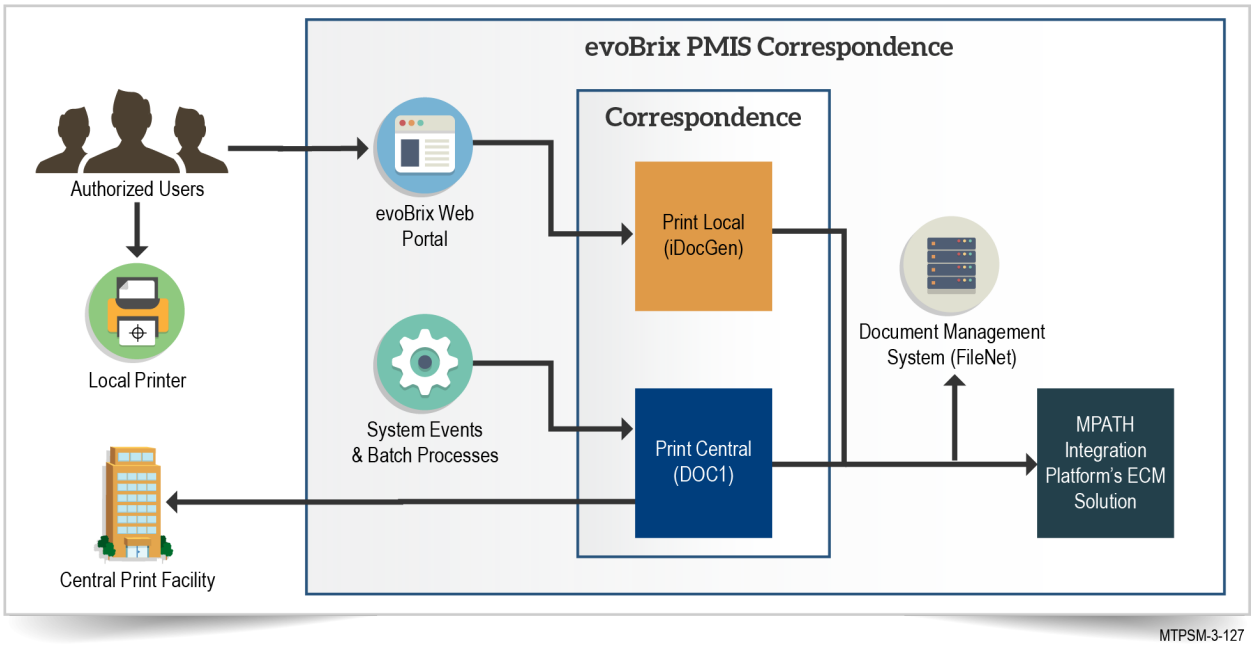
- The solution provides the ability to generate automated letters on the basis of predefined events, such as approval or denial of a provider enrollment application. These event-based letters are generated without any user interaction.
- The solution follows a template-based approach that can be modified per State requirements.
- Letters are standardized in accordance with US Postal Service (USPS) guidelines and addresses are validated against the most current USPS address database.
- The solution supports mass mailing that is required frequently to address specific populations groups.
- System-generated correspondences will be stored in IBM FileNet and can be accessed through evoBrix PMIS portal or printed on demand.

MTPSM-3-102

The evoBrix PMIS uses Pitney Bowes EngageOne High Speed Batch processing bundle (formerly DOC1) correspondence module for design and generation of outbound correspondences. Pitney Bowes EngageOne Designer provides a single flexible environment for all aspects of publication design, from data definition to layout and production, for use by a single user or through collaboration between IT and business users. The designer manages all publication resources and makes it easy to reuse elements across applications. The core document editor is a comprehensive design tool for designing letter templates to accommodate simple to highly complex letter designs.

Pitney Bowes EngageOne Generate provides sophisticated application logic and can create complex conditions using variable input content to generate effective, personalized communications.

Figure 3.10.1-160 illustrates the correspondence process flow, through the evoBrix PMIS system.



MTPSM-3-127

Figure 3.10.1-160. evoBrix PMIS Correspondence Process Flow. Illustrates both the Print Central and Print Local process flows.

All centrally-printed letters comply with state and postal guidelines for using economical postage, which includes standardizing letters in accordance with US Postal Service (USPS) guidelines and validating addresses against the most current USPS address database. evoBrix PMIS letters, provider supporting documents, State policies and procedures manuals, and training materials are stored in evoBrix PMIS DMS solution and can be accessed through the evoBrix PMIS portal or printed on demand. All documents archived in the evoBrix DMS solution are also sent to the MPATH Integration Platform's Enterprise Content Management repository. Figure 3.10.1-161 lists the most commonly used automated letters/notices that support the Provider Business Area.

#	Correspondence Title	Description
1	Provider Welcome Notice	This letter indicates that the provider is approved and welcomes the provider to participate in the Medical Assistance Program.
2	Denial Notice	This letter is generated by the system for each application that is denied for enrollment by the State.
3	License/Certification Term in 45 Days Notice	This letter is generated for all providers whose license/certification expires within the next 45 days.
4	License Termination Notice	This letter indicates the provider license has expired and that provider enrollment is end dated.
5	Provider Revalidation 90 Day Notice	This letter is generated for all providers who have 90 days to revalidate their enrollment.
6	Provider Revalidation 30 Day Notice	This letter is generated for all providers who have not revalidated their enrollment and have 30 more days to complete their revalidation.
7	Provider Revalidation Termination Notice	This letter is generated for all providers who have not revalidated their enrollment within the 90-day time frame and system terminates the enrollment.
8	Provider Revalidation Intermediate Cycle Notice	This letter is generated for all providers who have not revalidated in their intermediate cycle and system terminates the enrollment after the due date.
9	Sanctioned Notice	This letter indicates that the provider has been Sanctioned and is no longer eligible to participate in the Medicaid Program effective from sanction date.
10	Suspended Notice	This letter indicates that the provider has been Suspended and is no longer eligible to participate in the Medicaid Program effective from suspension date.
11	Application ID Notice	This email is generated by the system when the enrolling provider has entered the basic information for the first time successfully.

Figure 3.10.1-161. List of evoBrix PMIS Correspondence Letters. These are used to support the Provider Business Area.

Resource Support

Following are the necessary skillsets that are required to configure, support and maintain correspondence management:

- Experience with Pitney Bowes EngageOne Design tool
  - Comprehensive knowledge of all aspects of EngageOne Design tool to create letter templates including Data Definition, Logic Map, Layout Design, Barcode definition and Publication
  - Maintain repository database for all publication resources
- Experience with Pitney Bowes EngageOne Generate tool
  - Deployment and configuration of EngageOne Generate in Test and Production environments

- Integrate components of EngageOne Generate with evoBrix Correspondence Module

Team CNSI will utilize resources for the above skillsets to effectively manage the setup, configuration, administration, and maintenance of the evoBrix PMIS Correspondence module.

Change Management

Team CNSI will follow the standard Change Management process for Correspondence Management area. Our change management process includes methods for communicating, evaluating, and approving or rejecting changes throughout the project. This process ensures that proposed changes are evaluated for impact to system, schedule, scope, cost, and resources, which facilitates informed decision-making by all parties involved in the change. As a part of our Change Management process, a log of changes is maintained in the project repository and indicates the disposition and status of all change requests. A similar process is instituted to handle changes post-implementation as well. For more details on change management, please refer to Section 3.10.2.1 Project Management.

COR01

The Correspondence Management Solution must be able to generate correspondence (e.g., scheduled and ad hoc correspondence and bulletins) using standard letters or forms, letter templates, and free-form letters.

The evoBrix PMIS Correspondence module has both Print Central and Print Local capabilities; Print Central Letters are sent to a State-approved print and mail service, whereas Print Local Letters are editable by authorized staff members, locally, to be individually mailed out. Documents sent for centralized printing can be configured as scheduled letters or based on system events. Predefined document templates are designed, using standard letter templates or forms, based on business requirements, and can be filled with dynamic content before sending it to the central print facility.

Free form letters, which provide users the flexibility to change specific parts of the letter before printing, can be configured as a template. Users can provide dynamic content through the evoBrix PMIS screens, which are then plugged into the template, and the letter is generated with the dynamic content can be locally viewed and printed by the users. The evoBrix document template design adheres to standards defined by State-approved print and mail service.

Figure 3.10.1-164 depicts the first page of a sample letter, where dynamic content is

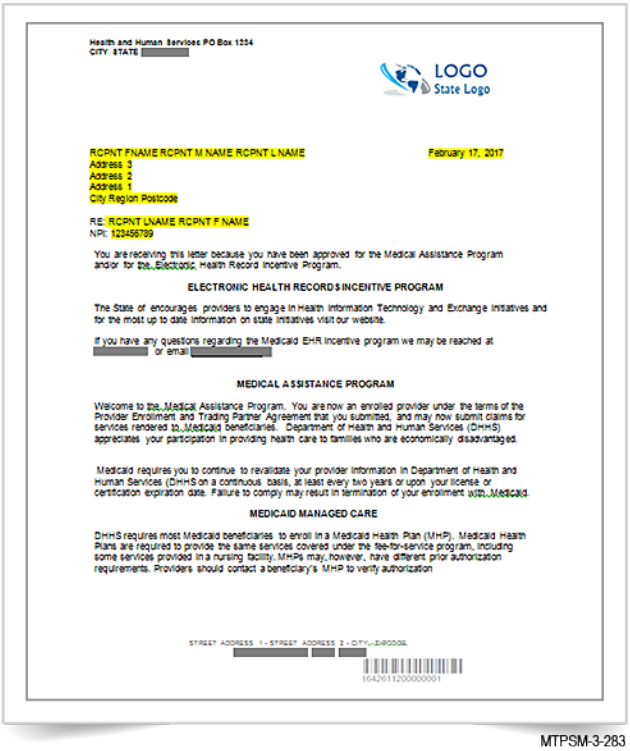


Figure 3.10.1-162. Sample Welcome Letter. Dynamic content is populated during letter generation.

highlighted in yellow. It shows address blocks, logos, and barcodes typical to all evoBrix Correspondence.

COR02

The Contractor shall configure, support and maintain a correspondence engine to generate correspondence and coordinate the print and distribution through a State approved print and mail service.

Team CNSI has extensive experience in setting up and configuring EngageOne, the correspondence engine. The evoBrix PMIS has a robust framework integrating with EngageOne, which is tried and tested to handle high volume letters. Team CNSI can perform optimum setup of the evoBrix PMIS Correspondence module, including the setup and maintenance of Pitney Bowes EngageOne Base for designing letter templates and document generation. Team CNSI will coordinate with State-approved print and mail service on all aspects of this integration including barcode configurations, margins, and coversheets.

COR03

The Contractor's solution shall utilize industry standard barcode technology that is approved by the Department.

The evoBrix PMIS Correspondence module has built-in capability to utilize industry-standard barcode technology while generating letters and supports a wide range of standard barcodes including UCC/EAN128 and interleaved2of5.

The evoBrix PMIS Correspondence module uses interleaved 2of5 for all our evoBrix correspondence which is compatible with Brainware's OMR engine used by the State. The barcode is embedded in all the batch print letters jobs, and can be used for automated sorting, separation, and stuffing of letters into envelopes by central print services. Figure 3.10.1-165 shows a sample barcode, which can be adjusted per State requirements.



Figure 3.10.1-163. Sample Barcode. This barcode includes the standard interleaved 2 of 5 symbol.

In the sample barcode shown above, barcode position 1 to 12 holds the unique ID generated for each letter recipient. Barcode position 13 marks the end of a set, for each letter recipient, and finally, position 14 to 16 specifies the page numbers

COR04

The Contractor shall utilize letter, notification and other templates for correspondence that are approved by the Department.

The evoBrix PMIS Correspondence module utilizes Pitney Bowes EngageOne Designer to create document templates based on State requirements and can be customized to adhere to State and Federal standards. Templates can be configured to include cover sheets, forms, verbiage, dynamic content such as return address, and optional run-time attachments at central printing. Templates can also be designed for use with standard mailing or e-mailing based on State requirements.

All templates will be sent for a formal review and approval the State Department prior to implementation. Any subsequent changes thereof would also be subject to the review and approval process before getting finalized and will follow the standard operations process flow for Change Management.

COR06

The Contractor's solution shall send documents and the necessary indexing metadata to the modular integration platform for storage of documents in the enterprise content management solution (ECM).

By default, the evoBrix PMIS Correspondence module archives all generated correspondences to the evoBrix DMS solution. Document metadata and index parameters are used during this archival process to link the correspondences back to business entities, to meet regulatory requirements, and to allow for easy search and retrieval.

The evoBrix PMIS will send all documentation and indexing metadata to the MPATH Integration Platform as well, for storage in the centralized enterprise content management solution.

COR07

The Contractor's solution shall store all sent or received documents in the ECM.

All outgoing correspondences are archived to the evoBrix DMS solution, as part of the evoBrix PMIS Correspondence module. The evoBrix PMIS will send all documents/letters and indexing metadata to the MPATH Integration Platform as well, for storage in the centralized enterprise content management solution.

COR08

The Contractor's Correspondence Management Solution must be able to integrate variable data to maximize efficiency.

Document templates designed as part of evoBrix PMIS Correspondence are reusable modular components, and letters can be generated based on varying input data and system events. Document templates are coupled with conditional logic to produce effective personalized communications. Complex conditions can be incorporated with ease to provide dynamic content.

COR10

The Contractor shall generate applicable notices to members, providers, and other entities (e.g., enrollment/disenrollment notices, requests for information, and program information).

evoBrix PMIS Correspondence module supports the ability to trigger applicable notices based on specific system events such as provider enrollment/disenrollment. The correspondences are generated based on letter templates configured for that specific system event and user/event-specific data is used to generate dynamic letters. The evoBrix PMIS module has automated processes for identifying providers requiring notifications, and utilizes queue based mechanisms to ensure correspondences are generated and sent out in a timely manner.

COR12

The Contractor's solution shall produce notices to applicants of the approval, rejection, and pending status of their provider enrollment.

The evoBrix PMIS Correspondence module can generate specific letters for provider enrollment events including approval or rejection of enrollment applications. The verbiage and content can be adjusted to suit different scenarios based on State requirements.

COR15

The Contractor's solution shall support official approval and denial notifications to the provider. The notification will support consolidated communication for multiple taxonomies in the case of split approval and denial of provider enrollment service determinations.

The evoBrix PMIS Correspondence module can generate specific letters for provider enrollment events including approval or rejection of enrollment applications. The letter templates used for generating correspondence can be customized based on input data including consolidated communication for multiple taxonomies (split approval and denial) as well as to send carbon-copied correspondences for multiple entities.

COR13

The Contractor's solution shall provide the ability to create materials at between a sixth and eighth grade reading level and for a culturally diverse population.

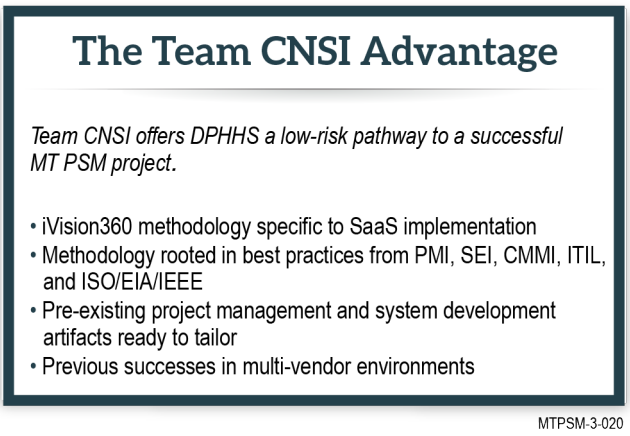
Letter templates generated by the evoBrix PMIS Correspondence module can be fully customized, including headers, footers and verbiage within the letter body. This allows evoBrix Correspondence module to support State-approved materials for all reading levels and for a culturally diverse population using standard forms, templates, and custom verbiage.

3.10.2 Project Management and System Development Requirements

The Contractor will be expected to apply proven project management and system development methodologies to the initial implementation of the proposed solution and to each subsequent enhancement or iteration of the solution.

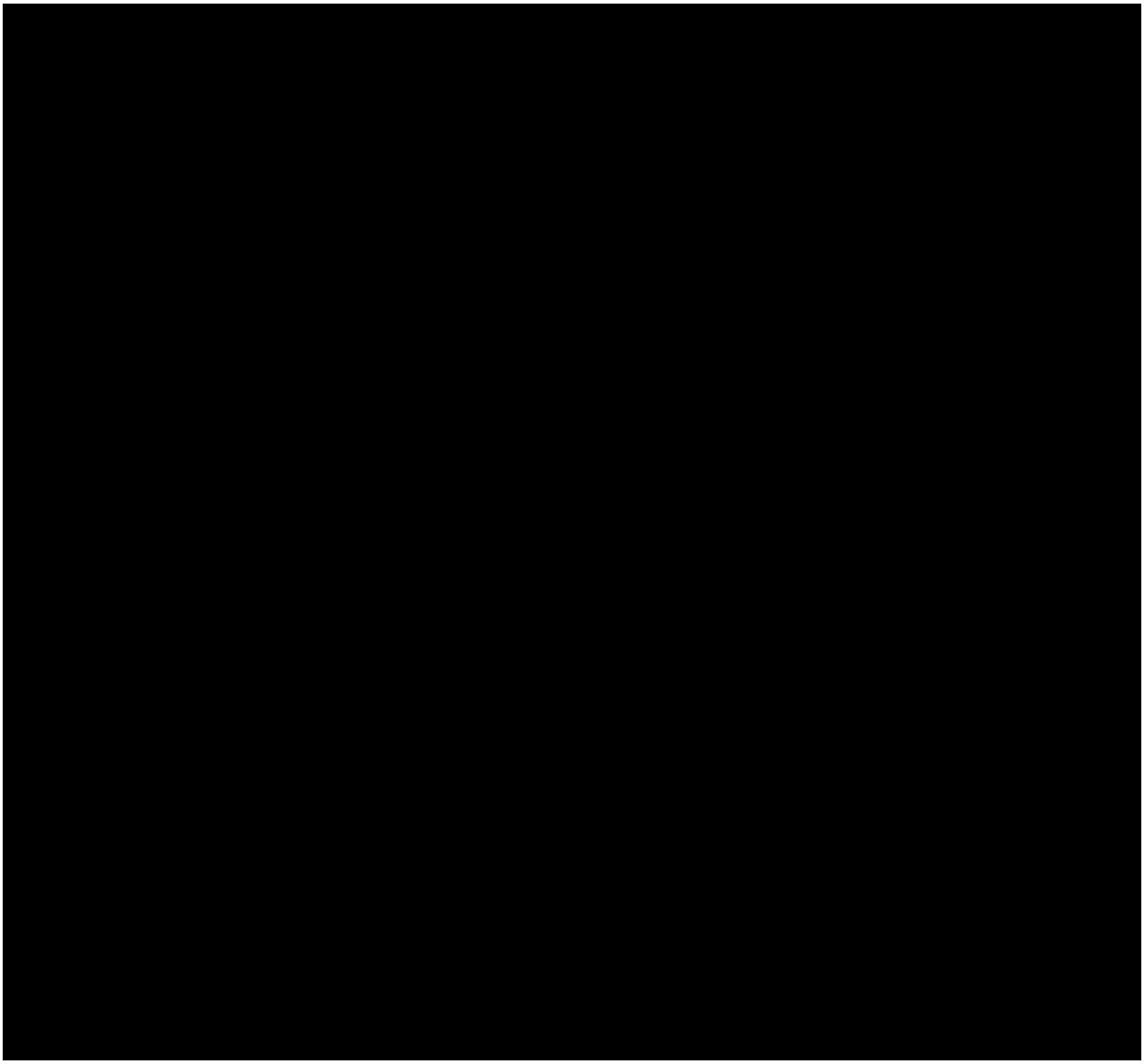
DPHHS does not require a particular project management or system development methodology. The Offeror must propose an approach that will satisfy the scope of work and incorporate all activities required, or their conceptual equivalent. The Contractor will be expected to adjust the project management approach or project schedules, as necessary, to collaborate with the Systems Integration Services Contractor and other contractors in order to incrementally build the MPATH modules and components. In addition, DPHHS will require the coordination of efforts among its staff and all contractors, as no single contractor can perform its required responsibilities without coordination and cooperation with the other contractors. The selected contractors shall maintain communication with other contractors and DPHHS management and staff as necessary to meet its responsibilities that pertain to this RFP's scope of work.

Team CNSI's iVision360 Cloud Framework (iVision360) incorporates Team CNSI's project management and system development methodologies. iVision360 specifically supports modular, Software as a Service (SaaS), evoBrix solution implementations such as the Provider Management Information System (PMIS) module proposed for DPHHS.



iVision360 provides a comprehensive and flexible approach that Team CNSI tailors to meet the specific needs of DPHHS. In contrast to a typical Design, Develop, and Implement (DDI) approach, iVision360 is a Solution, Configure, Implement (SCI) methodology. We will implement our SaaS PMIS module, with minimal customization, using the same methodology we applied to our PMIS implementations in the multi-vendor environments of Michigan, Illinois, and Utah. In all three states, Team CNSI used its experience and communication skills to engage in the collaborative activities necessary to coordinate software implementation as a part of a team composed of multiple vendors. Our iVision360 system development life cycle (SDLC) offers a set of project management (PM), scheduling, SDLC, and quality assurance processes and templates ready to tailor to DPHHS' needs. Our iVision360 methodology has the flexibility necessary to conduct software implementations in complex, multi-vendor situations. Taken together, Team CNSI's experience implementing PMIS in a multi-vendor environment, and our strong SDLC, allow us to offer a low risk pathway to implementation for DPHHS and the other states involved in the NASPO procurement.

Figure 3.10.2-1 shows an overview of the iVision360 PM framework and SCI SDLC.



We based our iVison360 methodology on application of industry best practices, such as the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK), the Software Engineering Institute's (SEI) Capability Maturity Model Integration (CMMI), the Information Technology Infrastructure Library (ITIL), and the International Standards Organization/Electronic Industries Alliance/Institute for Electrical and Electronic Engineers (ISO/EIA/IEEE) system and software development standards. Re-assessed at CMMI for Development 1.3, Level 3, Team CNSI brings practical and proven project management, data conversion system engineering, quality assurance, and verification and validation to the MT PSM engagement. Team CNSI also brings current experience working in a multi-vendor environment, acquired in Michigan, Illinois, and Utah. We have honed our skills in communicating, cooperating, and working across organizational boundaries which will facilitate meeting the states' goals for DPHHS and the other states involved in the NASPO procurement.

Following implementation of the MT PSM solution, Team CNSI continues to use its SCI methodology to manage changes and enhancements. Changes and enhancements begin with the base system functions as

implemented for DPHHS. For projects that affect the national Medicaid program, such as federal legislative changes, Team CSI updates the evoBrix PMIS module and provides the changes to each of the states we service. State-specific compliance and business features are applied only to the individual state's PMIS configuration. Team CNSI has practical experience managing the base evoBrix PMIS module and state-specific configurations for Michigan, Illinois, and Utah, and we are well-positioned to repeat the same configuration management for the MT PSM and the other states participating in the NASPO procurement.

Team CNSI's Operations Team manages the routine, periodic release of software updates. The Operations Team uses ITIL service processes to ensure the ongoing stability of the software environment.

From the beginning of the project, through final turnover to a successor contractor, Team CNSI's focus remains on satisfying the State's vision for PMIS, and continuing to foster a collaborative, open approach with all involved contractors.

In Sections 3.10.2.1 through 3.10.2.8 that follow, we provide additional details on how Team CNSI will use our SCI methodology to satisfy the State's requirements through our approaches to:

- Project Management Practices
- Systems Development Methodology
- Requirements Management
- Design, Configuration, and Build
- Data Conversion and Data Cleansing Methodology
- Testing Methodology
- Training
- Implementation and Acceptance Management
- Project Closure and Turnover

3.10.2.1 Project Management

The Contractor shall submit a formal Project Management Plan and project schedule, along with other project planning documents. The Contractor must adhere to the Project Management Institute (PMI) or similar industry-standard project management standards and approach throughout the Contract term. The offer must describe their approach to meet each of the Project Management requirements defined in Attachment F, Requirements Matrix.

The Team CNSI Advantage

Team CNSI leverages the Project Management Plan and Project Schedule from its previously successful SaaS implementations.

- Incorporates best practices from PMI, CMMI, ISO/EIA/IEEE, and ITIL
- Encompasses best practices honed through practical experience gained through PMIS SaaS implementations
- Fully aligns with DPHHS requirements

MTPSM-3-064

Team CNSI brings the same proven iVision360 project management methodology and system development framework that we used in our live production PMIS implementations to the NASPO procurement and the MT PSM project. Under the iVision360 methodology, Team CNSI's Michigan-Illinois alliance project was the first SaaS PMIS implementation in the nation. Team CNSI starts with our production evoBrix PMIS, and tailors it to meet the requirements defined in Attachment F, Requirements Matrix. iVision360 is based on industry best practices for project management and SaaS system deployment. SaaS projects inherently carry lower risk because the solution can be seen, touched, and explored from the beginning of the project.

Our iVision360 processes are assessed at Level 3 under CMMI for Development V1.3. Team CNSI will tailor iVision360 processes and templates to align with the specific needs of DPHHS. Team CNSI will bring reliable and effective project management, staffing, and deliverable support that meet DPHHS' specific needs for a successful MT PSM implementation, transition, operations, and turnover. Team CNSI will collaborate with DPHHS early in the planning stage of the project to produce:

- The tailored Project Management Plan (PMP), which defines the project governance structure and the processes for managing scope, schedule, staff, deliverables, configuration, data, communications, action items, risks, issues, change, and integration
- The tailored Project Work Plan, which defines the work breakdown structure (WBS) and the schedule, detailing the stages, phases, activities, and tasks supporting successful implementation, operation, and turnover of the MT PSM

Comprehensive Project Management Plan

Team CNSI's project management approach has the central theme of collaborative and transparent delivery. Engaging DPHHS and MT PSM stakeholder involvement is key to our approach in every phase of the project, and we strive to involve stakeholders in a meaningful manner.

Team CNSI starts with project planning and preparation activities immediately after the announcement of intent to award. One of the first activities is to produce the comprehensive PMP and obtain DPHHS approval of the plan. In reviewing section 3.10.7 of DPHHS' proposal, Team CNSI sees that DPHHS is listing each PMP component as a separate deliverable. Team CNSI's approach is to produce a master PMP containing content for each component within that PMP. This greatly reduces the number of deliverables that DPHHS will need to review and approve. DPHHS would otherwise need to conduct near simultaneous review and approval of the following and their associated Deliverable Expectation Documents (DEDs):

- PMT18 Project Management Plan
- DOC15 Communications Plan
- DOC38 Risk Management Plan
- DOC40 Issue Management Plan
- DOC18 Change Management Plan
- DOC24 Staffing Plan

DPHHS will receive a single master PMP for review and approval that will contain all the documentation in the preceding list. Team CNSI's comprehensive PMP details, mapped to DPHHS' document number, are outlined in Figure 3.10.2-2.

Project PMO Process Area	Section 3.10.7 Documentation ID/ Requirement No.	Main Activities
Governance Structure	PMT18	In collaboration with DPHHS, the Project Management Office (PMO) documents the governance structure for the project, describing Team CNSI's governance structure and how it will interface with the DPHHS project governance structure during the project. This section describes roles and responsibilities, and the escalation pathway for any project management concerns that cannot be addressed by the joint DPHHS/Team CNSI governance structure.
Scope Management	PMT18	Describes how the project's scope will be managed and the documents that the project will use to baseline scope.
Schedule Management	PMT18	Describes how the project schedule will be managed and the documents and plans that the project will use to baseline the schedule.

Project PMO Process Area	Section 3.10.7 Documentation ID/ Requirement No.	Main Activities
Staff Management	DOC24	Team CNSI develops and maintains a staff management plan defining specific roles and responsibilities, and identifying and assigning resources to provide quality products and services. This section includes a comprehensive a comprehensive "RASIC" matrix that lists major responsibilities and deliverables and defines: ■ Role responsible (R) ■ Role having approval authority (A) ■ Role or roles supporting (S) ■ Role or roles to be informed (I) ■ Role or roles to be consulted (C) This section also includes the project's training plan, a project roster listing Team CNSI staff members, DPHHS stakeholders, other project participants, such as the Integration subcontractor and the Independent Verification and Validation (IV&V) subcontractor. The roster includes identification of key team members and their backups.
Work Product Management	PMT18	Team CNSI documents the work flow and review steps for formal and informal documentation. This section provides transparency into Team CNSI's documentation development process as well as expectation for State review and comment cycles.
Project-specific Configuration and Data Management	PMT18	Team CNSI documents the repositories that are used to manage the project along with the project role responsible for administering access to the repository.
Communications Management	DOC15	Our approach for communication management includes defining: ■ Each routine type of communication the project is expected to produce, its key messages, vehicles (such as presentations and reporting), audience, timing and frequency of the communication, and responsibility for preparation and approval (where applicable) ■ Each regular meeting or event planned for the project, the participants, the moderator, the topics covered, and the location and frequency of the meeting
Action Item Management	PMT18	Our action item management process provides a place to log pending actions and decisions. The action Item process is available to all project staff and provides a convenient way to capture and track the many smaller items that do not fall into the category risks or issues. Action items can be escalated to risks or issues if they remain open too long.
Change Management	DOC18	Our change management process includes methods for communicating, evaluating, and approving or rejecting changes throughout the project. This process ensures that proposed changes are evaluated for impact to system, schedule, scope, cost, and resources. This facilitates informed decision-making by all parties involved in the change. As a part of our Change Management process, a log of changes is maintained in the project repository and indicates the disposition and status of all change requests.
Risk Management	DOC38	The risk management process systematically assesses the risks faced throughout the project. Each risk is identified, logged in the risk register, evaluated, and monitored until it no longer presents a risk to the project. factors of the project and identify specific risks. We manage risk by accepting, transferring, preparing contingence plans, or mitigating exposure.
Issue Management	DOC40	The issue management process systematically assesses issues the project is facing. Each issue is logged in the issue register, evaluated, validated, and assigned to an issue owner who is responsible for developing and managing to an issue resolution plan. Issues are monitored and managed until they are fully resolved.

Figure 3.10.2-2. Overview of Team CNSI's PMP. Team CNSI's PMP is based on PMI guidelines and is aligned to DPHHS' requirements.

The Quality Management Plan (DOC16) is delivered separately as it is prepared by Team CNSI's quality lead rather than our Project Management Office (PMO) team. This plan describes the quality processes

we use to assess performance against our CMMI-based processes, and to verify that the deliverables and documents provided to the State meet acceptable quality standards for content and construction

Team CNSI also develops a Measurement Management Plan tailored for the specific service level agreements (SLAs) and project measures required to support both Team CNSI's PMO reporting process and the Status Reports we prepare for the State. The Measurement Management Plan is an internal document that will not be submitted to the State for review and approval. The Measurement Management Plan defines the specific activities and Team CNSI roles responsible for collecting metrics required for the project. This includes schedule metrics, deliverable metrics, SLAs, earned value of work completed, planned value of work completed and the variance. On request, we will make it available for the State's perusal.

Controlling the Implementation and Ensuring Ongoing Success

Team CNSI's implementation strategy is systematic and comprehensive to ensure that both the system and stakeholders are ready to successfully execute the implementation during the transition phase and to begin production operations. Following implementation, our approach is supplemented by ITIL processes designed to support production operations. Team CNSI minimizes the dependencies and risks associated with deployment of the MT PSM.

Team CNSI understands the complexity of implementing a modular system such as PMIS because we have already implemented the evoBrix PMIS solution in Michigan, Illinois, and Utah. We accomplished these PMIS implementations in partnership with state stakeholders and multiple contractors. We also understand the necessity of a comprehensive strategy to ensure successful integration within a multi-vendor solution.

The Team CNSI PMO is the first step in establishing a culture of partnership on the project. Our governance processes are centered on the PMO and close collaboration with the State. The PMO is our management control center for each phase of the contract engagement and ensures that all contract, configuration, quality, and business process operations are performing to the service levels stipulated in the contract. Our Project PMO is composed of the Project Manager, the Contract Manager, the Business Operations Manager, the Certification Lead, the Integration Lead, and the Testing Lead. The Team CNSI PMO is responsible for maintaining Team CNSI's methodology and related processes. Each member of the Team CNSI PMO is also responsible for partnering with their DPHHS counterparts to establish a strong collaborative network.

Team CNSI's PMO performs the following activities:

- Provide project management leadership
- Maintain project management plans and processes
- Implement project management tools
- Establish and maintain project communications
- Establish performance monitoring framework and monitor progress
- Provide oversight of all Team CNSI's project responsibilities
- Build the necessary planning documents for project execution, operations, and turnover
- Engage in collaborative risk, issue, and change management activities with State and other subcontractors involved in the project

PMT01

The Contractor shall provide licenses as required by the Agency to allow users access to perform all necessary business functions.

Team CNSI will acquire all licenses necessary to perform required in scope business functions during the implementation of the PMIS and during the subsequent operational and turnover phases of the project. We provide a comprehensive list of licenses needed in Attachment L. Team CNSI will ensure that the licenses are acquired, and configured if necessary, before they are needed for use in implementing or operating the evoBrix PMIS.

PMT02

The Contractor shall support the Department in all program governance activities as necessary.

Team CNSI agrees to support the DPHHS in all program governance activities as necessary throughout the life cycle of the MT PSM project. Team CNSI's project management approach ensures that the necessary program governance structure and governance activities are identified through collaborative discussions. The project governance organization structure, along with relevant roles and responsibilities, will be documented in the Project Governance section of our PMP. Figure 3.10.2-3 shows part of a sample of the "Responsible, Approval Authority, Support, Inform, and Consult" (RASIC) matrix Team CNSI will tailor for the MT PSM.

	Team CNSI Project Roles												State Stakeholders							
Titles	Project Manager	Integration Manager	Business Operations Manager	Test Lead	Certification Lead	Provider Functioanl Lead	CRM Functional Lead	Implementation Lead	Data Conversion Lead	Technical Writer	QA Engineer	QA Auditor	Program Director	Program Manager	Project Manager	Provider Lead Business Analyst	CRM Lead Business Analyst	Itermfaces Lead	Data Conversion Lead Analyst	IVV Lead
Formal Project Deliverables																				
PMT18 - Project Management Plan	R	C	C	C	C				C	S	S	I	I	A	A					I
PMT19 - Project Work Plan	R	C	C	C	C	C	C	C	C	S	S	I	I	A	A	I	I	I	I	I
DOC03 - Conversion Plan	A								R	S	S	I	I	A	A	I	I		A	I
DOC04 - Configuration Management and Iteration Plans, Release Schedule	A	R	C	C				C		S	S	I	I	A	A					I
DOC46 - Detailed System Design Documents	A	C	I	I		R	R		I	S	S	I	I	A	A	A	A	A	I	I

RASIC Description:

Responsible. (Designated person who takes the initiative and responsibility to make the work happen)	R
Approve. (Must sign-off on the work before it is effective)	A
Support. (Is or must be committed because they provide resources and/or play a role in implementation)	S
Inform. (Must be notified of the results of the work but need not be consulted)	I
Consult. (Have information and/or capability necessary to complete the work and hence must be consulted)	C

MTPSM-3-271

Figure 3.10.2-3. Sample RASIC Matrix. The MT PSM RASIC Matrix will be populated with all project deliverables and the project team members from all organizations participating in the MT PSM module implementation. All State role and responsibility information is for sample purposes only.

Additional information regarding responsibilities will be documented in the Staff Management approach component of the PMP. This includes a RASIC Matrix covering all formal deliverables and major

activities performed during the project. The PMP is presented to DPHHS for review and approval during the planning phase of the project.

PMT03

The Contractor shall be responsible for the capture and dissemination to the Department of agendas, meeting minutes and documentation necessary for successful execution of the project.

Team CNSI agrees to prepare, capture, and disseminate agendas, meeting minutes, and documentation necessary for successful execution of the MT PSM engagement. Team CNSI agrees to follow the format and style guidelines documented in DPHHS' MPATH Documentation Standards as provided in the State's Proposal Reference documentation. Team CNSI is aware of requirements stated in SLA03 and agrees to distribute agendas at least 24 hours in advance of the meeting, and produce related meeting minutes within two business days for each meeting Team CNSI facilitates for the MT PSM project.

PMT04

The Contractor shall participate in necessary meetings with the stakeholders and/or other Contractors.

Team CNSI agrees to participate in necessary meetings with DPHHS project stakeholders and other Contractors to support the work required for the successful implementation and operation of the MT PSM. We will work collaboratively with DPHHS' MT PSM project management team to establish or identify the standard meetings required for the project. This includes the weekly and monthly status meetings mentioned in the requirements in this section of Team CNSI's response to DPHHS' RFP. Team CNSI will document any regular repeating meetings as elements of the Communication Management section of our PMP, which will be submitted to DPHHS for review and approval.

PMT05

The Contractor shall provide deliverables or documentation as defined in the Project Work Plan (PWP) and approved by the Department.

Team CNSI agrees to provide the deliverables and documentation defined in the PWP and approved by the State. Team CNSI documents our deliverable and documentation management processes as elements of the Deliverable Management section of our PMP. The PMP will be submitted to DPHHS for review and approval. Team CNSI's deliverable management process features multiple content and format reviews to ensure high quality documentation deliverables are produced for the State. Refer to our response Section 3.10.7, Project Deliverables and Documentation, for a more thorough discussion of our deliverable management processes.

PMT08

The Contractor shall support the State and its Contractor(s) in Independent Verification and Validation (IV&V) activities associated with the contract including CMS Certification(s).

Team CNSI agrees to support the State and its Contractor(s) with the Independent Verification and Validation (IV&V) activities associated with the MT PSM engagement as described in the Medicaid

Enterprise Toolkit (MECT) and Medicaid Enterprise Life Cycle (MECL). Team CNSI has extensive experience working productively with multiple vendors on its projects. We understand that IV&V will require our help to satisfy status reporting to CMS. Team CNSI is prepared to support the State and its IV&V Contractor to ensure the documentation specified in MECT Appendix B or noted in a CEMT checklist item is included in the scope of work for this procurement. Team CNSI understands the importance of the IV&V Contractor's role in supporting DPHHS' goal to achieve CMS certification. Team CNSI plans to have a productive partnership with DPHHS' IV&V Contractor beginning with the development of the Certification Plan that will occur during the Planning phase of the project.

Team CNSI fosters strong interpersonal relationships through its collaborative approach to requirements validation, gap identification and validation, and solution definition. We welcome and encourage the participation of the IV&V contractor from the early stages of the project through implementation. Team CNSI will include the State's IV&V Contractor in collaborative meetings and status reviews.

PMT09

The Contractor shall conduct a monthly status meeting to discuss project tasks and activities (e.g., deliverables, milestones, issues, risks, and SLAs).

Team CNSI agrees to conduct a monthly status meeting to discuss project tasks and activities. The monthly status meeting is driven from the content provided in the monthly status report discussed in PMT17. This includes:

- Progress review of the schedule including recently completed and upcoming milestones and deliverables
- Identification and discussion of issues and risks
- Review and discussion of performance against SLAs
- Other information as required by DPHHS

The meetings will appear as a scheduled event in the Communications Management section of the Team CNSI's PMP and in the Project Work Plan under Project Monitoring and Control.

Refer to the response to requirement PMT17 for full details of the monthly status report.

PMT10

The Contractor shall conduct weekly meetings to discuss issues, risks, progress of current projects, solution changes, resource changes, and other areas specific to the scope of work.

Team CNSI agrees to conduct weekly meetings to discuss emerging issues and risks, project progress, change management, resource concerns, and other areas specific to the MT PSM engagement. The meetings will include designated DPHHS team members, Team CNSI PMO team members, and other Team CNSI subject matter experts as needed.

The meetings will appear as a scheduled event in the Communications Management section of the Team CNSI's PMP and in the Project Work Plan under Project Monitoring and Control.

The meeting will provide a place for weekly collaboration on:

- Schedule status (recent completions, in-progress tasks, and upcoming deliverables and milestones)
- Newly identified potential risks, issues, changes, and escalated action items
- Any other agenda items brought up by the attendees that require project management level collaboration

PMT11

The Contractor must employ a project management approach that will satisfy the scope of work and incorporate all activities described in the RFP. The Contractor shall adjust the project management approach or project schedules, as necessary, to collaborate with the module vendors in order to incrementally build the enterprise platform.

Team CNSI's project management approach is built on our prior project successes implementing the evoBrix PMIS solution for Michigan, Illinois, and Utah. In all three of these projects, Team CNSI worked collaboratively with multiple vendors and state stakeholders implementing our SaaS PMIS solution. In all three cases, the projects were accomplished as planned.

Our PMP documents the full scope of project management activities necessary to manage all phases the of the Project. We will work in collaboration with DPHHS and its other Contractors to ensure that commitments with interdependencies are coordinated to meet DPHHS' needs in building its enterprise platform.

Please refer to our response to Requirement PMT18 additional details about our project management approach.

PMT12

The Contractor shall conduct a project initiation kick-off meeting with key stakeholders and the State's project team.

Team CNSI agrees to conduct a project initiation kick-off meeting. Our standard project management approach is collaborative. The kick-off meeting allows the project team to get off to a good start with a common basis of understanding. Team CNSI's approach is customer-centric. We place a high priority on understanding the State's culture. During contract negotiations, we will work with the State to begin the process of understanding of the State's culture. We collaborate with the State to identify both content and approach to delivery for the project initiation kick-off meeting. This initial collaboration allows us to work with the State to identify the messaging needed, in the right terms, to start the project off in the State's environment.

The resulting kick-off presentation has a dual purpose. It is used as the communication tool that brings together all stakeholders at the start of the project. The kickoff material is also used to orient new team members who join the project after the initial kickoff.

PMT13

The Contractor shall implement procedures and tools for tracking project action items, decisions, issues, risks and defects.

Team CNSI's consolidated PMP contains the procedures for managing action items, decision, issues, risks, and defects throughout the project. These procedures were assessed as compliant with CMMI for Development, V1.3 Level 3, in April 2017.

At the beginning of the project, Team CNSI establishes a Microsoft SharePoint Project Documentation Repository to provide a central, organized, collection point for project communication and information exchange. Some of the procedures and tools we use include:

- Team CNSI's procedure for tracking action items allows new action items to be logged by any member of the team with authorization to log into the SharePoint site. Action items include any item that can be completed without escalation to the project's joint Team CNSI and DPHHS governance structure. Some examples of action items include recording a request for some documentation mentioned at a meeting, a reminder to provide the values to populate a list, a decision that needs to be made at the team level, or passing information discovered by one team to another team also affected.
- Team CNSI's risk procedure includes routine evaluation of identified and emerging risks to ensure that appropriate risk management strategies are developed. Risks are possibilities that might impact the project. Under our procedures, a risk owner is assigned to develop a strategy to address the risk. This may include contingency planning, mitigation planning, risk-transfer planning, or agreement to accept the risk. Risks logged in the repository include a description of the triggering conditions. Once a risk is opened, it is tracked until it is no longer relevant to the project, or the risk has been triggered. Because Team CNSI captures risks early, and discusses them regularly at weekly and monthly status meetings, we are prepared to invoke the appropriate risk response if the risk becomes a reality. When this occurs, the risk is transferred to an active issue item where it is managed through closure. Examples of risks include a possible government action that would result in new requirements imposed on the project before it is implemented or a potential airline strike that would prevent required travel to Helena.
- Our procedure covers routine evaluation of identified and emerging issues. Issues are situations that are impeding the progress of the project. Like action items and risks, issues are documented in the Project Documentation Repository and assigned an issue owner. The issue owner reviews the issue and assembles the resources necessary to overcome the issue. The issue owner coordinates with the team to identify possible approaches to resolving the issue. If the issue is complex enough, the issue owner may conduct a formal Decision Analysis and Response session to select the best solution. All documentation related to the issue is captured in the Project Documentation Repository. If the solution has the potential to affect project scope or timeline, the issue and solution are escalated to senior Team CNSI and DPHHS staff to complete any necessary change request authorizations to support the selected solution. Examples of issues include delay in making a critical decision about the solution for a gap, or delay, beyond the agreed-upon review period, in approving a deliverable necessary to start the next phase of the project.
- Our procedure for change management provides a structured method for requesting changes to baselined scope, schedule, or cost. The change request is documented in the Project Documentation Repository and undergoes evaluation by the affected stakeholders. For changes to the evoBrix PMIS module, Team CNSI performs the necessary investigation and analysis to determine the impact to the project and alternative and recommended solutions to address the change. For any type of change, DPHHS evaluates the proposed change and decides to either move forward with the change by approving it, defer the change to a later stage of the project, such as a post-deployment enhancement by placing it on hold, or to forego the change by cancelling it. The analysis and decision details are recorded in the Project Documentation Repository. Examples of changes include a request to place the project on hold for six months due to impending DPHHS reorganization, or requesting a new feature be added to the MT PSM after design has been approved.

- Team CNSI's process for decision management is called Decision Analysis and Resolution (DAR). Pending decisions are logged in the SharePoint Project Documentation Repository and a decision owner is assigned. The decision owner is responsible for identifying the team members needed to reach the decision The DAR process includes identification of alternative solutions and objective evaluation criteria. A formal DAR meeting is held where the team verifies the evaluation criteria and assigns a weight to each factor. The team then systematically evaluates each alternative against the weighted evaluation criteria. This process identifies the best decision in an objective way. The results of the DAR are presented to project decision-makers in the form of a recommendation. The project decision-makers can either approve the recommendation or ask the team to repeat the process using different criteria. The process continues until a final decision has been rendered. The results of each step of the DAR process are documented in SharePoint.

Team CNSI uses Atlassian's Jira for defect tracking. Jira is a full featured software development tool that includes an excellent defect tracking function. Additional information on Jira can be found in the Section 3.10.2.6, Testing, under the heading Defect Tracking.

PMT14

The Contractor shall provide an electronic document repository for project documents and deliverables. The Contractor, Department staff and other contractors with the appropriate security level must have the ability to upload/attach new or revised versions of documents. The repository must perform version control and allow users to view all prior versions.

Team CNSI will provide a SharePoint Project Documentation Repository that provides security by role and organization. The SharePoint Documentation Repository has the capability of supporting multiple security profiles aligned to the user's roles and responsibilities. SharePoint provides the ability to upload, download, and attach new or revised versions of documents. SharePoint has native mode version control tracking and allows users with appropriate security access, to view all prior versions.

Project Documentation Repository

Through our many years of performing projects in the state and federal government sector, we found that having a highly accessible project documentation repository makes the tasks of managing and controlling the project easier for Team CNSI and its customers. In keeping with our principles of transparency and collaboration in multi-vendor projects, it is easier when there is a central location all stakeholders can use to deposit and share project information. Team CNSI's SharePoint Project Documentation Repository is the communications and sharing hub for the project. Figure 3.10.2-4 shows the major functions of the SharePoint Project Documentation Repository.

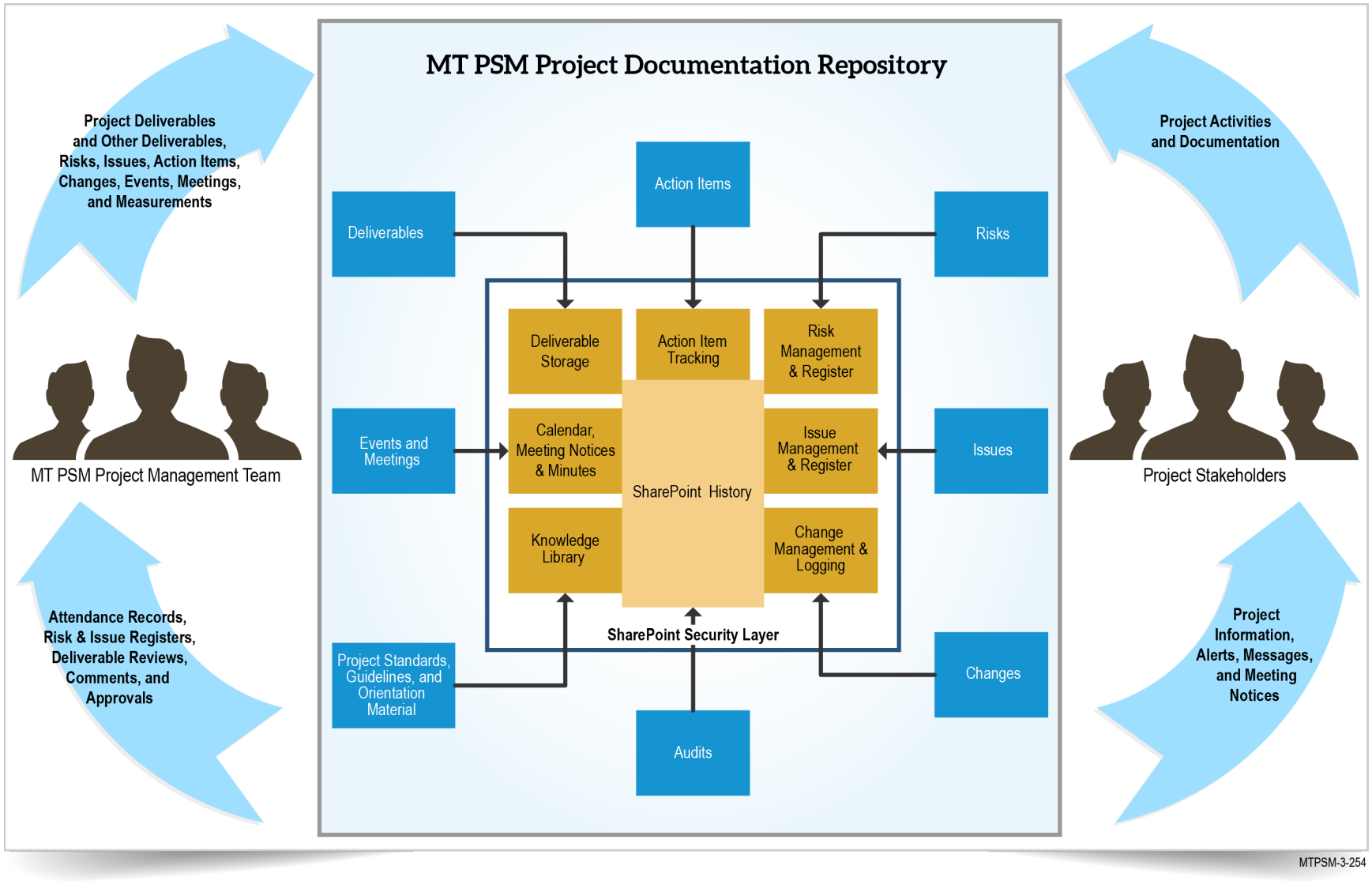


Figure 3.10.2-4, Team CNSI's SharePoint Project Documentation Repository. Available 24x7 to authorized users, the SharePoint Project Documentation Repository is used to manage most project deliverables and monitoring and control tasks.

Our SharePoint Project Documentation Repository delivers superior project data management, accessibility, and security. The repository is web-enabled and configured expressly for effective project management. It will be available 24x7 to authorized users. It supports the ability to capture and manage key project information including:

- Deliverables and other project documents
- Action items
- Risk management
- Issue management
- Change request management
- Events and calendar information
- Publications and knowledge library items
- Contact information

Deliverables and other project documents are stored with full history and version control. Users "check out" a document (or other item) while making updates, which ensures that no other user can change the item until it is checked back in. The Project Documentation Repository provides the ability to view previous versions of a document. Authorized users can revert the current document back to a previous version when needed.

Access is defined by user, type, and level. For example, a specific user may be granted read-only access to risks and issues but may have read and update access to change requests. The access types include deliverables and other project documents, action items, risks, issues, change requests, events, and contacts. The access levels within each type are read (R), read and update (RU), create read and update (CRU), and create read update and delete (CRUD).

Specific user access can also be defined for each individual document. For example, a specific user may be able to access the PMP, but may not be granted access to the Data Conversion Plan. Further, a user with access to a document may be granted the ability to only view the document, but not download it, while another user may be granted the access to view and download the document.

The Project Documentation Repository supports the ability to define teams of users, such as DPHHS and IV&V. Access controls can be applied to groups or to selected individuals within a group. Figure 3.10.2-5 shows a preliminary mock-up of the SharePoint site for the MT PSM project.

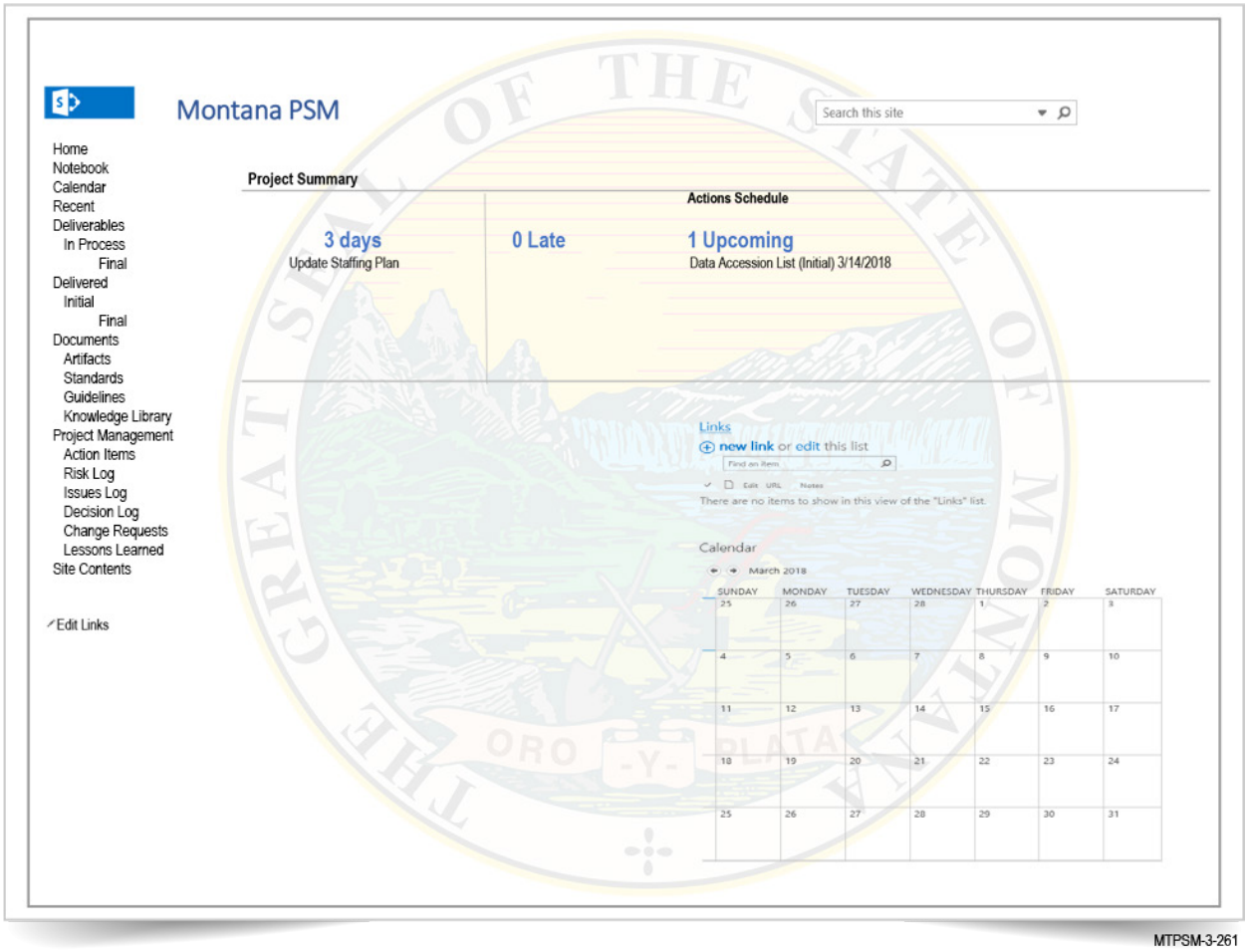


Figure 3.10.2-5. Mock-up of MT PSM SharePoint Repository. The MT PSM SharePoint repository is the communication hub for the project. It provides access to documentation, facilitates meeting scheduling, risks, issues, action items, change management, and decision management.

Team CNSI will collaborate with DPHHS to identify the organizations, roles, responsibilities, and individuals who will require access to the SharePoint Project Documentation Repository. Access will be reviewed and updated as staff changes are processed.

PMT15

The Contractor shall establish and utilize a deliverable review and acceptance process agreed upon by the Department that incorporates the following:

a. Review cycles, which will be conducted and scaled to the size and complexity of the deliverables.

b. Deliverables will need to reflect coordination with the overall modular program and will follow agreed upon change control processes.

c. Informal reviews and walkthroughs of draft and final deliverables are encouraged.

d. Queuing up excessive deliverables for simultaneous review is unacceptable to the Department.

Team CNSI's deliverable review and acceptance process, recently assessed at CMMI for Development V1.3 Level 3, will be used for the MT PSM project. The deliverable review and acceptance process will be provided in the Documentation Management section of our PMP.

- Team CNSI has a robust internal review process including peer reviews, technical writing reviews, and independent quality reviews.
- Team CNSI plans for two review cycles for each formal deliverable. The review periods are based on the size and complexity of the deliverable and are detailed in our PWP and schedule. This aligns with DPHHS' SLA Requirement SLA02.
- Team CNSI's deliverable preparation process incorporates all affected stakeholders including other contractors providing the multi-vendor coordination necessary to support State's modular program. We include all affected stakeholders in the collaboration process needed to develop deliverables.
- After approval by DPHHS, deliverables are baselined. Project change management procedures are applied to all changes to baselined deliverables.
- Team CNSI routinely shares drafts and in-process documentation through collaborative sessions for requirements/solution analysis, design/solution modeling, test planning, and implementation planning. We believe that early participation in the construction of a deliverable leads to greater stakeholder comprehension, and higher quality results from deliverable reviews. Collaborative sessions are detailed in our PWP and schedule.
- Team CNSI has made a concerted effort to recommend a plan where there is no excessive buildup of deliverables for any one stakeholder area. In the Planning phase of the MT PSM project we will revisit the proposed plans and incorporate any adjustments that are needed to ensure DPHHS stakeholders are not asked to review multiple deliverables at the same time.

PMT16

The Contractor shall provide deliverables that at a minimum meet the following quality standards:

a. Provide accurate and comprehensive content, reflecting the specific requirements for the deliverable.

b. Ensure appropriate technical level for the audience.

c. Utilize correct grammar, spelling, and versioning.

d. Ensure diagrams are clear, concise, and value added.

e. Follow industry-related standards.

f. Appropriately define and reference information.

Team CNSI uses multiple complimentary approaches to ensure the deliverables for the MT PSM engagement meet our stringent quality standards.

- Team CNSI maintains a standardized Style Guide to ensure that all deliverables are based on a common foundation. The style guide defines standards for style as well as usage. We use the Chicago Manual of Style (The University of Chicago, 2010) as the foundation for our Style Guide.
- Our iVision360 methodology provides a set of predefined deliverable templates including those necessary for gap analysis, requirements traceability, solution modeling, test planning, and implementation planning. The templates reflect lessons learned on previous implementation efforts including the SaaS PMIS implementation in Illinois. Where aligned with expected deliverables, these templates serve as the deliverable expectation documents (DEDs) as they outline all expected content in the deliverable. The templates are available for DPHHS review prior to beginning work on the deliverables.

- We perform formal peer reviews as well as informal document reviews to confirm that the business content presented in our documents is accurate, comprehensive, and reflects the specific requirements for the deliverable.
- The peer review/informal review process, along with a culture of collaboration, work together to ensure the deliverable contains an appropriate technical level of content for the intended audience.
- We employ professional technical writers and quality engineers who work with the teams to tailor or create documentation in accordance with our methodology. The technical writers and quality engineers work with the document authors to ensure that the document:
  - Uses correct grammar, spelling, and usage
  - Meets all Team CNSI document standards, including versioning
  - Includes diagrams and illustrations that are clear, concise, and add value to the deliverable
  - Adheres to relevant industry standards
  - Provides comprehensive reference information for any outside references

PMT17

The Contractor shall submit a monthly status report. The monthly status report must contain, at a minimum:

a. A complete set of updated and current output from the Project Work Plan along with a copy of the corresponding Project schedule files in electronic version.

b. A description of the overall completion status of the Project including schedule variations that report the earned value of the work completed, the planned value of the work completed, and the variance.

c. Planned tasks and activities for the next month.

d. The Deliverable status, with percentage of completion and time ahead or behind schedule for particular tasks.

e. Identification of any staffing issues or changes in the Resource Allocation Matrix.

f. An updated status on all issues being monitored.

g. An updated status on all risks being monitored.

h. Provide metrics necessary to support the State CIO's Legislative Finance Committee (LFC) reporting requirements.

i. Provide testing status and metrics.

j. Provide System enhancement hourly pool total hours used and total hours remaining.

k. An updated status on all SLA being monitored.

Team CNSI will prepare a monthly status report compliant with DPHHS' requirements. The Team CNSI PMO is responsible for collecting and validating the information provided in the monthly status report. The monthly status report will drive the agenda of the Monthly Status meeting described in our response to requirement PMT09 and will include:

- Electronic versions of the updated PWP and schedule. The PWP will be delivered as a Microsoft Word file. The schedule will be delivered as a Microsoft Project file.
- Overall project completion status including earned value of the work completed, planned value of the work completed, and the variance.
- Planned tasks and activities for the upcoming month.

- Deliverable status with percentage of completion and time ahead or behind for key milestones and critical path tasks.
- The issue log, with updated status on all issues being monitored.
- The risk register, with updated status on all risks being monitored.
- The metrics necessary to support the State CIO's Legislative Finance Committee reporting requirements.
- Beginning with the Solution Validation – System Test Phase, testing status and test metrics by test.
- A high-level review of the System Enhancement hourly pool including hours used and total hours remaining.
- Team CNSI provides continuous monitoring of many SLAs through the HealthBeat feature, which is available 24X7. For SLAs that do not appear in HealthBeat, such as performance on Agenda and Meeting Notes (SLA02), Team CNSI will develop a dashboard to collect and report these items. The Team CNSI MT PSM PMO will be responsible for establishing the measurement dashboard and ensuring timely collection of data for inclusion in the monthly status report. As a part of the monthly status report, Team CNSI will provide an analysis of any SLA exceptions occurring during the reporting month.

PMT18

The Contractor shall develop and maintain a Project Management Plan (PMP): The purpose of the Project Management Plan is to provide a comprehensive baseline of what needs to be achieved by the project, how it is to be achieved, who will be involved, how it will be reported and measured and how information will be communicated with the project. It will serve as a reference for decision and clarifications. All relevant project plans including but not limited to the Communication Plan, Change Management Plan, Staffing Management Plan, Quality Management Plan, Risk Management Plan, Issue Management Plan and the Work Breakdown Structure are incorporated into the Project Management Plan. It is a living document that evolves as the project progresses and is updated with the latest relevant information as required. The Project Management Plan may be broken into separate documents, but all documents will be considered sections of the Project Management Plan.

Team CNSI uses a comprehensive PMP that addresses the elements required by DPHHS. The WBS referenced in this requirement is provided as a component of the Project Work Plan deliverable as integrated into the project schedule.

Figure 3.10.2-6 shows a sample table of contents from our comprehensive PMP deliverable.

Table of Contents

Preface
- Purpose
- Scope
- Audience
- Referenced Documents

Section 1 – Project Overview
- 1.1 Introduction
- 1.2 Project Management Plan Summary
- 1.3 Project Timeline
- 1.4 Assumptions and Constraints
- 1.5 Project Documentation Repository
- 1.6 Project Management Plan Review Cycle

Section 2 – Project Governance
- 2.1 Overview of Project Governance Structure
- 2.2 Montana Provider Solution Roles and Responsibilities
  - 2.2.1 Team CNSI Governance Structure
  - 2.2.2 Montana DPHHS Project Governance Structure

Section 3 – Scope Management

Section 4 – Schedule Management

Section 5 – Staff Management
- 5.1 Staff Management Approach Summary
- 5.2 Management of Staff Changes

Section 6 – Work Product Management
- 6.1 Pre-Delivery Reviews
- 6.2 Work Product Baseline Management
- 6.3 Work Product Approval Management
- 6.4 Montana Provider Solution Deliverables

Section 7 – Project-Specific Configuration and Data Management

Section 8 – Communications Management
- 8.1 Communications Management Approach
- 8.2 Communications Roles and Responsibilities
- 8.3 Communications Matrices
  - 8.3.1 Regularly Scheduled Events
  - 8.3.2 Regularly Scheduled Reporting

Section 9 – Action Item Management
- 9.1 Action Item Management Approach
  - 9.1.1 Action Item Monitoring
  - 9.1.2 Action Item Escalation and Transfer
- 9.2 Action Item Management Roles and Responsibilities

Section 10 – Risk Management
- 10.1 Risk Management Approach
  - 10.1.1 Risk Monitoring
  - 10.1.2 Risk Escalation and Transfer
- 10.2 Risk Management Roles and Responsibilities

Section 11 – Issues Management
- 11.1 Issue Resolution Approach
  - 11.1.1 Issue Monitoring
  - 11.1.2 Issue Escalation and Transfer
- 11.2 Issue Resolution Roles and Responsibilities

Section 12 – Change Management
- 12.1 Change Management Approach
- 12.2 Change Management Roles and Responsibilities

Appendix A – Project Documentation Repository
- A.1 Access Responsibilities
- A.2 How to Request Access
- A.3 How to Report Problems

Appendix B – Supplementary Information on Action Item Management
- B.1 SharePoint Action Item Portal Required Information
- B.2 Action Item Process Overview

Appendix C – Supplementary Information on Risk Management
- C.1 SharePoint Risk Portal Required Information
- C.2 Risk Process Overview

Appendix D – Supplementary Information on Issue Management
- D.1 SharePoint Discrepancy (Issues) Portal Required Information
- D.2 Issue Process Overview

Appendix E – Supplementary Information on Change Management
- E.1 SharePoint Change Log Portal Required Information
- E.2 Change Log Process Overview

Appendix F – Staff Management Approach Subsidiary Plan

Appendix G – Measurement Management Approach Subsidiary Plan

Appendix H -- Montana Provider Solution Quality Management Subsidiary Plan

Appendix J – Integration Management

Glossary

Acronyms

MTPSM-3-120

Figure 3.10.2-6. Team CNSI Sample PMP Table of Contents. This illustration shows how Team CNSI's standard PMP might be tailored for the MT PSM engagement.

Information from the introduction to this section is repeated here for the benefit of the evaluators. Team CNSI's core PMP includes the sections shown in Figure 3.10.2-7.

Project PMO Process Area	Section 3.10.7 Documentation ID/ Requirement No.	Main Activities
Governance Structure	PMT18	In collaboration with DPHHS, the Project PMO documents the governance structure for the project describing Team CNSI's governance structure, and how it will interface with the

Project PMO Process Area	Section 3.10.7 Documentation ID/ Requirement No.	Main Activities
		DPHHS project governance structure during the project. This section describes roles and responsibilities, and the escalation pathway for any project management concerns that cannot be addressed by the joint DPHHS/Team CNSI governance structure.
Scope Management	PMT18	Describes how project's scope will be managed and the documents that the project will use to baseline scope.
Schedule Management	PMT18	Describes how the project schedule will be managed and the documents and plans that the project will use to baseline the schedule.
Staff Management	DOC24	Team CNSI develops and maintains a staff management plan defining specific roles and responsibilities, and identifying and assigning resources to provide quality products and services. This section includes a comprehensive a comprehensive "RASIC" matrix that lists major responsibilities and deliverables and defines: ■ Role responsible (R) ■ Role having approval authority (A) ■ Role or roles supporting (S) ■ Role or roles to be informed (I) ■ Role or roles to be consulted (C) This section also includes the project's training plan, a project roster listing Team CNSI staff members, DPHHS stakeholders, other project participants, such as the Integration subcontractor and the IV&V subcontractor. The roster includes identification of key team members and their backups.
Work Product Management	PMT18	Team CNSI documents the work flow and review steps for formal and informal documentation. This section provides transparency into Team CNSI's documentation development process as well as expectation for State review and comment cycles.
Project-specific Configuration and Data Management	PMT18	Team CNSI documents the repositories that are used to manage the project along with the project role responsible for administering access to the repository.
Communications Management	DOC15	Our approach for communication management includes defining: ■ Each routine type of communication the project is expected to produce, its key messages, vehicles (such as presentations and reporting), audience, timing and frequency of the communication, and responsibility for preparation and approval (where applicable). ■ Each regular meeting or event planned for the project, the participants, the moderator, the topics covered, and the location and frequency of the meeting,
Action Item Management	PMT18	Our action item management process provides a place to log pending actions and decisions. The action Item process is available to all project staff and provides a convenient way to capture and track the many smaller items that do not fall into the category risks or issues. Action items can be escalated to risks or issues if they remain open too long.
Change Management	DOC18	Our change management process includes methods for communicating, evaluating, and approving or rejecting changes throughout the project. This process ensures that proposed changes are evaluated for impact to system, schedule, scope, cost, and resources. This facilitates informed decision-making by all parties involved in the change. As a part of our Change Management process, a log of changes is maintained in the project repository and indicates the disposition and status of all change requests.
Risk Management	DOC38	The risk management process systematically assesses the risks faced throughout the project. Each risk is identified, logged in the risk register, evaluated, and monitored until it no longer presents a risk to the project. factors of the project and identify specific risks. We manage risk by accepting, transferring, preparing contingence plans, or mitigating exposure.

Project PMO Process Area	Section 3.10.7 Documentation ID/ Requirement No.	Main Activities
Issue Management	DOC40	The issue management process systematically assesses issues the project is facing. Each issue is logged in the issue register, evaluated, validated, and assigned to an issue owner who is responsible for developing and managing to an issue resolution plan. Issues are monitored and managed until they are fully resolved.

Figure 3.10.2-7. Team CNSI's Standard PMP Content. Team CNSI will customize the PMP to meet DPHHS' specific needs.

In addition to the PMP, Team CNSI also prepares a Quality Management Plan (DOC16). The Quality Management Plan is delivered separately as it is prepared by Team CNSI's quality lead rather than our PMO team. This plan describes the quality processes we use to assess performance against our CMMI-based processes, and to verify that the deliverables and documents provided to the State meet acceptable quality standards for content and construction

Team CNSI develops a Measurement Management Plan tailored for the specific SLAs and project measures required to support both Team CNSI's PMO reporting process and the Status Reports we prepare for the State. The Measurement Management Plan is an internal document that will not be submitted to the State for review and approval. The Measurement Management Plan defines the specific activities and Team CNSI roles responsible for collecting metrics required for the project. This includes schedule metrics, deliverable metrics, SLAs, earned value of work completed, planned value of work completed and the variance. On request, we will make it available for the State's perusal.

PMT19

The Contractor shall develop and maintain a detailed Project Work Plan (PWP) and a Gantt Chart that is aligned with the scope of the work outlined in this RFP. The PWP must identify realistic person hours of effort for each task and identify planned completion dates for all deliverables and milestones. Additionally the PWP must include the elements necessary for the IMS include: start and end dates of major phases, key project milestones, integration points, cross module dependencies, and sufficient information to support the State CIO's Legislative Finance Committee (LFC) reporting requirements. The PWP must be continually refined and updated as the project progresses and will retain the baseline for comparative reporting.

Team CNSI will tailor its standard PWP format to meet the specific needs of DPHHS. Team CNSI's standard PWP contains a high-level Gantt Chart showing major phase and activity start- and end-dates which will be aligned to the scope of work outlined in this RFP. Our standard PWP contains the detailed WBS and schedule.

To develop the PWP and schedule, Team CNSI performs a top-down evaluation of the phases, activities, and tasks necessary to support the scope of work defined in the RFP. We use the results of this analysis to define our initial WBS. We then do a bottom-up evaluation of the WBS to ensure that all necessary work has been identified. With the WBS defined, Team CNSI then performs an analysis of the effort and resources needed to complete each component of the WBS. Following industry standard methods, we then identify the schedule dependencies to produce the high-level schedule. We assign labor categories, hours by labor category, and costs to the schedule. Most of this work is done in advance of contract negotiations to ensure that Team CNSI has sufficient lead time to transition staff members from projects that are ramping down or to hire qualified staff. Individuals assigned to the labor categories are monitored

through the Staff Management Plan component of the Project Management Plan. We use a resource utilization matrix to ensure no team members are overloaded.

The schedule is provided in both PDF and Microsoft Project formats and includes:

- Phase, activity, and task start- and end-dates
- Task duration
- Resource labor categories, number of staff, person-hours by labor category, schedule dates, and blended rate, for calculation of earned value
- Key project milestones and milestones representing key integration points and cross-module dependencies with collaborating contractors work
- Deliverables, expected DPHHS review cycles, and expected deliverable approval dates
- Milestone identification for major linkage points between Team CNSI's schedule and other contractor's schedules

During the Planning Phase, Team CNSI will collaborate with DPHHS to ensure that all necessary information is present in the schedule to ensure that the information needed to support the State CIO's Legislative Finance Committee is available.

Team CNSI continually refines the schedule. Our standard practice is to review and update the project schedule every week as a part of regular status reporting. This promotes early notification of tasks that are not performing as expected. We adjust the schedule for approved change requests and to reflect task and activity completion. We have sufficient flexibility in the schedule to respond to changes with minimum impact on other elements of the schedule.

PMT21

The Contractor shall coordinate with the Department and with the module vendors as required by the Department, to support the program-level change management process consistent with the Enterprise Change Management Plan.

Team CNSI understands that the Enterprise Change Management Plan is to be developed by DPHHS' Integration Contractor. Per the RFP Question and Answer Documents, the plan is pending development at the time this response is being prepared. During the planning phase of the project, Team CNSI agrees to coordinate and collaborate with the State, the State's Integration Contractor, and with the module vendors as required to support the program-level change management process consistent with the Enterprise Change Management Plan.

Team CNSI has extensive experience working in multi-vendor projects where coordination is required at an enterprise level. The project environments for our successful PMIS implementations in Michigan, Illinois, Utah, and Washington all involved multiple vendors and major project and program shifts during the projects. Working in collaboration with the State and its contractors, we worked together to align on the best course of action to keep the project's forward momentum going. For example, when approaching a key coordination milestone, one of the partnering contractor's vendor experienced a problem delaying their readiness to participate in a joint activity. We worked together to identify a plan where most of the work could begin on schedule by creating stubs for inputs and saving the outputs for later processing. Using this strategy, we completed all testing activity with minimal delays. We understand the importance of achieving success for the entire organization and will support the State in performing these activities.

PMT25

The Contractor shall be required to work collaboratively with the Department and the System Integrator to provide schedule information to be included in the Integrated Master Schedule (IMS). Elements necessary for the IMS include; start and end dates of major phases, key project milestones, integration points, cross module dependencies, and sufficient information to support the State CIO's Legislative Finance Committee (LFC) reporting requirements.

Team CNSI will tailor its standard schedule to meet the needs of DPHHS. Due to our experience in multi-vendor environments, we know that it is necessary to coordinate activities and synchronize schedules to successfully implement the solution. Having an independent System Integration Vendor is an advantage for this project. With or without the benefit of an independent System Integrator, Team CNSI works with other vendors to identify touch points, requirements for inter-contractor solution configuration and testing. We will work collaboratively with the DPHHS and its System Integrator to provide information to be included in the Integrated Master Schedule. We will ensure that our schedule provides the necessary linkage to the other Contractors where interdependencies exist including:

- Phase, activity, and task start- and end-dates
- Key project milestones, and milestones representing key integration points and cross-module dependencies with collaborating contractors work
- Deliverables, expected DPHHS review cycles, and expected deliverable approval dates

During the Planning Phase, Team CNSI will collaborate with DPHHS and the System Integrator to validate that all necessary information is present to support the State CIO's Legislative Finance Committee reporting requirements.

PMT27

The Contractor shall coordinate module deliverable and milestone walkthroughs and participate in other module walkthroughs as required by the Department.

Module demonstrations and walkthroughs are the foundation of Team CNSI's SCI methodology. Team CNSI begins the Solution Analysis phase with demonstrations of the PMIS module. We continue with solution-specific walkthroughs throughout Solution Modeling activities.

There are multiple reasons we use module walkthrough and demonstrations:

- To demonstrate where Team CNSI's PMIS module meets DPHHS requirements
- To discuss and validate requirement gaps that may exist in the PMIS module
- To helps the DPHHS visualize how the solution will be configured to address their specific needs
- To facilitate DPHHS' understanding of how Team CNSI presents material we've discussed in collaborative sessions
- To ensure that reviewer questions are raised early and answered before formal reviews begin

For Certification, Team CNSI understands the critical importance of the formal MECL milestone reviews. These reviews are an essential component of the CMS process.

As the project reaches critical milestones, Team CNSI will perform milestone walkthroughs to review progress against the plan for that phase including:

- Schedule
- Budget
- Deliverables
- Open Risks
- Open Issues
- Open Decision
- Open Change Management Requests

We agree to participate in DPHHS-required module walkthroughs of other modules as necessary for the implementation of the MT PSM.

PMT29

The Contractor shall submit a monthly System Enhancement Pool report that details tickets invoiced to the hourly pool and must include hours used and hours remaining for the Department's approval.

Team CNSI will submit a monthly System Enhancement Pool report detailing tickets invoiced to the hourly pool, hours used, and hours remaining. This is a component of the monthly Status Report. It will be submitted as a report requiring the Department's approval each month.

PMT31

The Contractor shall cooperate with the State's PMO and the IV&V contractor to give an accurate, honest reporting of the project status.

Team CNSI is committed to honest and transparent project reporting. We agree to provide accurate and honest reporting of the project's status to the State's PMO and the Department's IV&V contractor.

PMT32

The Contractor shall contribute to the State's and/or the Systems Integration Services collaboration site, technical and non-technical project artifacts for the Contractor's module or module components including requirements, use cases, user stories, storyboards, system design documents, supplemental specifications, test cases, test scripts, test results, user, system and training documentation at the State's direction.

Team CNSI agrees to contribute to the State's or System Integration Services collaboration site for technical and non-technical project artifacts for our PMIS module and module components including baselined requirements, use cases, test cases, test scripts, test results, user and system training documentation as directed by the State excluding proprietary software packages integrated with the PMIS module.

Team CNSI will work with the State and the System Integrator to develop a process the apply approved changes to baselined deliverables already loaded to the State's or System Integration Services collaboration site.

3.10.2.2 System Development Methodology

The Contractor will be expected to follow an industry-standard systems development methodology for the initial implementation of the proposed solution and throughout the Contract term. The Offeror must propose a System Development Methodology approach that achieves the expected outcomes of the SDLC-based activities stated below.

Team CNSI employs iVision360, an SDLC that aligns to industry standards. Our SDLC was recently assessed as compliant with CMMI for Development, V1.3, Level 3. Team CNSI developed the Solution, Configure, Implement (SCI) methodology to meet the specific unique requirements of a SaaS solution.

The Team CNSI Advantage

Team CNSI's SDLC, iVision360, is designed to support implementation of modular SaaS solutions.

- Solution, Configure, Implement (SCI) begins with a working system that meets most of DPHHS' requirements
- Used for successful implementations in Michigan and Illinois
- Tailoring, rather than "from scratch" creation streamlines pre-deployment project work
- Assessed at Level 3, CMMI for Development V1.3, April 2017

MTPSM-3-125

Team CNSI's SCI Methodology

Team CNSI will use its SCI methodology to achieve DPHHS' implementation objectives. Team CNSI's iVision360 is focused on successful project delivery from initial planning through production deployment and operations and is specifically designed to support modular SaaS implementations. It contains elements of a standard waterfall methodology as well as some elements of agile methodologies. The greatest difference between our SCI SDLC and the traditional Design, Development, and Implementation (DDI) approach is that we begin with a full featured, working PMIS module. Activities such as requirements validation are handled through demonstrations rather than lengthy discussion. Seeing how the PMIS module operates, from the beginning of the project, eliminates many of the uncertainties of ensuring that a text-based requirement is fully understood by the contractor.

Team CNSI's SCI methodology will be utilized to achieve DPHHS Implementation objectives. Figure 3.10.2-8 provides a mapping of the SCI stages to standard DDI phases:



[redacted]

©2017 CNSI | 3.10-283



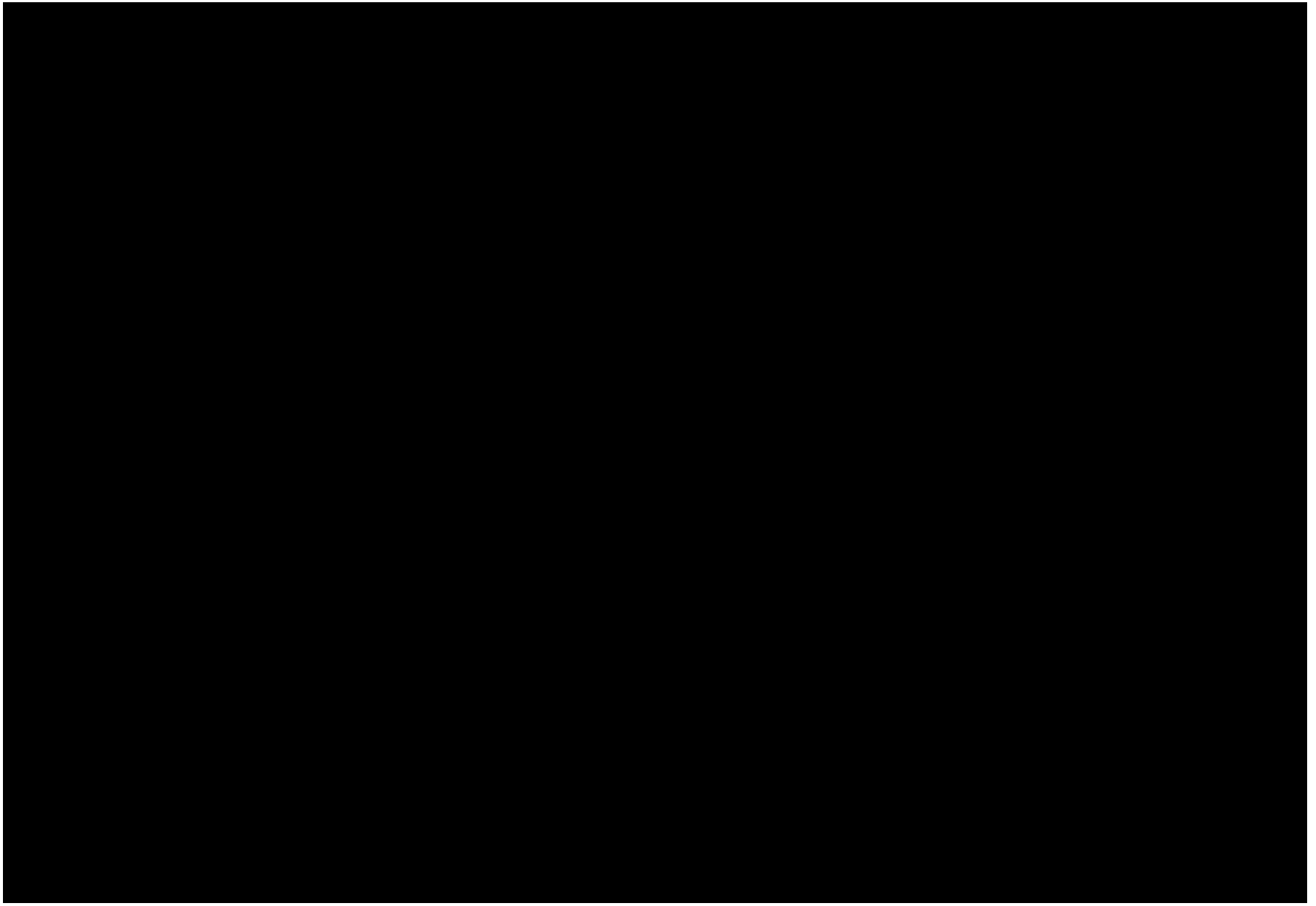
The SCI methodology has the following exit criteria:

- Acceptance of all Implementation phase deliverables
- Correction of all defects identified in testing per the Test Plan
- Retirement of existing DPHHS systems following successful implementation of complementary functionality within Team CNSI's scope
- Transition of all MT PSM functions to operations, and retiring all existing related business operations contracts and processes
- MT PSM is certified by CMS

Team CNSI acknowledges and accepts its responsibility to assist and support DPHHS in its efforts and activities for achieving system certification at the earliest reasonable opportunity. Therefore, upon contract award, Team CNSI will commence the required activities to ensure that the critical success factors pertaining to services and technology are met and our MT PSM solution is certifiable after six continuous months of operations. Our primary activities in this regard will include:

- Preparing and supporting the MECT Operational Milestones Reviews
- Preparing and providing CMS Readiness Checklist inputs
- Creating and providing documentation for the Certification Review package
- Participating in, and supporting all, CMS review activities
- Creating Corrective Action Plans, when required

There are four stages in the SCI iVision360 methodology, as previously shown in Figure 3.10.2-9. Figure 3.10.2-10 shows these phases in additional detail. Inputs, processes, activities, required reviews and outputs, and the supporting reference materials are described in detail following Figure 3.10.2-10.



©2017 CNSI

Stage 1 - Planning

The Planning phase involves creation of a set of integrated plans to guide project team members through the activities of the life cycle. The major inputs to this phase include the Team CNSI's Project Management Planning process and related document templates for the Project Management Plan (PMP) and Project Work Plan (PWP), DPHHS' RFP, previous project plans Team CNSI used for PMIS module implementations, inputs from the State's System Integration Contractor, and other Contractors participating in the MT PSM project.

The top-level plan for the MT PSM project is the **PMP**, which defines the following:

- PMP Overview
- Project Governance
- Scope Management
- Schedule Management
- Staff Management
- Work Product (Deliverables) Management
- MT PSM Configuration, Data Management and Security
- Communications Management
- Action Item Management
- Risk Management
- Issues Management
- Change Management
- Decision Management

The finalized **PWP** is a key output of the Planning phase. The PWP contains a description of the project schedule planning process, the high-level timeline for the project, and the detailed WBS and project schedule. In collaboration with DPHHS, Team CNSI tailors its standard PMIS project schedule to the specific needs of DPHHS. This includes specific milestones, deliverables, and project management artifacts that DPHHS requires. The schedule includes any interdependencies identified between Team CNSI and other Contractors participating in the MT PSM project. The schedule contained in the PWP is baselined on approval from DPHHS and is updated weekly as a part of standard project management and control processes.

For the MT PSM project, Team CNSI will also prepare the **Certification Plan** to support DPHHS' certification of the MT PSM under CMS MECT using the most recent guidance available through the MECL.

Planning activity results in a series of activities designed to monitor and control the project. This includes:

- Regular status reporting
- Regular status meetings
- Risk monitoring
- Issue resolution management
- Change management oversight
- Schedule management activities including completion tracking, milestone tracking, and schedule updates
- Regular communications activities
- Escalation of any risk, issue, or change that cannot be resolved by the MT PSM team
- Regular updates to the PMP and its subsidiary plans
- Other activities required by DPHHS' project management team

- Routine quality audits of project management processes, requirements management, and deliverables

These activities are conducted throughout the life of the MT PSM project. SCI project management practices are based on PMI and CMMI best practices. After transition to operations, processes based on ITIL and ISO 9001 are added to manage ongoing system and business operations.

[redacted]

Stage 4 - Implementation

The Implementation Phase includes the major activities leading up to, and following system deployment. This includes:

- User Acceptance Test
- Deployment
- System Certification

User Acceptance Test

Key inputs to the UAT phase include the DSDDs, the Test Plan, the configured code as of Solution Validation completion, and a comprehensive set of UAT test cases. Most the test cases are reused from our SaaS base solution. UAT is completed by Team CNSI business operations personnel, DPHHS project team members, providers, and other contractors where required. Team CNSI leverages its experience and lessons learned from previous UAT activities as the foundation for our UAT approach. Team CNSI places the highest priority on intra- and inter-team communication, establishing shared goals, and providing transparent access to defect tracking. UAT participants document deficiencies in meeting DPHHS' requirements, in the defect tracking system. The defects are prioritized, managed, fixed, and deployed by Team CNSI while UAT participants re-test the corrected defects.

In parallel with UAT, Team CNSI conducts performance testing, parallel testing, disaster recovery testing, and implementation planning activities. The UAT phase overlaps with deployment activities to allow for provider business-to-business testing.

Data conversion, exception management, and data cleansing activities continue during this phase as the data is made ready for the production environment.

Deployment

The initial Implementation Plan is the key input to this phase. The implementation planning process produces a complete list of activities that must be completed to ensure successful deployment of the system and related business operations activities. The activity list spans technical and business readiness from provisioning the production environment though ensuring providers and business operation staff have successfully completed training. The activity list is a collaborative product of Team CNSI, DPHHS, and other organizations involved in the deployment. Collaboration activities include planning sessions and operations readiness reviews. Team CNSI will leverage the knowledge gained through our previous PMIS deployments. Our extensive practical knowledge of the activities required to successfully deploy the system and initiate system and business operations to ensure a smooth, low-risk implementation and production cutover using our implementation checklist and our implementation calendar, which are artifacts included in the Implementation Plan. Figure 3.10.2-11 provides an excerpt sample from a prior PMIS implementation. Figure 3.10.2-12 provides a sample calendar page from a prior PMIS implementation. The implementation checklist and calendar include more detail than is carried in the schedule.

Provider Enrollment Project Implementation Checklist

Task ID	Task	Oranization: Actor	Planned Start Date	Planned End Date	Actual Completion Date	Approver	Approval Date	Status Description
LEGEND								
	Green - Task is completed							
	Red - Task is delayed							
	White - Task is open							
Infrastructure Setup and Readiness for Go-Live								
1	Verify the readiness of [redacted]/State PE production hardware and infrastructure, including Application servers, DB Servers, networking and firewall rules	Team CNSI: GS, DK, AM Host: BG, AMM	1/26/2015	5/28/2015		CNSI: JH Host: BG, AMM		
2	Verify License and Maintenance agreements for software used in deployment	Team CNSI: GS Host: BG	3/2/2015	3/6/2015	3/6/2015	CNSI: JH Host: BG	3/6/2018	Completed
3	Verify appropriate storage (SAN/NAS) have been created and installed for WebSphere, Oracle, Interfaces, conversion	Team CNSI: GS Host: BG	3/23/2015	5/28/2015		CNSI: JH Host: BG		
Transition Tasks								
130	State stops accepting provider applications & paper-based updates	State: JRH, JRH, AC, NG, LR, RR	5/29/2015	5/29/2015		State: JRH, JRH, AC, NG, LR, RR		
136	Deploy State PE (Application and Interfaces) Code in Production Environment	Team CNSI:AM, MB	7/11/2015	7/16/2015		CNSI: JH		
[redacted] State PE Go-Live - (12:00AM) July 20 2015								
Management Gate Meeting - Sponsor Meetings								
144	Management Gate Meeting - Program Leadership Meeting (Gate-1) "Approve entry to 14-day implementation activities"	Program Leadership	7/2/2015	7/2/2015		N/A		
145	Sponsor Meeting "Status Update"	Sponsors & Program Leadership	7/15/2015	7/15/2015		N/A		
146	Management Gate Meeting - Executive Leadership/Sponsor Meeting (Gate-2) "Final Go/No-Go Decision"	Executive Leadership/Sponsors	7/16/2015	7/16/2015		N/A		

MTPSM-3-338

Figure 3.10.2-11. Sample Excerpt of Implementation Checklist. The implementation checklist includes all the details necessary to complete implementation of the PMIS module. This example shows a few tasks from three of the many areas tracked in the checklist.

Provider Enrollment Implementation June 2015

Monday	Tuesday	Wednesday	Thursday	Friday
June 1	2	3	4	5
	Host/CNSI: Complete Production SAN/NAS Setup, Production DB Setup & Application/Interfaces Setup State: Complete generating Round 1 mail to providers		Host/CNSI: Confirm Go-Live readiness of PE production hardware and infrastructure	CNSI/Host: Start verifying access to Production Environment (Application, DB, Interfaces) State: Start verifying access to Production Environment (VPN, DB, Support tools)
8	9	10	11	12
	CNSI/Host: Complete verifying access to Production Environment (Application, DB, Interfaces) State: Complete verifying access to Production Environment (VPN, DB, Support tools)			Host/SSO/CNSI: Complete Production SSO Setup & Integration State: Verify access to SSO Production Environment
15	16	17	18	19
State: Start SSO User Registration				

MTPSM-3-339

Figure 3.10.2-12. Sample Implementation Calendar. Team CNSI creates a complete calendar of activities leading up to deployment of the system. This excerpt shows sample activities for a single month. The Implementation Calendar for MT PSM will cover all months included in the implementation period.

The implementation activities include final data conversion, provider and operations training, and multiple review gates where DPHHS can review implementation readiness. The final review gate provides Team CNSI authorization to deploy the system in the production environment.

There are many detailed tasks that occur during the final implementation stages to prepare for the transition to Operations. Team CNSI maintains an Implementation Report that tracks each task to completion, including DPHHS reviews. The final submission of the report provides DPHHS with the information required to approve the start of Operations. At the end of this phase, the project transition phase is complete with MT PSM going live, and the Operations phase begins.

Post-Deployment and System Certification

Post-deployment activities confirm all implementation activities have been successfully completed and bring closure MT PSM pre-production activities. Data collection for CMS certification commences immediately upon implementation of the production system. Certification data collection activities continue for a minimum of six months of production operations before DPHHS can request CMS certification. Team CNSI business operations staff, DPHHS staff, and DPHHS' IV&V contractor will be involved in the data collection and certification readiness activities.

Team CNSI has successfully supported federal certification activities with CMS for our Michigan and Washington MMIS projects. Both states received certification on the first attempt with zero findings. Our MT PSM solution is based on previously-certified components and currently aligns with the guidance provided in Medicaid Enterprise Certification Life Cycle (MECT 2.2) for future certifications.

3.10.2.3 Requirements Management

The Contractor must work with the DPHHS MPATH Team to confirm the Contractor's understanding of the RFP requirements and to reconcile the RFP requirements for the scope of work against the proposed solution. The Offeror must describe their approach to meet each of the detailed Requirements Management requirements defined in Attachment F, Requirements Matrix.

Team CNSI's capability for understanding its customer's requirements is one of the fundamental keys to our continued success. We work collaboratively to understand customer requirements and convert those requirements into software and operational solutions that can be designed, developed, tested, and successfully deployed. Requirements traceability is carefully maintained throughout the process. Team CNSI's past successes in implementing the PMIS module in Michigan, Illinois, and Utah were a direct result of collaboration, communication, careful attention to detail, and verifying that the developed systems addressed all approved requirements.

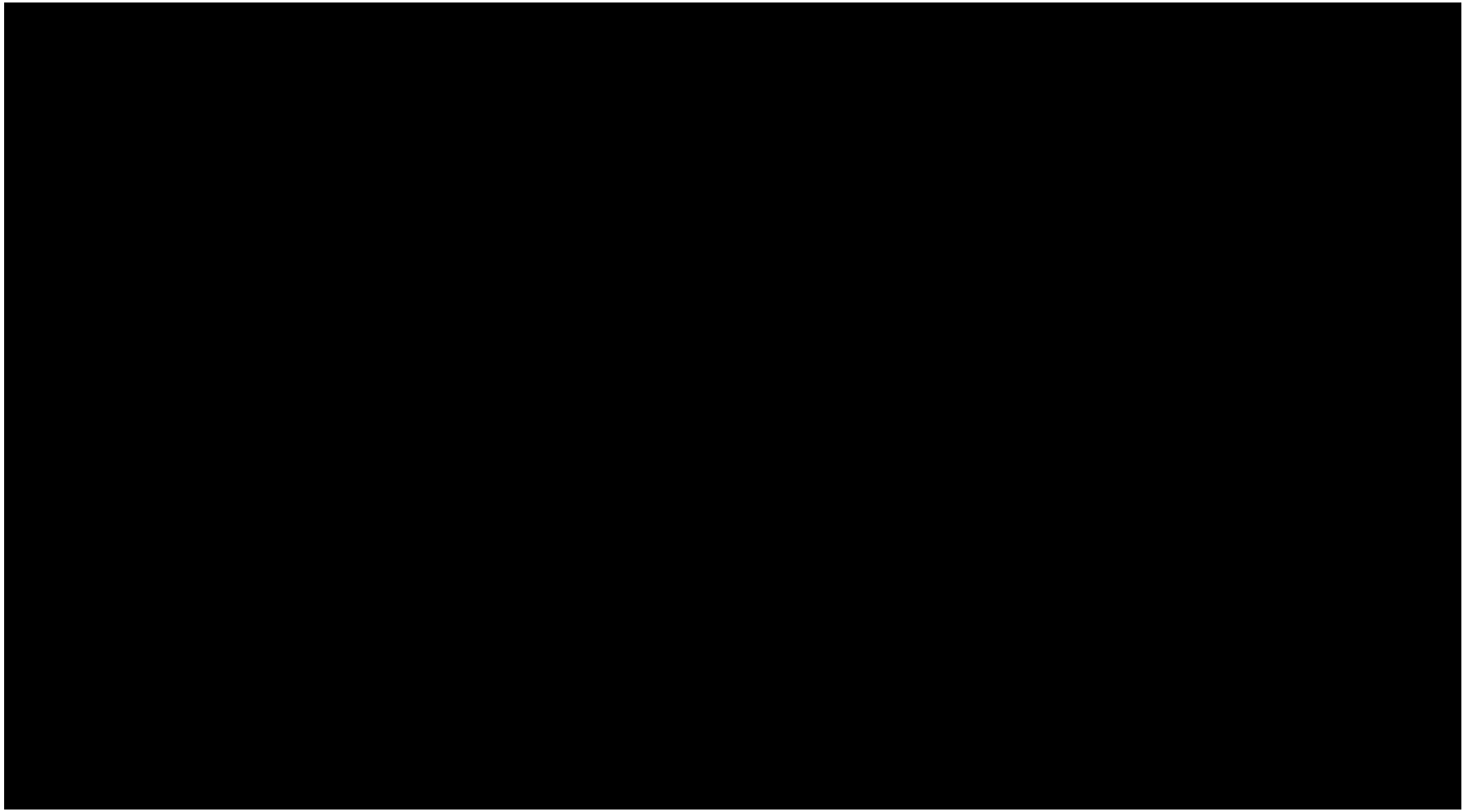
The Team CNSI Advantage

Team CNSI's strategy for requirements management is proven on multiple projects and reduces project risks.

- Team CNSI has a successful track record for effective management of requirements supporting MMIS deployments in Michigan and Washington, and provider enrollment releases in Illinois and Utah
- Leverages the evoBrix MITA traceability to demonstrate how the solution out-of-the box supports core requirements
- Maps the identified gaps that require state-specific configuration to solution components and test cases to provide bi-directional traceability throughout the project

MTPSM-3-309

[redacted]



©2017 CNSI

[redacted]

The Summary Solution Analysis Report is presented to DPHHS for approval. On approval, gaps are baselined and are managed throughout the remaining phases of the project. The Summary Solution Analysis Report presents the details of all gaps approved for configuration by subsystem within the PMIS module. Including Options A and B, Team CNSI will provide the following subsystems in the gap analysis:

- PMIS
- General Services
- Customer Relationship Management
- SiteVisitPro

RQM01

During the requirements validation sessions, the Contractor must demonstrate a fully functioning solution that has been initially configured based on the Contractor's understanding of the requirements described in the RFP and publicly available policy documents, manuals, and fee schedules.

[redacted]

RQM02

The Contractor shall work with the Department to confirm the Contractor's understanding of the requirements and to clarify and/or elaborate requirements where necessary to achieve desired business outcomes.

[redacted]

RQM03

The Contractor shall document any gaps between the initially configured solution and the business requirements in the requirements management tool. Gaps must show bi-directional traceability with applicable business requirement(s), design, test cases, test results, MECT criteria and certification artifacts.

Team CNSI uses a traceability process that fully aligns with DPHHS' requirements. Our traceability process begins with the State's requirements. These requirements are mapped either to existing features in the working evoBrix PMIS module or to a gap that will require configuration for the Montana solution. The first step of the process occurs during Team CNSI's RFP response development where gaps that will require specific solution configuration for Montana have been identified.

The State's requirements are loaded into the Team CNSI Gap Traceability Matrix. A unique gap identifier is assigned to the requirements not fully met in the base evoBrix PMIS module. The gap identifier is carried forward to map to design artifacts, user stories, test cases, and test results, providing bi-directional traceability for all gaps that require solution configuration. The PMIS module is already mapped to MITA business area and business function. Team CNSI will add the MECT checklist and certification artifacts to the traceability matrix. The sample gap traceability matrix, previously presented in the introduction section, is duplicated in Figure 3.10.2-15 for the reviewer's convenience.

[redacted]

RQM04

The Contractor shall, during requirement validation, provide designated Department staff access to a fully functioning environment to become familiar with the solution.

Team CNSI will configure a functioning sandbox environment for use by the State. This environment will be made available during the Solution Analysis phase of the project as defined in the project schedule.

RQM05

The Contractor shall utilize project control tools to formally track all requirements and related design, configuration, testing, and certification artifacts. The Contractor's requirements management tool shall ensure approved changes to requirements are linked back the approved change request.

[redacted]

RQM06

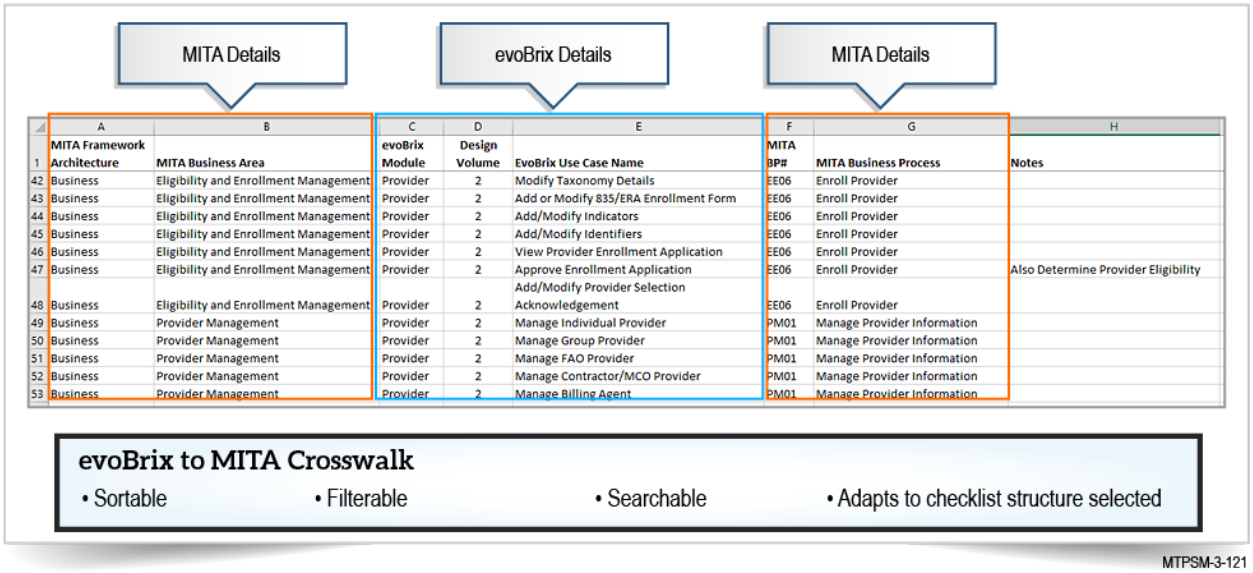
The Contractor shall develop, maintain and submit a Requirements Traceability Matrix (RTM) to track detailed requirements and their realization throughout all project phases. This should include how the requirement is realized (e.g., configuration, custom development, base functionality). All revisions must be reviewed and approved by the State.



RQM07

The Contractor's requirements management tool shall have the ability to manage requirements traceability by module(s), MITA business area, MITA business process and MECT checklists.

Team CNSI's design documentation is pre-packaged with traceability to MITA Business Area and MITA Business process as shown in Figure 3.10.2-16. Team CNSI will extend this to include linkage to the approved gaps, MECT Checklist items, and MECT Certification Artifacts.



	A	B	C	D	E	F	G	H
1	MITA Framework Architecture	MITA Business Area	evoBrix Module	Design Volume	EvoBrix Use Case Name	MITA BP#	MITA Business Process	Notes
42	Business	Eligibility and Enrollment Management	Provider	2	Modify Taxonomy Details	EE06	Enroll Provider	
43	Business	Eligibility and Enrollment Management	Provider	2	Add or Modify 835/ERA Enrollment Form	EE06	Enroll Provider	
44	Business	Eligibility and Enrollment Management	Provider	2	Add/Modify Indicators	EE06	Enroll Provider	
45	Business	Eligibility and Enrollment Management	Provider	2	Add/Modify Identifiers	EE06	Enroll Provider	
46	Business	Eligibility and Enrollment Management	Provider	2	View Provider Enrollment Application	EE06	Enroll Provider	
47	Business	Eligibility and Enrollment Management	Provider	2	Approve Enrollment Application	EE06	Enroll Provider	Also Determine Provider Eligibility
48	Business	Eligibility and Enrollment Management	Provider	2	Add/Modify Provider Selection Acknowledgement	EE06	Enroll Provider	
49	Business	Provider Management	Provider	2	Manage Individual Provider	PM01	Manage Provider Information	
50	Business	Provider Management	Provider	2	Manage Group Provider	PM01	Manage Provider Information	
51	Business	Provider Management	Provider	2	Manage FAO Provider	PM01	Manage Provider Information	
52	Business	Provider Management	Provider	2	Manage Contractor/MCO Provider	PM01	Manage Provider Information	
53	Business	Provider Management	Provider	2	Manage Billing Agent	PM01	Manage Provider Information	

Figure 3.10.2-16. evoBrix to MITA Crosswalk. The evoBrix to MITA Crosswalk provides bidirectional traceability between the PMIS module design components and the related MITA Business Areas and Business Processes.

3.10.2.4 Design, Configuration, and Build

The Contractor shall undertake activities to resolve gaps between the RFP requirements and the proposed solution. Once designs have been approved by DPHHS, the Contractor shall configure and/or customize the solution based on the desired business outcomes. The Offeror must describe their approach to meet each of the Detailed Design, Configuration, and Build requirements defined in Attachment F, Requirements Matrix.

Teams CNSI's approach to system design, configuration, and build is systematic and comprehensive to ensure that both the system and stakeholders are ready for operations in a multi-state source enterprise. The strategy outlined here has been refined through multiple implementations and decades of experience in large healthcare projects that have been successfully implemented.

The Team CNSI Advantage

Team CNSI's strategy for design, configuration, and build is proven on multiple projects and reduces risks, timeline, and costs.

- Team CNSI has a successful track record of effective implementations, including MMIS deployments in Michigan and Washington and provider enrollment relelases in Illinois and Utah
- Leveraging the evoBrix solution allows Team CNSI to focus on Montana-specific differences rather than new system development
- Team CNSI's deep understanding of CMS certification protocols have resulted in a successful track record, achieving certifications in Michigan, Washington, and Iowa

MTPSM-3-103

At the core of Team CNSI's implementation strategy is the evoBrix solution, which is highly configurable and built on components previously certified in Michigan. Using a Solution, Configure, Implement (SCI) methodology, Team CNSI applies a unique approach designed for implementing a modular system, which minimizes time-intensive custom development by focusing on configuration of functionality. This reduces the overall risks to the implementation and timeline. For example, Team CNSI implemented the electronic health records payments functionality in Michigan on time in four months, and provider enrollment in less than eleven months for Illinois.

[redacted]

©2017 CNSI | 3.10-298

[redacted]

DCB01

The Contractor's solution shall accommodate customer preferences for communications by electronic inbox, written correspondence, email, text, and phone

Team CNSI's evoBrix PMIS does accommodate DPHHS' preferences of communications by electronic inbox, written correspondence, email, text and phone.

evoBrix PMIS integrates with Pitney Bowes EngageOne Base (formerly DOC1) module to generate correspondence letters for communication. Furthermore, evoBrix PMIS also supports electronic inbox and email communications. MT PSM CRM solution supports text and phone communications.

DCB02

The Contractor shall develop and submit a design session schedule, agendas, and minutes for review by the Department.

With over 18 years of experience in large healthcare projects, Team CNSI fully understands how critical it is to plan and manage solution sessions. Team CNSI leverages the lessons learned and templates from prior projects to prepare and present to DPHHS the solution session schedule, agendas, and minutes for review.

Team CNSI first plans and prepares the session schedule. To effectively manage participants' time, each team sets up what are referred to as "island times." The "island time" approach establishes designated times for each business area to meet. By scheduling consistent meeting times each week, we resolve the many logistical and scheduling difficulties and support an efficient review of the solution. A sample "island time" schedule from one of our other projects is shown in Figure 3.10.2-18. Team CNSI will work with DPHHS to update the team names and schedule for Montana.

Collaborative Application Design Schedule

Day	Session Date	Time	Business Area
Wednesday	7/26/17		Holiday
Thursday	7/27/17	8:30AM - 12:00PM	Provider Reports
		1:00PM - 4:00PM	Provider Reports
Friday	7/28/17	8:30AM - 12:00PM	Provider Enrollment
		1:00PM - 4:00PM	Provider Correspondence
Saturday	7/29/17	8:30AM - 12:00PM	Provider Enrollment
		1:00PM - 4:00PM	Provider Interfaces
Sunday	7/30/17	8:30AM - 12:00PM	Provider Customer Relationship Management
		1:00PM - 4:00PM	Open

Color Key:
Provider Reports
Provider Enrollment
Provider Correspondence
Provider Interfaces
Provider Customer Relationship Management

MTPSM-3-114

Figure 3.10.2-18. Sample "Island time" Schedule for Solution Sessions. Island times allow participants to know exactly when they will be meeting.

It is anticipated that not every team member will need to attend every session. Therefore, the lead for each team will publish a session agenda for the sessions in advance of the meetings. In addition to the agenda, Team CNSI creates a presentation outlining the gap solution prior to the sessions. This allows DPHHS to review and come prepared to the session with applicable questions on the gap solution. At the conclusion of each session, the Team CNSI lead facilitates a summary review with the meeting participants, ensuring there is agreement on the solution decisions and action items captured in the session. Meeting minutes are then created and provided to the project teams for review.

Team CNSI will post an agenda 24 hours in advance of all meetings, while meeting minutes for the meetings will be posted within two days of completing the meeting. All meetings are scheduled through the Team CNSI SharePoint Documentation Repository. Agendas are posted to SharePoint 24 hours in advance of the meetings, along with any materials to be reviewed at the meeting. Meeting minutes are posted to SharePoint promptly within two days after the meeting is complete. In addition to capturing the meeting notes, Team CNSI also captures follow-up action items with assignments and due dates, emerging risks, and potential issues. We also keep a list of "Parking Lot" items that are outside the scope of the meeting but need to be addressed at some point in the future.

DCB03

The Contractor shall conduct collaborative design sessions to address all gaps identified during requirements validation.

[redacted]

[redacted]

DCB04

The Contractor shall, in the design sessions, recommend solutions for each configuration gap, as defined in requirements validation, that will produce the desired business outcomes. If a gap cannot be addressed via configuration, the Department may consider making policy changes before approving customizations to the solution.

[redacted]

DCB05

The Contractor shall demonstrate completed functionality frequently as the solution is configured/built, using a fully functioning environment.

Team CNSI's fully leverages the operational evoBrix PMIS solution throughout the SCI process to provide demonstrations. The first demonstrations occur early in the project to help users visualize and validate gaps during the solution analysis. Demonstrations are also used during solution sessions when showing the system helps the user in being able to understand the proposed solution to the gaps.

Team CNSI continues to demonstrate the modified system during the Configuring phase. These demonstrations are periodically scheduled after several configuration iterations are complete, so that the users can see complete business functionality. This allows the users to confirm progress as well as validate if the requirements were well understood by Team CNSI.

DCB06

The Contractor shall migrate completed releases promptly through various testing levels all the way to User Acceptance Testing (UAT).

Team CNSI has a proven, robust testing process which has helped us in successful implementation of the Provider module for the states of Michigan, Washington, and Utah.

Per the proven testing process, every release is thoroughly tested in various testing levels, as mentioned below, before it makes its way to User Acceptance Testing (UAT).

Iteration Testing

Code for a release is thoroughly tested and any Severity 1, 2, or 3 bugs, if any, are fixed and regression tested before migrating the release into System Testing

System Testing

Code for a release is thoroughly tested and any Severity 1, 2, or 3 bugs, if any, are fixed and regression tested before migrating the release into System Integration Testing

System Integration Testing

Code for a release is thoroughly tested and any Severity 1, 2, or 3 bugs, if any, are fixed and regression tested before migrating the release into End to End Testing

End-to-End Testing

Code for a release is thoroughly tested and any Severity 1, 2, or 3 bugs, if any, are fixed and regression tested before migrating the release into User Acceptance Testing

User Acceptance Testing

Code for a particular release is thoroughly tested and any Severity 1, 2 and 3 defects, if any, are fixed and regression tested before migrating the release into Production

DCB07

The Contractor shall provide the design for online help approach and documentation, as appropriate.

The operational evoBrix solution includes online, context-sensitive help, which provides users information on the fields and content displayed on the screens, and provides other pertinent information required to execute actions and steps within the solution. Prior to creating the final context-sensitive online help, Team CNSI will create a design approach along with a strawman depicting a structure of the online help file. DPHHS will review and approve the design approach before the final online help is created. Team CNSI uses Adobe RoboHelp to create the context-sensitive online help.

DCB08

The Contractor shall work with the Systems Integrator and the Department to establish required interfaces as defined in the detailed scope of work.

Team CNSI will work with the System Integrator (SI) and DPHHS to leverage the configurable evoBrix Interface Service Repository (ISR) to integrate to the required external systems as defined in the RFP.

Team CNSI will leverage the SI to coordinate with the owners of the interfaces to identify and finalize the layout and data required for each interface that needs to be exchanged between Team CNSI's MT PSM solution and other State or vendor agencies.

Team CNSI will also work with the SI to put together a plan to identify all the tasks needed by each stakeholder to get the interface layout and data finalized. SI will monitor the plan and help Team CNSI, the State agency, and/or Vendor agency to mitigate any slippages.

DCB09

The Contractor shall provide office space for Contractor staff and meeting rooms as necessary to support the scope of work and contractual obligations.

Team CNSI will leverage its existing experienced resources and infrastructure, combined with a local Helena, MT, office and resources to deliver the most cost effective, lowest risk solution and services. The Helena, MT, facility will include office space and meeting rooms to support the necessary activities to fulfill Team CNSI's obligations as defined in the scope of work and contract. This furnished work space will include:

- Secure offices
- Cubicles with at least one secure drawer
- Desk space for visiting Team CNSI and DPHHS staff, with at least one secure drawer
- Conference space for meetings, collaborative sessions, and training
- Break rooms and rest rooms
- Ample parking

©2017 CNSI

DCB11

The Contractor shall develop auditing and general controls to ensure the effective use of the technical architecture and data in meeting requirements.

Team CNSI understands the primary purpose of DPHHS is to establish a common framework to improve communication and co-operation among the parties that create, use, and manage the system so they can work in an integrated, coherent fashion. The Team CNSI approach is to create a Systems Engineering Management Plan that provides the methods and artifacts needed to accurately and adequately document the system, operations architecture. and design; use our Enterprise Architecture Solution Assessment (EASA) methodology to manage auditing and general control that helps in efficient assessment of the architecture. Team CNSI believes in leveraging our end-to-end solution offerings to establish ourselves as a viable and experienced technology and business partner for our clients. To this extent, Team CNSI maintains strategic relationships with several product and services vendors to ensure that we can design, implement, and maintain flexible, platform-independent solutions to effectively accommodate client business needs. We have successfully implemented our solutions with a broad array of partners and vendors in multiple states and have seen the positive results of multi-vendor collaboration.

Team CNSI understands that the MT PSM solution will coexist with several other business modules and technology components in the DPHHS Enterprise environment. The Enterprise environment will be governed by DPHHS based on their enterprise architecture board, with the support of the System Integrator vendor, who will be responsible for Enterprise-level integration across all the business modules and technology components, in a truly multi-vendor environment. Team CNSI has the technology and project management expertise to ensure that the system and supporting technical and business operations are aligned with the enterprise architecture board. We understand the need to support and manage the variety of the artifacts for architecture and design that are used by the various disparate systems supporting the Medicaid Enterprise. Effectively managing the various artifacts is a key to successful integration in the DPHHS distributed environment.

DCB12

The Contractor must provide all technology and equipment for contractor staff necessary to support and complete the scope of work and the contractual obligations.

Team CNSI will provide the technology and equipment for its staff necessary to support all project activities necessary to fulfill obligations defined it the scope of work and contract. This includes:

- Business-class internet service for optimal production and connectivity
- Laptops (or alternative): minimum one per project staff member
- Voice over Internet Protocol (VoIP) telephones or equivalent: one per individual workspace/one per conference space
- Printer/Copy/Scan/Fax Utility: minimum one per facility
- Secure network connection, via hard wire to a data port, or wireless access: one per individual workspace
- Shredding bins for sensitive data disposal
- Projection Device (large monitor or projector): one per conference space (six-person or larger)
- Appropriate standard cubicles and task chairs for individual workspaces
- Smaller cubicles for guest workspaces (individuals not permanently seated at the facility)

- Appropriate work surfaces and chairs in all conference spaces
- Breakroom stocked with a variety of beverage vending machines (such as coffee, tea, soda, water), a snack vending machine, a sink, and a refrigerator

DCB13

The Contractor shall be responsible for operating and maintaining any software needed to support all module components and project tools in use by the Contractor.

Team CNSI acknowledges and accepts the responsibility for operating and maintaining all necessary software for the module components and project tools as defined in the contract for the MT PSM. To accomplish this, Team CNSI has established software management policies and procedures based on the iVision360 methodology. Tailored to support Team CNSI's software components and tools in alignment with the MT PSM solution implementation and operational needs, this approach allows for the following:

- Configurations management: Team CNSI's configuration management procedures are based on major deliveries of large healthcare projects and are tailored to meet Montana requirements. The ITIL-aligned processes and procedures provide a framework to avoid any unauthorized changes, manage releases to multiple environments, and provide traceability to configuration items throughout the life cycle of the MT PSM project.
- Software release management: Team CNSI maintains a release tracking sheet where all the software releases are maintained. This sheet serves as the guide to promote the software package along with publishing applicable release notes to the appropriate stakeholders. Jira is used to manage and track the modifications to the source code, and Subversion is used by the configuration management team to maintain version control of each software release package.
- Asset Management: Team CNSI collaborates with DPHHS to create and maintain full asset management and change documentation, including inventories and versions of all software and hardware. The asset management documentation includes details such as network configurations, operating systems, databases, storage arrays, and hardware specifications, and is maintained in tools as defined in Figure 3.10.2-20. Team CNSI works with DPHHS to plan, coordinate, and integrate releases for all assets.

Tool	Task	Description
SharePoint	Project Repository	Collection and tracking of project documentation, including manuals, plans, status reports, meeting minutes, and project-related artifacts including solution/configuration mapping documents, Issues, Risks, Action Items, Meeting Scheduling, and Change Management.
Subversion	Managing Code Development and Configuration Items	Management of code development and tracking of version of configuration items. A separate SVN Software Development Library server is used to maintain the repository.
Jira	Defect Management	Used to manage defects and enhancements to the system. The Jira database is maintained on a separate server. CNSI uses the IBM Rational Unified Change Management (UCM) approach, which allows users to connect various versions of components from SVN and relate them to activities in Jira.
iTOP	Hardware Asset Management	Management of all hardware configuration items to manage multiple environments.

Figure 3.10.2-20. Asset Management Tools. Team CNSI maintains all assets using defined configuration management processes and tools.

In addition to the tools listed above, Team CNSI will maintain any software needed to support all module components. Detailed information about various applications and areas that are required to support all module components are listed below in Figure 3.10.2.-21.

Product/Application/Area	Version	Category	Vendor
IBM Cognos	10.2.2	Reports	IBM
IBM FileNet	5.2.x	ECM	IBM
IBM InfoSphere DataStage	11.5	Conversion	IBM
Oracle Database	12c	Database	Oracle
Oracle RAC	12c	Database Cluster	Oracle
Oracle JDK	1.6.x/1.7.x/1.8.x	Application Server	Oracle
Oracle Siebel CRM	8.1.1.14 PS 13	CRM	Oracle
Oracle SOA	12.1.3	Integration Tool	Oracle
Oracle WebLogic (Base)	12c	Integration Tool	Oracle
Oracle WebLogic (Cluster)	12c	Integration Tool	Oracle
Oracle Enterprise Manager	12c	Monitoring Tool	Oracle
Oracle Advanced Security	12c	Database Security	Oracle
Oracle MySQL	5.x	Database for OTRS	Oracle
Linux	OEL	Operating System	Oracle
Spectrum UAM	11	Correspondence	Pitney Bowes
EngageOne DOC1GEN	6.0.1	Correspondence	Pitney Bowes
EngageOne DOC1 Designer	6.x	Correspondence	Pitney Bowes
EDIFECS XEngine Server	8.8	EDI	EDIFECS
Avaya		IVR	Avaya

Figure 3.10.2-21. Software Topology. List of software needed to support Team CNSI's evoBrix PMIS solution.

DCB14

The Contractor's solution shall have the ability to print a properly formatted representation of the entire screen (including sections not displayed without scrolling) and associated data in the application.

The Print icon provides access to the Print command. On web pages/details pages, the user can click the Print Button on the Utility Bar, and on dialog boxes user can click the Print icon, as shown in Figure 3.10.2-21. This icon is displayed on all dialog boxes. The Print button enables the user to print a printer-friendly version of the page. By default, the page is printed in a portrait format.

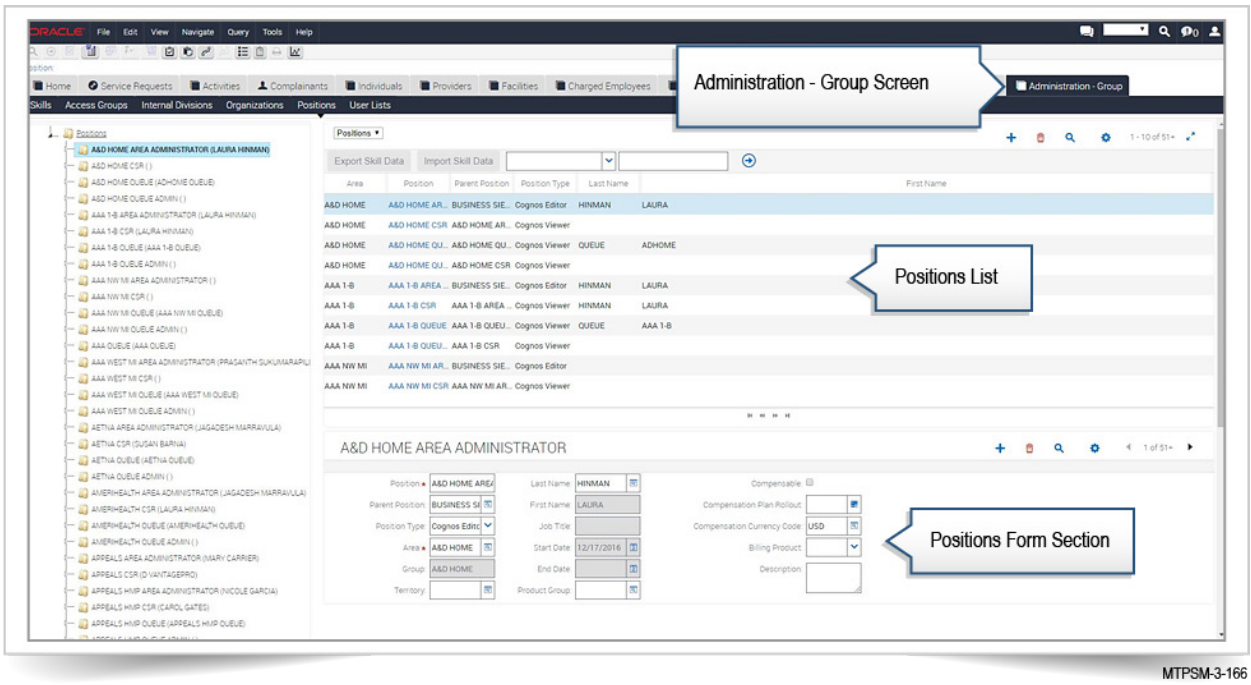


Figure 3.10.2-21. evoBrix Print Features. The evoBrix solutions allows users to print a properly formatted representation of the screen.

DCB15

The Contractor shall provide recommendations for simplified business rules and business processes to the Department.

As part of the solution analysis and modeling activities, Team CNS systematically identifies opportunities to simplify business rules and processes. For example, during our provider module solution activities for our Utah project, Team CNSI identified and documented over 20 business process change opportunities. Team CNSI has already started the review of the Montana RFP requirements and collection of business process change candidates. During the execution of the solution sessions, Team CNSI will recommend business process simplification as part of the solution for DPHHS to consider.

DCB18

The Contractor shall configure, support and maintain all components of the solution in a manner that reflects performance expectations described in this RFP.

Team CNSI acknowledges and accepts the responsibility to configure, support, and maintain the MT PSM solution in accordance of the performance expectations and service levels defined in the RFP. To ensure service levels are met throughout the contract term, Team CNSI leverages our 24x7 Network Operations Center located in Rockville, Maryland; our HealthBeat tool, iTOP Configuration Management Database (CMDB), Oracle Ops Center, and Oracle Enterprise Manager. Team CNSI uses this standard toolset to measure, monitor, and report performance against the defined service levels on an ongoing basis throughout the life of a contract.

Team CNSI's service level reporting solution provides DPHHS with configurable management capabilities. Figure 3.10.2-22 shows the tool architecture. This solution uses a service level Automation Engine which is configured to automatically or manually track various service levels related to system and business functions, such as interfaces and report generations. This allows Team CNSI and DPHHS to have visibility of daily system and business functions and their corresponding service level performances. The tool is also equipped with tracking, reporting, and management capabilities using Team CNSI's HealthBeat as the front-end application.



DCB19

The Contractor's solution shall be free of any software components that are the result of legacy code transformation.

Team CNSI acknowledges and accepts that the MT PSM solution be free of any software components that are the result of legacy code transformation. Team CNSI's evoBrix solution is a fully modern solution and is at its core an operational modular Medicaid platform built on a highly scalable technical architecture that is web-based, rules-driven, and service-oriented, and can interoperate with the best-of-breed COTS products in a modular fashion. Based on this technical architecture foundation, Team CNSI's

evoBrix is fully backed by its solid track record of enabling the states of Michigan, Washington, Illinois, and Utah to successfully run provider and/or claims management functions.

DCB20

The Contractor's solution shall provide Web based content that is supported by standard web browsers and are mobile and tablet compatible.

Team CNSI's proposed evoBrix PMIS solution is developed with W3C web-based standards and is designed to work on Internet Explorer, Safari, Firefox, and Chrome browsers. It is designed to be robust and highly scalable. Additionally, it separates content from logic and is interoperable with other systems/ interfaces compliant with responsive layouts regardless of being used on computers, laptops, or tablets.

DCB21

The Contractor's solution shall allow the Department to edit and change any static text in the application and correspondence templates. All static text must be approved by the Department.

Because evoBrix satisfies a significant portion of Montana's functional requirements out of the box, the solution sessions primarily focus on the configuration the MT PSM solution, including the static text within the application and correspondence templates. Team CNSI will work collaboratively with DPHHS during these meetings to identify and document the edits and changes. Once finalized, the static text will be documented in the detailed design documentation and presented to DPHHS for approval using our deliverable review process as outlined in Section 3.10.37, Project Deliverables and Documentation.

3.10.2.5 Data Conversion, Cleansing, and Migration

Data conversion, cleansing, and migration activities required to support the scope of work contained in this RFP include planning, identifying and analyzing conversion specifications, testing, execution and coordination of all data and file conversion, migration and data cleansing processes.

Data conversion often encounters risks and issues related to the complexities in defining the relationship between source and target data structures, differences in the data required for processing between legacy and new systems and the historical changes to processing requirements and valid codes that may result in data inconsistencies and missing data conditions. The Offeror must describe their approach to meet each of the detailed data conversion, cleansing and migration requirements defined in Attachment F, Requirements Matrix.

Data Conversion and Migration Strategy

Conversion of the legacy data is an integral component of any MMIS implementation. Team CNSI is highly experienced in managing all aspects of the process to convert legacy data into the new system.

Team CNSI has successfully accomplished data conversions for the states of Maine, Washington, Michigan, Utah, and Illinois. The technical and management processes used on those large-scale

The Team CNSI Advantage

Team CNSI offers a proven, configurable data conversion solution.

- Highly iterative conversion process
- Exhaustive source data mapping
- Mature exception reporting and handling process
- Comprehensive data cleansing framework
- Automated data validation tools
- Configurable and automated conversion process driven by mappings

MTPSM-3-173

initiatives to support conversion ensured traceability of legacy data and smooth data transition. While working closely with the states, the Team CNSI also executed the production implementation, which involved the final data conversion. In addition to these highly successful initiatives, Team CNSI has also accurately converted legacy data for a multitude of initiatives for the Michigan MMIS system.

Team CNSI's data conversion methodology has been implemented and proven for a multitude of States. As an example, for the State of Illinois provider conversion, 186,000 source providers, and 2.6 million source records were converted successfully into 186,000 target providers and 8 million target records without any issues. Our conversion strategy, shown in Figure 3.10.2-23, ensures that the applicable MT PSM data is converted in such a way as to allow for as much data as possible to be transformed and used to minimize re-entry of the data and avoid costly post-implementation operational data fixes.

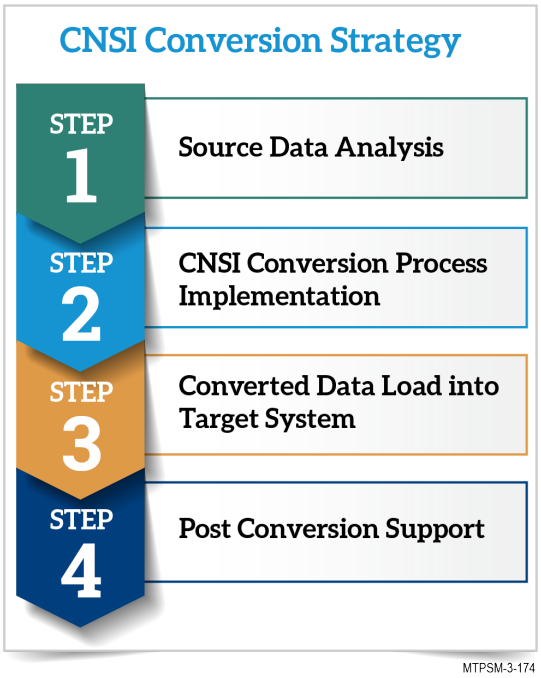


Figure 3.10.2-23. Data Conversion Strategy. Our solution utilizes a proven data conversion strategy.

As part of the data conversion strategy, Team CNSI will work with MT PSM team to identify operationally relevant data from MT PSM's applicable functional areas that need to be converted over to the MT PSM solution. Using our proven data conversion processes, which have been refined and time-tested over multiple MMIS implementations, Team CNSI will consolidate, analyze, transform, and iteratively migrate the data from all historical/active data sources from the existing MT PSM systems to the target/new system. Additionally, our conversion strategy ensures that there is full accountability along with extensive support for robust exception handling, reconciliation, and reporting to provide a comprehensive picture of not only the final conversion data outcome but also improve the quality of the converted data in the MT PSM solution. Team CNSI's data conversion strategy and the applicable conversion processes ensure that any historical data anomalies or operationally inadmissible data are fully corrected or accounted for to make it operationally reliable, functional, and relevant before the converted data starts its life cycle in the new MT PSM solution. Figure 3.10.2-24 details the steps in the Team CNSI Conversion Strategy.

Process Step	Details
Source Data Analysis	Team CNSI data conversion team will carry out a detailed and comprehensive source data analysis with the State team. Source data analysis includes source identification, source data formats, incomplete source data, and business rules spanning multiple timespans.
CNSI Conversion Process Implementation	Team CNSI data conversion team will plan and carry out a well-defined data conversion and migration. The conversion process will be an iterative process with special emphasis on exception identification and resolution. An extensive validation and reconciliation process, along with a reporting mechanism, is incorporated into the conversion process to provide a comprehensive feedback mechanism to account for all applicable legacy data records in their migration to the MT PSM system. During this phase, the State will have to address any source data issues that are reported, and Team CNSI will support and reprocess the data that is fixed.
Converted Data Load into Target System	Team CNSI data conversion team will load the converted data into the Target System as part of the implementation. Storage requirements for the final source dataset are also determined.

Process Step	Details
Post Conversion Support	Team CNSI data conversion team will provide post-conversion support during operations to address any converted data issues and clarifications.

Figure 3.10.2-24. Team CNSI's Data Conversion Strategy. Our solution has a detailed phased approach to conversion.

DC01

The Contractor shall convert all member and provider data history for any member or provider that has been active within the past three years and three (3) years of all applicable operational data from the State's legacy systems. The Department may require additional data to be converted on an exception basis to support ongoing business needs (e.g., TPL recovery, SURS recovery and drug rebate). The Contractor shall produce comparative reports for all converted data. Any data quality issues will be addressed by the State within each source system.

Building on our experience and successful past conversions, the Team CNSI data conversion team is well equipped to address any unique challenges with respect to data conversion in each business area. Our approach, to commence the conversion activities early in the life cycle, acknowledges the fact that data is the single largest factor in the continuity of business from legacy to the new system. We begin conversion planning and analysis literally from day one to provide sufficient lead time to support the MT PSM solution. Team CNSI also understands that different State agencies have different types and formats of transactional and operational data that may not lend itself to traditional data conversion approaches. Based on our experience in working with many states and understanding the challenges in dealing with legacy data varieties, Team CNSI supports a broad swath of data types that include Character, Numeric, Date, and Large Objects (Binary Large Objects, Character Large Objects) data type fields, in addition to other free-form fields with embedded data elements. Team CNSI has developed several pre-built data conversion routines that help the overall conversion experience by accelerating the formatting, standardization, and data cleaning that is a must for transforming the data in a standardized manner to facilitate streamlined conversion.

As part of the MT PSM conversion effort, the conversion team will convert all the supporting source data to ensure that the business and usage requirements are met right from go live in the new MT PSM solution. Team CNSI will also ensure that timely reconciliation reports, comparing the source and target converted datasets, are provided to the State so that data quality issues can be taken up early on and addressed within the source system, improving the conversion data quality for subsequent runs.

The conversion data is classified into two main categories:

- Reference Data – All data which is used across multiple records or functional areas is defined as reference data. For example: procedure codes, diagnosis codes, user IDs.
- Transactional Data – All data which is generated for specific transactions is defined as transactional data. For example: individual claim records.

The conversion process will take the following into account:

- Conversion of all operationally relevant and required source data for day-to-day operations
- Sufficient historical data to ensure all audit and legal requirements are addressed
- Varying time periods for different functional areas which are required for reporting, analytics, and business operations

The data conversion process is designed to meet the following specifications:

- Be repeatable across multiple environments, including development, system testing, user acceptance testing (UAT), and production environments
- Be scalable to support varying data load volume and complexity
- Have a robust exception handling mechanism to provide feedback on the data quality to improve the data conversion outcome
- Have the means to cleanse the data, either by correcting the source data or providing the applicable business rules to accomplish it as part of data migration
- Have a comprehensive reporting mechanism to provide statistics on the converted data

The prerequisites for the data conversion process include the following:

- Source file layouts
- Source file data extracts
- Data standardization to provide the data in an agreed-upon format
- Data cleansing, as applicable, based on the feedback from the conversion process

Data Conversion Phases

The data conversion process will be executed in the following phases, as summarized in Figure 3.10.2-25.

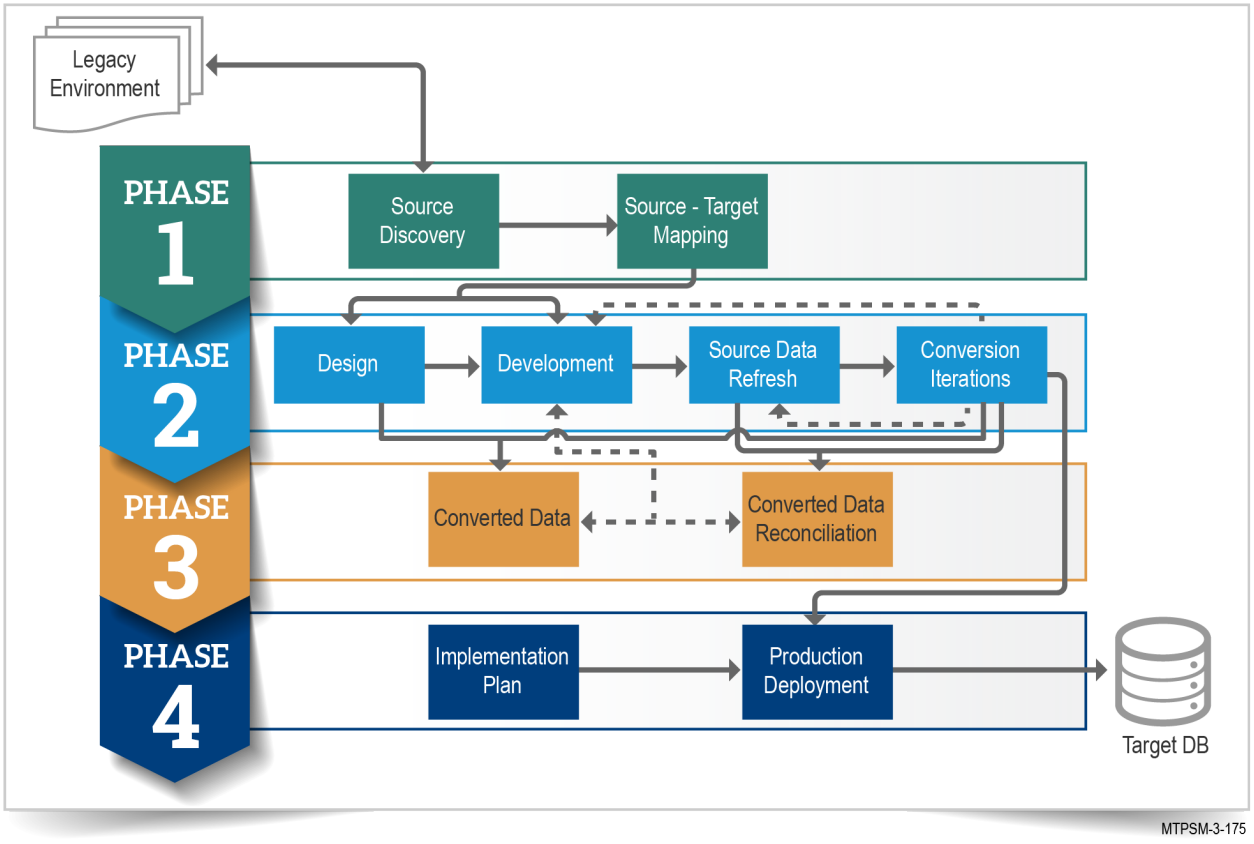


Figure 3.10.2-25. Data Conversion Process Phases. Our solution will provide a highly detailed and accurate conversion process through phases.

Phase 1

- Source Discovery – As part of the process for Source Discovery, the Team CNSI data conversion team will work with the MT PSM team to thoroughly understand the legacy data model and how data is stored within the legacy processes in the source system. Team CNSI will then work with the appropriate stakeholders to identify sources in the legacy source environment and prepare a master list of sources to be converted.
- Source to Target Mapping – Our data conversion team will work with the appropriate stakeholders to prepare a master source to target mapping document.

Phase 2

- Design and Development – Our data conversion team will design and develop the required conversion jobs for converting the data from the source system to the target system.
- Conversion Iterations – Upon completion of the design and development, the Team CNSI data conversion team will run the source data through an iterative process wherein invalid source data will be identified. Comprehensive reports will be submitted to the State after each iteration so that the invalid data identified can be fixed before the next iteration.

Phase 3

- Converted Data Validation – Our data conversion team will carry out extensive converted data validation through the target application as well as through extensive backend querying. Comprehensive reports will be submitted to the State on a periodic basis.
- Converted Data Reconciliation – Our data conversion team will carry out thorough extensive converted data reconciliation between source data and target converted data. Detailed Comprehensive reports will be submitted to the State on a periodic basis.

Phase 4

- Deploy to the production environment – Our data conversion team will deploy the converted data to the production environment in accordance with the implementation plan.

DC02

The Contractor shall provide authorized Department or other designated staff access to an environment to validate converted data and provide support for the data validation effort.

Team CNSI's data conversion team will carry out detailed validation and reconciliation of the MT PSM converted data as part of the overall conversion process (please refer to DC01-06). Along with this activity, the conversion team will assist the MT PSM team in carrying out an independent validation and reconciliation of the converted data. This is achieved by:

- Giving the MT PSM team access to the conversion environments holding the converted data.
- Assisting the MT PSM team in carrying out an independent backend reconciliation of the converted data.
- Assisting the MT PSM team in carrying out an independent frontend validation of the converted data.
- An iterative conversion process during which exception and reconciliation reports are generated and reviewed with the MT PSM team after each conversion iteration. Based on the MT PSM review and feedback, appropriate corrective action will be taken either in the source system or during the

conversion process based on specific business rules provided. This will be validated and verified during the next conversion iteration.

Separate and independent validations and reconciliations done by the data conversion team and the MT PSM team ensure:

- The converted data is looked at from multiple viewpoints so that all possible business scenarios are accounted for, validated, and reconciled.
- The MT PSM team can look at the converted data in the target database as well as through the frontend application.
- As the conversion team deals with live production data for the conversion iterations, the conversion process will account for all possible data inconsistency scenarios and surprises from the source data.

DC03

The Contractor shall work with the State to identify the data elements from existing legacy systems that will or will not be converted to the Contractor's solution. The Contractor shall work with the State to achieve desired business outcomes without familiar data elements.

Producing Source-to-Target Mapping

Data mapping is a critical aspect of the data conversion process. Data mapping is the process of selecting which source data from the legacy source system will be converted to the relational tables of the target system to meet all the business requirements. The Team CNSI data conversion team will work with the MT PSM team to prepare a source-to-target mapping document.

A detailed gap analysis is performed for the MT PSM. The scope of this analysis includes all the key elements required in the target system and the availability of those elements in the source system. Several scenarios are considered when looking at the data fields:

- Some of the source fields may not be required in the target system
- Certain target fields need to be auto generated from date, sequence, or random numbers
- Certain target fields require translation from source data attributes to target data attributes
- Certain target fields contain default values that need no input from the source fields
- Certain source fields are required from the source system but are not present in the target system

To document these rules, Excel will be used for detailed source-to-target data mapping. Data element mapping is where the detailed analysis and documentation for converting each data element required by the target system to meet needs of the business areas is accomplished. The data entities and elements are documented in the format in the conversion design document as shown in Figure 3.10.2-26, which provides sample target data entities and elements documented in the conversion design document.

No	Target Table	Target Column	Target Column Data Type	Target Column Data Format	Nullable? (Y/N)
1	Target Table 1	Target Column 1	Number	30	N
2	Target Table 1	Target Column 2	Varchar2	60	Y

Figure 3.10.2-26. Source Data - Target Data Mapping. The table provides a sample target mapping.

Figure 3.10.2-27 provides sample source data entities and elements documented in the conversion design document.

Source System	Source Table	Source Column	Source Column Data Type	Source Column Data Format	Mapped? (Y/N)
Source 1	Source Table 1	Source Column 5	Number	20	Y
Source 2	Source Table 2	Source Column 3	Varchar2	40	Y

Figure 3.10.2-27. Source Data - Source Data Mapping. The table provides a sample source mapping.

Figure 3.10.2-28 provides sample transformation and validation rules documented in the conversion design document.

Transformation rules	Validation Rules	Mapping Notes/Comments	Remarks
Straight Copy	Numeric values only. Exception out other values.	N/A	Remark1
No special characters to be converted. Replace with spaces during conversion.	Validate that no special characters are present	N/A	N/A

Figure 3.10.2-28. Source Data - Transformation and Validation Rules. The table provides a sample of the transformation and validation rules for target mapping.

The data mapping effort in preparing the source to target mapping document will clearly define the conversion process so that it is understandable by analysts, reviewers, and authorizers critical to the success of the conversion effort. The basic metadata requirements for the target, source, and conversion rules for the data mapping effort are identified in the design document. Each data element can be a simple one-to-one conversion or an extremely complex many-to-many conversion with dependencies on the multiple associated columns on both. Figure 3.10.2-29 provides the most basic conversion process where a single source data element is converted to a single target data element.



Figure 3.10.2-29. Basic Conversion for Source Data Element. Single source data element conversion.

Figure 3.10.2-30 provides a representation of a more complex scenario where four source data elements (with one of those source elements being a previously converted target element – a 'conversion' dependency) are required to create two target data elements.

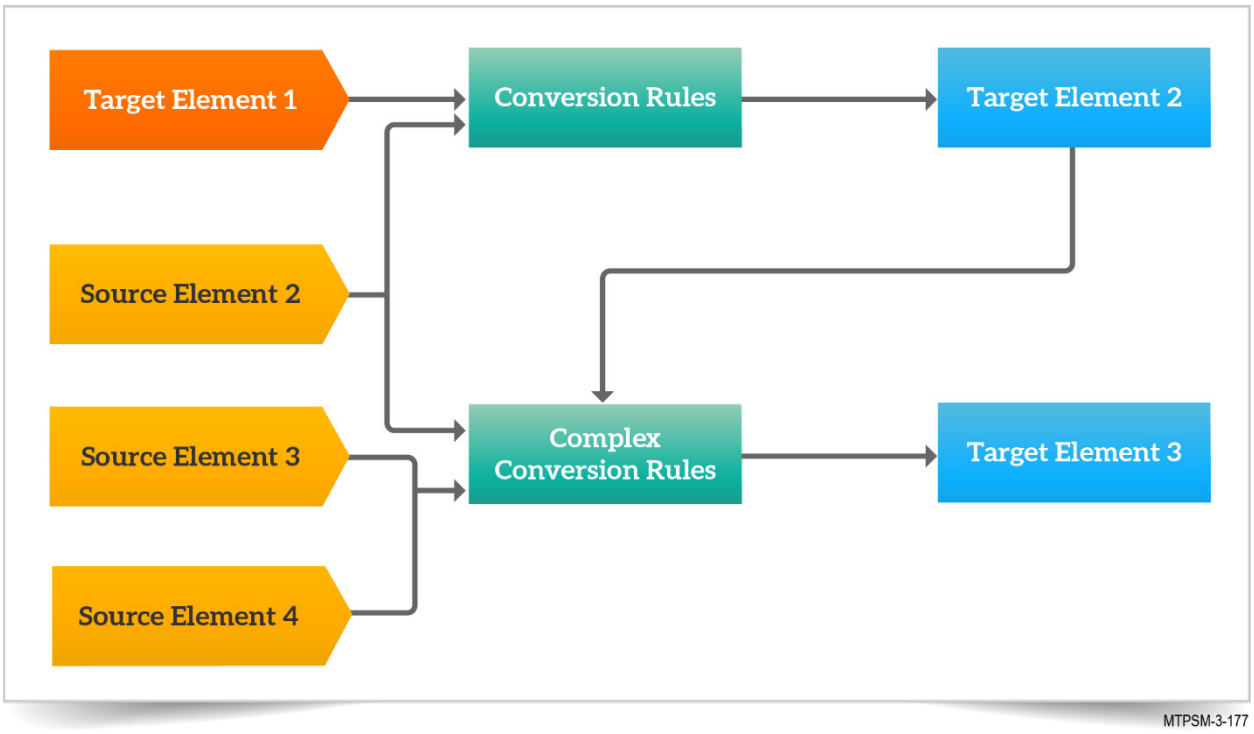


Figure 3.10.2-30. Complex Conversion for Source Data Element. An example of a multi-source data element conversion.

DC04

The Contractor shall work with the State to identify data elements or fields in the Contractor's solution that are not available to be converted from the legacy system, and whether the conversion programs should fill them with default or initial values.

The Team CNSI data conversion team will produce detailed source-to-target mapping for MT PSM (please refer DC03). Every field for the MT PSM module on the target side which does not have a corresponding source side field mapping will be accounted as shown in Figure 3.10.2-31.

Source Data Element	Resulting Conversion Team Update
All reference data field values will be accounted for in the target MT PSM functional DSDD. For example, Status of a Provider.	Conversion Team will set up and utilize the target reference values as part of the conversion for MT PSM. The conversion mapping document will clearly specify how the reference data field values will be used.
All default values in the target data model. For example, Primary key values for tables, audit fields.	Conversion Team will populate all fields which require default values in the target system. The conversion mapping document will clearly specify and list all default values.

Figure 3.10.2-31. Target Reference and Default Values Setup. Conversion Team to account for all reference values needed.

Source Data Elements not Present in the Target Data Model

The Team CNSI data conversion team will identify source data elements which are required but not present in the target data model during the conversion mapping exercise. The conversion team will work

with Team CNSI's functional team and data modeling team to address these missing data elements on the target side based on the functional requirements for MT PSM.

One of the following outcomes, shown in Figure 3.10.2-32, will be arrived at and the conversion team will address the missing source data elements accordingly:

Source Data Element	Resulting Conversion Team Update
Missing source data element has been included in the target data model.	Conversion Team will add the missing source data element to the conversion mapping document and map the required conversion rules.
Missing source data element has been deemed not required for the target data model and not included. MT PSM team has indicated that the data element is required to be stored for legal and/or audit requirements.	Conversion Team will store the required data element on the target side in a secure backend environment.
Missing source data element has been deemed not required for the target data model and not included. MT PSM team has indicated that the data element is not required to be stored.	Conversion Team will not include the data element on the target side in any form.

Figure 3.10.2-32. Source Data Elements not in Target Data Model. Conversion Team will ensure source data fields are addressed in the target system.

As part of the conversion mapping exercise any reference data element or values not present in the MT PSM functional DSDD will be taken up and accounted for with Team CNSI's functional team and data modeling team.

DC05

The Contractor must perform one or more trial conversions as necessary, before final conversion of the data, and present the results to the State.

Team CNSI's data conversion process is an iterative process (please refer to DC01). As soon as the conversion development phase is complete, the conversion team will run conversion iterations on a predefined basis (at least once a week for the MT PSM). Exception and reconciliation reports will be generated and reviewed with the MT PSM team after each conversion iteration. Multiple conversion iterations with live legacy system production data will address all possible source data inconsistency issues before the final go-live conversion run. This strategy mitigates the risk of relying on a single trial conversion run prior to the go-live production run and brings in a disciplined approach of multiple, incrementally improving iterative conversion runs, that will benefit the State in ensuring a smooth transition to the new MT PSM solution.

Case in Point: The conversion team ran a total of 28 iterations on a weekly basis for the Illinois provider implementation. The iterations used live legacy production source as of the iteration run date. This enabled the Team CNSI conversion team to generate highly accurate exception and reconciliation reports for the data to be converted as well as account for all data inconsistencies right until the final Go Live conversion run. The state was involved in reviewing the exception and reconciliation reports for every iteration and addressing resolutions in a timely manner.

As an example, for the State of Illinois provider conversion, 29 full conversion iterations were run (including the final Go Live PE Conversion Iteration). Figure 3.10.2-33 summarizes the conversion details.

No	Description	Count
1	Iterative Full Conversion Runs for Illinois PE Conversion	28
2	Final Full Conversion Runs for Illinois PE Conversion	1
3	Illinois PE Extract Files Received in Each Iterative Full Extract	16
4	Illinois PE Extract Files Received in the Final Full Extract	16
5	Illinois PE Target Transactional Tables	14
6	Illinois PE Action Items Raised During PE Conversion	53
7	Illinois PE Action Items Raised During PE Conversion Pending Resolution	0

Figure 3.10.2-33. Sample Statistics for Illinois PE Conversion. Conversion Team ran multiple iterations as part of the conversion process.

Detailed Exception Reports were generated for the 29 full conversion iterations.

Figure 3.10.2-34 details the number of error records from the total number of records converted from the Illinois Health and Family Services (HFS) system to the Illinois PE subsystem for each conversion run undertaken as part of the conversion process. As the conversion process matured, the error records count showed a significant reduction. The significant upward spike for Conversion Iteration Number 6 was due to a change in conversion requirements, which resulted in incorrect data being generated. This spike was resolved in the subsequent conversion iterations, clearly demonstrating the importance of early engagement with the State agencies in validating the conversion mapping rules so that they may be acted upon on a timely basis ensuring a much cleaner converted data quality.

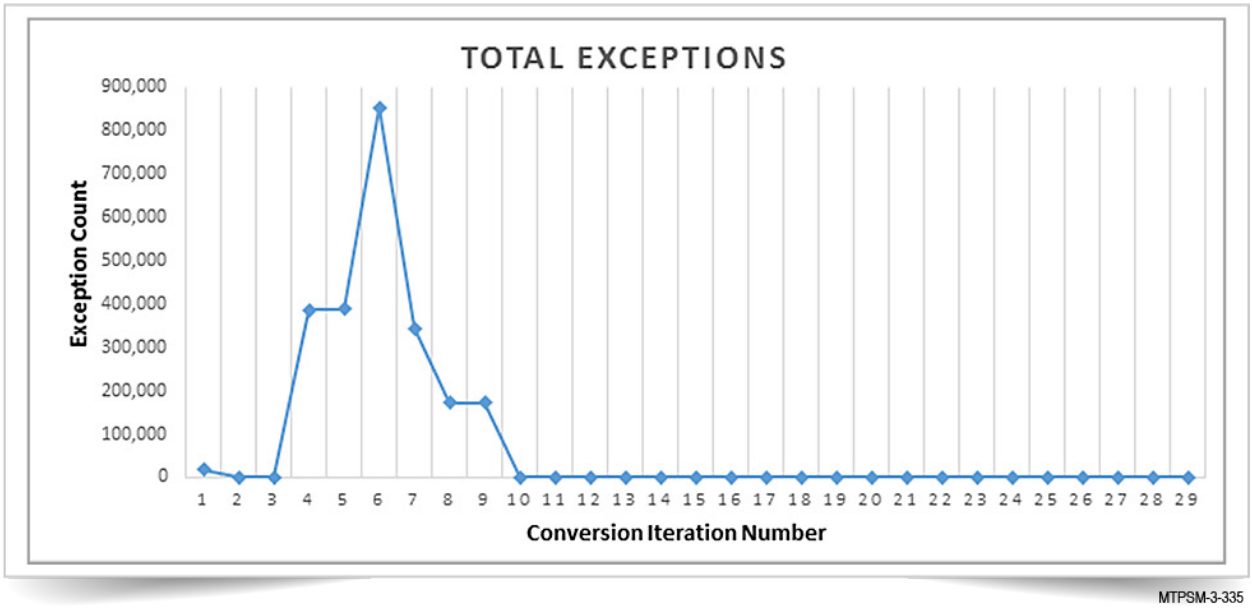


Figure 3.10.2-34. Sample Statistics for Illinois PE Conversion. Detailed exception reports were generated.

Figure 3.10.2-35 details the total number of records converted from the Illinois HFS system to the Team CNSI IL PE subsystem for each conversion run undertaken as part of the conversion process.

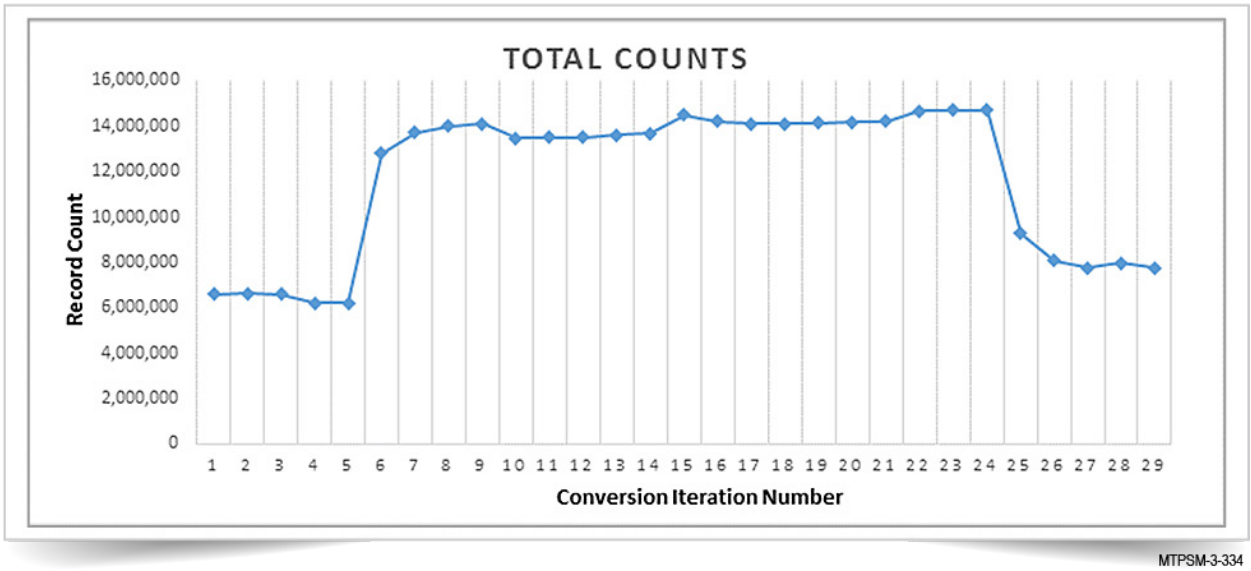


Figure 3.10.2-35. Sample Statistics for Illinois PE Conversion. Detailed reconciliation reports were generated.

DC06

The Contractor shall produce the reports necessary to demonstrate adequate checks and balances within the data conversion process.

Testing and Validation of Converted Data

A multi-step testing and verification process will be used for testing and verification of data during the data conversion process. Figure 3.10.2-36 summarizes the testing performed by multiple teams.

Type of Testing	Owner
Source-to-target data transformation and verification of business rules (unit level)	Team CNSI Data Conversion Team
Target data dependency validation (environment level)	Team CNSI Data Conversion Team
Source-to-target data reconciliation (unit and environment level)	Team CNSI Data Conversion Team MT PSM Team
Review of conversion rules, especially on the target side, by analyzing the equivalent data wherever applicable	Team CNSI Data Conversion Team
Comparison of State converted data (actual) with State converted/non-converted data (expected) wherever applicable	Team CNSI Data Conversion Team
Target data validation and verification via application screens (environment level)	Team CNSI Data Conversion Team MT PSM Application and Testing Teams

Figure 3.10.2-36. Multi-step Testing Process. Our solution ensures high accuracy by having multiple teams test the data during the data conversion process.

System Reporting

The Team CNSI data conversion team ensures that the conversion goes through the following checks:

- Validation: Ensure that the converted data is validated for all functional and business rules of the target system
- Reconciliation: Ensure that all required source records are converted and accounted for

For system reporting, the Team CNSI data conversion team generates the following reports during the iterative phase of the conversion process:

- Conversion Exception Report: The report lists the statistics for the source data and converted target data along with a detailed listing of exceptions which have occurred during the iteration
- Conversion Reconciliation Report: The report lists the reconciliation between the source data and the target data to ensure that all the source records are accounted for

Figure 3.10.2-37 illustrates a sample Conversion Summary Report that was generated as part of the Illinois Provider Enrollment implementation. Team CNSI will generate similar reports for MT PSM with full traceability and accountability for every legacy/source conversion file right from inception to loading them in the target system's application tables. The conversion process also meticulously tracks the specific source records that do not adhere to the agreed upon conversion validation and business rules, and directs them to conversion exception tables to support detailed reporting.

No	Conversion Job	Execution Date/Time	Source Data File	Target Data Table	Rows Loaded	Rows Rejected	Exceptions Flagged
1	Provider Job	04/25/2015 09:33 AM	Provider.dat	TBL_PROVIDER	186,334	0	0
2	Application Job	04/25/2015 09:38 AM	Provider.dat	TBL_APPLICATION	186,334	0	0
3	Address Job	04/25/2015 09:42 AM	Address.dat	TBL_ADDRESS	542,069	0	0
4	Provider Location Job	04/25/2015 09:48 AM	Location.dat	TBL_PROVIDER_LOCATION	186,334	0	0
5	Enrollment Step Job	04/25/2015 09:52 AM	Provider.dat	ENROLLMENT_STEP_DETAIL	1,727,801	0	0
6	Provider Location Association Job	04/25/2015 09:58 AM	Association.dat	TBL_PRVDR_LCTN_X_PRVDR_LCTN	3,280	0	0
7	Provider Location Address Job	04/25/2015 10:02 AM	Location Address.dat	TBL_PRVDR_LCTN_X_ADDRESS	372,668	0	0
8	Provider Location Indicator Job	04/25/2015 10:05 AM	Provider.dat	TBL_PRVDR_LCTN_INDICATOR	205,626	656	328
9	Provider Location Identifier Job	04/25/2015 10:08 AM	Provider.dat	TBL_PRVDR_LCTN_IDENTIFIER	582,410	0	0
10	Provider Location License Certification Job	04/25/2015 10:12 AM	Certification.dat	TBL_PRVDR_LCTN_LCNS_CRTFCTN	199,764	0	0

Figure 3.10.2-37. Sample Statistics for Illinois PE Conversion from a Conversion Summary Report. Summary report of the provider data that was converted for Illinois PE with high level statistics on the number of rows processed/converted, rejected, and legacy records that were logged as exceptions.

Figure 3.10.2-38 illustrates a sample Conversion Detailed Exception Report listing the specific legacy records along with the record number of those records from the incoming source/legacy file with the supporting business/validation rule that had failed. The State can leverage the Conversion Detailed Exception Report to decide whether to correct the data in the source system, make an exception for the legacy record, or provide a revised rule to successfully convert it into the target MT PSM solution.

No	Conversion Job	Execution Date/Time	Record Number	Record Identifier	Exception Code	Exception Description	Exception Target Elements	Exception Source Elements
1	Provider Location Indicator Job	04/25/2015 10:05 AM	112	PROVIDER_ID: 123456789 BEGIN_DATE: 01/01/1972 END_DATE: 12/31/9999	PE-917	Provider Indicator Discrepancy: The legacy in-state indicator value is missing.	Table: TBL_PRVDR_LCTN_INDICATOR Field: INDCTR_OPTION_VALUE	Table: Provider Field: IN_STATE_FLAG
2	Provider Location Indicator Job	04/25/2015 10:05 AM	2389	PROVIDER_ID: 987654321 BEGIN_DATE: 04/23/1979 END_DATE: 12/31/9999	PE-125	Provider Indicator Discrepancy: The legacy provider is not available in the target system.	Table: TBL_PRVDR_LCTN_INDICATOR Field: PRVDR_ID	Table: Provider Field: PROVIDER_ID
3	Provider Location Indicator Job	04/25/2015 10:06 AM	15897	PROVIDER_ID: 454545454 BEGIN_DATE: 10/23/29U6 END_DATE: 12/31/9999	PE-003	Provider Indicator Discrepancy: The legacy provider indicator for the provider has an invalid begin date.	Table: TBL_PRVDR_LCTN_INDICATOR Field: START_DATE	Table: Provider Field: BEGIN_DATE

Figure 3.10.2-38. Sample Illinois Provider Conversion Detailed Exception Report. Detailed exception report of the provider data that was converted for Illinois PE that shows some of the types of exceptions captured for source records that do not meet the validation or business rules.

Validation of Converted Data

As part of the Data Conversion process detailed in Figure 3.10.2-39, the Team CNSI data conversion team will provide detailed reports for each conversion run undertaken for MT PSM to the State team.

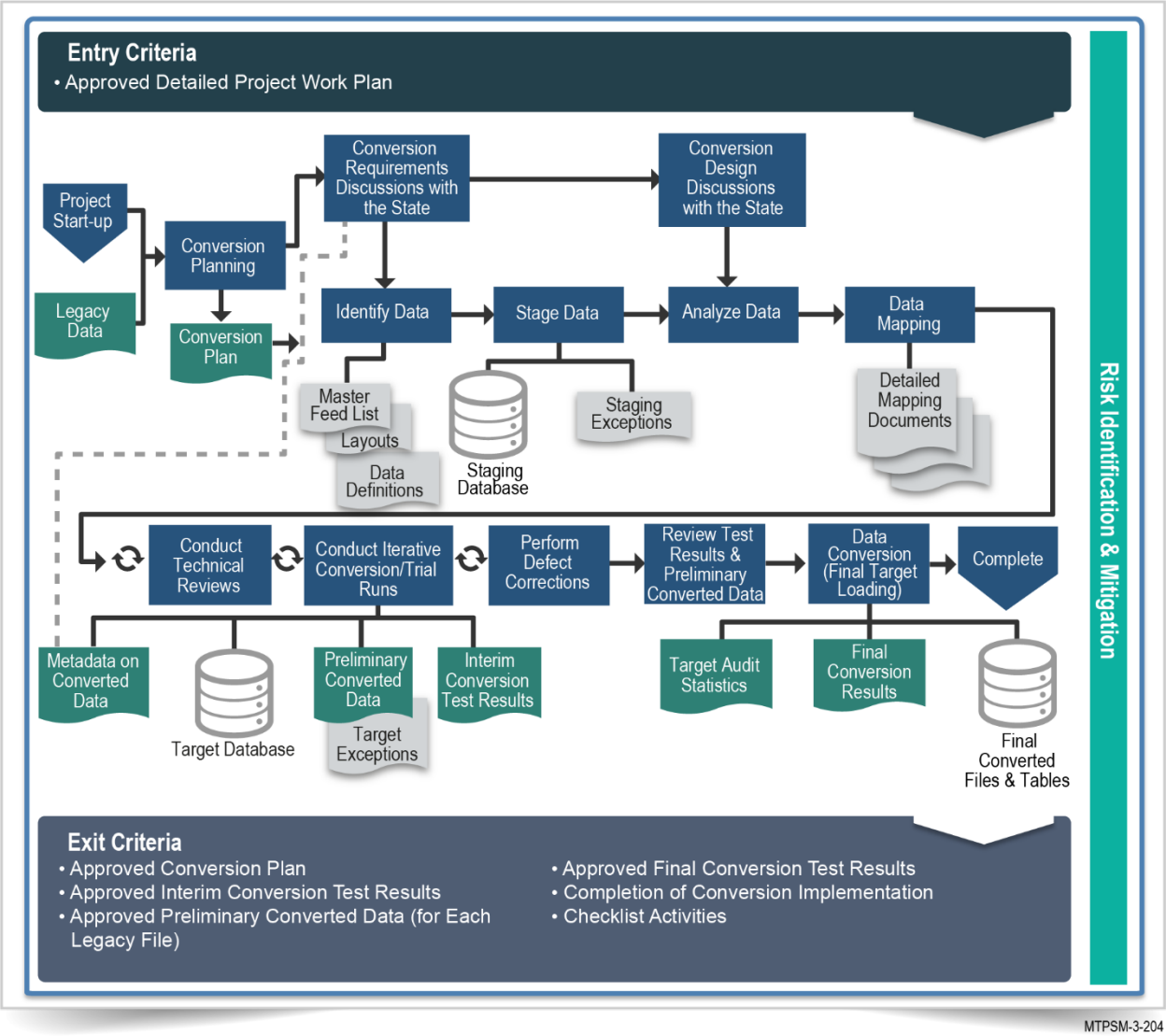


Figure 3.10.2-39. Detailed Data Conversion Process. Our solution provides a proven conversion process for the system.

The conversion team will assist DPHHS in cleansing the data in the source system using the guidelines provided below. Wherever it is not possible to cleanse the source data, Team CNSI will work with the State to develop the necessary business rules so that the data correction necessary to get it into the MT PSM solution could be accommodated as part of the conversion process.

- Staging Jobs: The team will generate a worksheet that provides details of the different source file layouts and how they correspond to the conversion staging tables. Also included is the pre-defined exception range that applies for each staging job to validate the source data for the respective job.
- Staging Jobs Exceptions List: The team will generate a worksheet that provides a comprehensive listing of the array of exception (or validation) codes, their descriptions, the associated target table/source file to which they apply, and an indication of whether the exception validation is record level or field level. The source data will first be validated against these staging jobs exceptions to pass the first-level validation before any data gets to the conversion/transformation jobs phase.
- Staging Exceptions Report: The team will generate a worksheet that provides a sample listing of the staging jobs and the associated exceptions raised during a job run. These exceptions and the

associated references to the source data records will be provided to the MT PSM team for further data analysis for the requisite corrective action, following which the source data will be re-sent for future clean loads.

- Transformation (XFRM) Jobs: The team will generate a worksheet that provides details of the different target tables and how the conversion/transformation jobs are applied to the equivalent staging tables.
- XFRM Jobs Exceptions List: No content is provided. Similar to the Staging Jobs Exception List worksheet, the team will generate a worksheet that provides a comprehensive listing of exception (or validation) codes, their descriptions, the associated target/source tables to which they apply, and an indication of whether the exception validation is record level or field level. The source data will then go through rigorous checks based on the requirements of the target data model and, more importantly, on the conversion mapping rules.
- XFRM Exceptions Report: The team will generate a worksheet that shows a sample target conversion/transformation job and the associated exceptions raised during a job run. These exceptions and the associated references to the source data records will be provided to the MT PSM Team for further data analysis for the requisite corrective action, following which the source data will be re-sent for future clean loads and conversions.

Detailed converted data validation will be done by the MT PSM Team, as applicable, independently using the following guidelines:

- Confirmation of no duplicates in the source data
- High-level record counts validation
- Confirmation of counts of unique instances of business key values
- Confirmation of no duplicates in the target data
- Field-level validation to confirm a possible range of valid values
- Field-level validation to confirm there are no NULL values for a mandatory target field or fields

Conversion Exception Handling

Exception handling will occur at all three stages of the conversion process:

- Conversion Load Stage: Data type mismatches and missing required fields will be reported by the conversion team as exceptions
- Conversion Transformation Stage: A wide variety of exceptions can occur due to referential integrity issues, invalid values, and other validations
- Index Rebuild Stage: Exceptions related to indexes and constraints will be reported by the conversion team as exceptions

The following information will be inserted into exception tables for each conversion job that is run:

- Job name
- Run date and time
- User identification (ID)
- Number of rows loaded
- Number of rows rejected
- Number of exceptions reported
- Source file name (load jobs only)
- Each job will be assigned a unique job ID in the exception tables

The following information will be inserted into exception tables for each exception flagged in a job:

- Job ID
- Exception date and time
- User ID
- Exception code (as defined in the data conversion exceptions list)
- Exception description (as defined in the data conversion exceptions list)
- Exception level (field, record, or job level)
- Exception details

Conversion Reconciliation

The conversion reconciliation ensures the converted data is not only valid, per the conversion business rules, but also functionally accurate as well. The conversion reconciliation will:

- Mitigate data migration risk by addressing data quality issues early on
- Minimize the number of conversion and/or data issues during iterative conversion runs
- Provide a detailed and accurate view of the data starting from the lowest level of granularity (column/table level)
- Mitigate post go-live data fixes that are complex to execute once the target system becomes operational (as providers/State would change the data)

The conversion reconciliation will look at converted data from multiple functional and business viewpoints to ensure accuracy of conversion. The conversion reconciliation will classify the results as:

- Successful: The conversion reconciliation matches the source data with the converted target data
- Failure: The conversion reconciliation was unable to match the source data with the converted target data
- Warning: The conversion reconciliation was unable to match the source data with the converted target data but is allowable as it satisfies the functional and business requirements

As an example, for the State of Illinois provider conversion, 90 individual reconciliation verifications were carried out for each conversion iteration. Figure 3.10.2-40 illustrates some of the reconciliations that were done in the provider subject area.

No	Query Group	Description	Count	Validation / Reconciliation
1	Provider	Illinois Provider Record validations	16	Successful
2	Provider Location Details	Illinois Provider locations and address validations	21	Successful
3	Provider Other Details	Illinois Provider Specialty Matrix, Licenses / Certifications, and Taxonomy Validations	14	Successful
4	Provider Identifiers and Indicators	Illinois Provider Identifiers and Indicators Validations	32	Successful
5	Provider steps	Illinois Provider Enrollment and Checklist steps validations	7	Successful

Figure 3.10.2-40. Sample Statistics for Illinois PE Conversion. Summary of the reconciliations carried out by provider sub module.

Figure 3.10.2-41 lists sample reconciliation queries across the provider sub modules. The reconciliation status is the outcome of the comparison between the source and target reconciliation/evaluation metrics. Team CNSI leverages an automated framework to orchestrate the end-to-end reconciliation process and, working with the State, strives toward a 99% accuracy in the overall converted data in the evoBrix PMIS solution.

No	Reconciliation Description	Source Reconciliation Criteria	Source Count	Target Reconciliation Criteria	Target Count	Reconciliation Status
1	Validating total Provider Application records converted from source to target.	Count of total records in Source Provider Table A.	<Number>	Perform join between Target Table X AND Target Table Y with Application ID and count of total records that are Active.	<Number>	Success / Failure
2	Validating total Provider records converted from source to target.	Count of total records in Source Provider Table A.	<Number>	Count total records in Target Table X that are Active.	<Number>	Success / Failure
3	Validating total Provider records converted from source to target with respect to enrollment type.	Count of total records in Source Provider Table A for each enrollment type.	<Number>	Count total records for each enrollment type in Target Table X that are Active.	<Number>	Success / Failure
4	Validating total Provider Individual/Sole records converted from source to target with respect to enrollment type.	Count of total records in Source Provider Table A with enrollment types to be validated.	<Number>	Count total records in Target Table X that are Active with enrollment types to be validated.	<Number>	Success / Failure
5	Validating total Provider Organization records converted from source to target with respect to enrollment type.	Count of total records in Source Provider Table A with enrollment types to be validated.	<Number>	Count total records in Target Table X that are Active with enrollment types to be validated, where the Target Table's Provider Organization Business Name has a mandatory value.	<Number>	Success / Failure

Figure 3.10.2-41. Sample Statistics for Illinois PE Conversion. Reconciliation examples carried out for provider conversion.

DC08

The Contractor shall convert electronic documents identified by the Department in a format approved by the Department.

Team CNSI's data conversion team will convert electronic documents identified for MT PSM as part of the conversion process as outlined below. The converted documents will be accessible through Team CNSI Enterprise Content Management (ECM) solution, managed through IBM FileNet P8.

- Define unique set of parameters for each document type for the documents to be converted.
- Leveraging the iterative data conversion approach, the documents will be converted as follows:
  - Load the legacy electronic documents in the conversion environment as a binary file.
  - Convert the equivalent document parameters to be able to uniquely access the document.
  - Move the converted document (binary) file to the FileNet staging database along with the converted document parameters and their values.
  - Leverage the data ingestion component provided by FileNet to upload the converted document (binary) files, parameters, and values onto the ECM repository for document storage which completes the conversion effort.
  - The converted document can then be accessed from the application. The evoBrix PMIS ECM solution supports the storage of a wide variety of document formats including but not limited to Word, PDF, Visio, Excel, PowerPoint, TIFF, and JPEG.

- Exceptions and reconciliation reports will be generated for each document and reviewed with the MT PSM ECM and State teams for any corrections to invalid documents for reprocessing.

Figure 3.10.2-42 outlines the document conversion process.

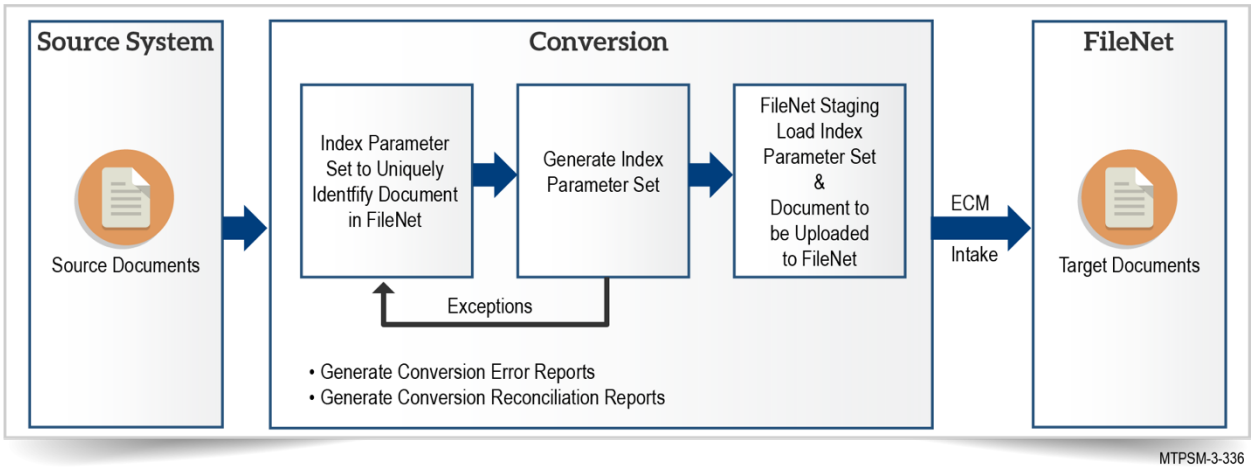


Figure 3.10.2-42. Document Conversion Process. Our solution ensures that all required source documents are converted and accounted for in Team CNSI ECM (FileNet) solution.

DC09

The Contractor shall provide convenient access to electronic documents from systems being replaced.

The evoBrix PMIS seamlessly integrates with the FileNet content management solution by IBM, which is Team CNSI's Enterprise Content Management (ECM) solution, to access electronic documents. The legacy converted files that represent document content are stored in the FileNet storage area and protected by the FileNet security model. Only authorized users who have been granted access to the content by a FileNet application administrator will have access to the electronic documents. Additionally, the unique set of parameters associated with a document, that are also converted and brought over to FileNet, will be utilized to access a document. This can be done through content-based retrieval (CBR) queries, direct SQL queries, navigation of the network file structure containing a file storage area.

Please refer to our response to Section 3.10.1.8, Enterprise Content Management, for more details about Team CNSI's Enterprise Content Management solution for access to electronic documents for MT PSM.

3.10.2.6 Testing

Testing is a critical component for successful implementation of any system configuration/development effort, therefore, in depth, process driven, fully documented testing processes are required for all implementations and configuration changes within the Montana Healthcare Programs enterprise. The testing activities shall include planning, managing and executing a comprehensive testing effort to include unit, system, regression, parallel, integration and UAT.

Prior to implementing a new release, the Contractor is responsible for ensuring that all required tests are performed and evidence that each component meets or exceeds all relevant functional, technical, security, and performance requirements is provided. The Offeror must describe their approach to meet each of the detailed testing requirements defined in Attachment F, Requirements Matrix.

Team CNSI's test program is designed to ensure a successful PSM implementation for the State of Montana. Team CNSI offers plans and procedures based on the same foundation we used for testing multiple successful provider implementations, including the states of Washington, Michigan, Illinois, and Utah. Our libraries of test cases provide a test suite structured to verify and validate that the Provider Services Module solution performs as expected for DPHHS.

The Team CNSI Advantage

Team CNSI offers mature test planning and proven test cases to support the MT PSM solution testing program.

- CMMI Level 3 assessed testing process
- IEEE 829 standard for software and system test documentation
- Multi-phased layered testing approach with a strong focus on testing as early and as often as possible
- Proven scalable and configurable testing foundation
- Dedicated and highly trained team of professionals with years of Medicaid and MMIS testing experience

MTPSM-3-416

Team CNSI offers a new paradigm for Medicaid Enterprises modular implementation. In contrast to the traditional legacy approach of design, development, and implementation (DDI), Team CNSI conducts the project using a solution, configuration, and implementation (SCI) approach. To execute the SCI approach, Team CNSI uses the PMIS solution module as the baseline. Team CNSI compares the needs of DPHHS with the existing PMIS module and performs a gap analysis between the two. In the Solution Modeling Stage, after gap analysis is conducted, Team CNSI works with DPHHS to identify and model solutions to close the gaps. During the Configuration Stage, Team CNSI performs configuration to tailor DPHHS solution needs and close the gaps. The configured solution undergoes rigorous system testing as the last activity in the Configuration Stage. In the Implementation Stage, Team CNSI engages the configured DPHHS solution in user acceptance testing (UAT). Following successful UAT, the transition phase concludes with the Implementation Stage where, following performance and load testing, the DPHHS solution is deployed.

Because of the SCI approach, the PMIS system is used as-is as much as possible and only minimal modifications are completed to meet the requirements of the State of Montana. The scope of testing during the Configuration Stage and the Implementation Stage is concentrated on new features, modified existing features, and regression testing of the fully configured MT PSM. Figure 3.10.2-43 shows the responsibilities for DPHHS and Team CNSI.

Role	Responsibility
Team CNSI	■ Develop and maintain test plans, automated test scripts, and test results per DPHHS requirements ■ Develop, document, and manage process for PMIS development unit tests, system testing, integration testing, interface Testing, UAT, parallel testing, regression testing, performance and load testing, and disaster recovery testing ■ Conduct and document results for all phases of testing except for UAT for the core PMIS which will be operated by DPHHS following deployment ■ Support and mentor the State team during User Acceptance Testing
DPHHS	■ Develop and document MT PSM UAT strategy and plan for areas DPHHS will operate following deployment ■ Execute UAT test cases and document results; document defects and test defect repairs ■ Review and approve Team CNSI's Test Plan and test results ■ Provide testing governance

Figure 3.10.2-43. DPHHS and CNSI Responsibilities. This figure summarizes what DPHHS and Team CNSI must do to ensure the MT PSM is successfully validated and verified.

Team CNSI's Test Strategy

Team CNSI offers a highly efficient, multi-layered, comprehensive test approach that minimizes risk to DPHHS. Through previous MMIS implementation experiences in Michigan, Washington, Illinois, and Utah, Team CNSI refined the test strategy we are offering for the MT PSM project. In this section, we

describe the testing approach that has led to these successful start-ups and deployments. Figure 3.10.2-44 summarizes our test process flow from end to end.

Figure 3.10.2-44. Test Process Overview. Team CNSI's testing process is well defined, uses proven tools, and is supported by experienced staff.

Team CNSI will return to the themes presented in Figure 3.10.2-44 throughout this section of our response.

The remaining sections of this overview describe Team CNSI's:

- **Test Planning Approach** describing Test Plan development, the layers of testing conducted, and a description of the purpose of each type of testing conducted
- **Test Layers** describing the components of the test program from the smallest testable units to full UAT
- **Test Execution Approach** describing the methods we apply to executing tests for all layers of testing
- **Test Case Construction and Traceability Approach** describing how test cases are reused from our other PMIS implementations
- **Test Automation Methods** including the tools used and how automation is applied to testing the MT PMIS
- **Defect Management Process** including the tools use, defect severity levels, and defect management life cycle
- **Test Management Monitoring and Control** describing the approach for tracking test progress
- **Test Scheduling and Acceptance** summarizing the test execution schedule and State acceptance

Test Planning Approach

The PSM Test Plan is tailored from the test plans used for our previous PMIS module deployments. Team CNSI will submit the Test Plan to DPHHS for review and approval. The test plan will document the processes, tools, and guidelines that will be followed to successfully complete implementation of the PSM for DPHHS.

Team CNSI's Test Plan provides our approach and methodology for all aspects of testing. This includes:

- Iteration/unit testing
- System testing
- Regression testing
- UAT including coordination with the State's UAT
- Performance and Load testing
- Security testing
- Pre-deployment smoke testing
- Post-Operations system changes testing

Through our other successful Medicaid project deployments, Team CNSI has found that having a single plan that addresses the standardized policies, tools, and processes provides consistency and predictability and ensures compatibility with the other systems in the State's MMIS. Figure 3.10.2-45 shows a sample Table of Contents for Team CNSI's PSM Test Plan.

Table of Contents

Preface **5**
Document Purpose 5
Document Scope 5
Audience 5
Referenced Documents 6
Section 1 – Overview **7**
1.1 Project Overview 7
1.2 Scope of Test Activities 7
1.3 Test Objectives 8
1.4 Assumptions and Constraints 8
1.5 Risks 8
Section 2 – Test Approach **9**
2.1 Roles and Responsibilities 9
2.2 Mandatory Peer Review Process 10
2.3 Gap Traceability Matrix Management 10
2.4 Test Planning 11
2.4.1 Test Environments 12
2.4.2 Iteration Test Planning 12
2.4.3 System and Regression Test Planning 13
2.4.4 User Acceptance Test Planning 14
2.4.5 Performance and Load Test Planning 15
2.5 Test Case Tailoring Process 16
2.5.1 Test Case Construction for State-specific Use Cases 17
2.6 Test Tools 19
2.7 Test Automation 19
2.8 Test Data Preparation 20
Section 3 – Test Case Foundation Inventories **21**
3.1 System Test Cases 21
3.2 End-to-End Test Cases 22
3.3 Regression Test Cases 22
3.4 User Acceptance Test Cases 23
3.5 Performance and Load Test Cases 23
Section 4 Test Management **24**
4.1 Test Management Overview 24
4.2 Test Readiness Reviews 25
4.3 Defect Management 26
4.4 Test Results Reporting 27
Section 5 – Test Schedule **28**
Appendix A – Test Case Inventories **29**
A.1 evoBrix System Test Case Base Inventory 29
A.2 State-specific System Test Cases 33
A.3 End-to-End Test Cases 36
A.4 User Acceptance Test Cases 37
A.5 Supplementary State-specific User Acceptance Test Cases 38
A.6 Performance and Load Test Cases 39
Appendix B – Test Entry Checklists **40**
Appendix C – Test Exit Checklists **44**
Appendix D – Using Jira to Record Defects **48**
Glossary **50**
Acronyms **51**

MTPSM-3-413

Figure 3.10.2-45. Sample Test Plan Table of Contents. The PSM solution is supported by a proven test approach and strategy for testing that Team CNSI tailors to DPHHS's needs.

As shown in Figure 3.10.2-45, our test plan includes testing objectives, definitions of testing phases, and overall testing strategy. It also includes a description of standardized tools, as well as common methods of testing functional and non-functional gaps, in each layer of testing as described in the next section of this overview. As a part of project planning activities, Team CNSI will ensure that our test plan is in conformance with the State's testing requirements.

The Test Plan defines test schedule, timeline for creating test environments used for each layer of testing as well as the processes the Team CNSI and DPHHS test teams will use in test data creation and for test execution. It also identifies the sequence of testing activities and their interdependencies. Our Test Plan and processes conform to the IEEE 829 Standard for Software and System Test Documentation. This standard describes a set of basic test documents that are associated with the dynamic aspects of software testing. Team CNSI's Test Plan will be tailored to the specific needs of the MT PSM solution. Tailoring involves modifying generic elements, such as specific test schedule dates and personnel assigned to roles in the plan. Samples of the testing progress, defect tracking, and analysis of results and trends are provided in the approved Test Plan.

Per the Test Plan and the approved project schedule, Team CNSI tracks progress through test execution, measuring progress of execution against the project schedule, tracking test cases that pass and fail, and tracking defects and their resolution. Team CNSI has a standardized test reporting process that is practiced on all projects, which includes progress/velocity and defect trend analysis to identify and assess risk. This data set is provided to DPHHS at mutually agreed-upon intervals which are recorded in the approved Test Plan. Furthermore, Team CNSI will also record mutually agreed-upon criteria in the

approved Test Plan based on which testing can be exited. Meeting the criteria signals the exiting test step has been met, thus signaling readiness to exit the test.

Test Layers

Team CNSI's PSM design documentation is the source for our functional test program. Team CNSI plans and executes testing through a layered approach. Team CNSI's Test Plan outlines the activities for each of the testing stages. Figure 3.10.2-46 shows our testing approach as a visual hierarchy building from the bottom to the top.

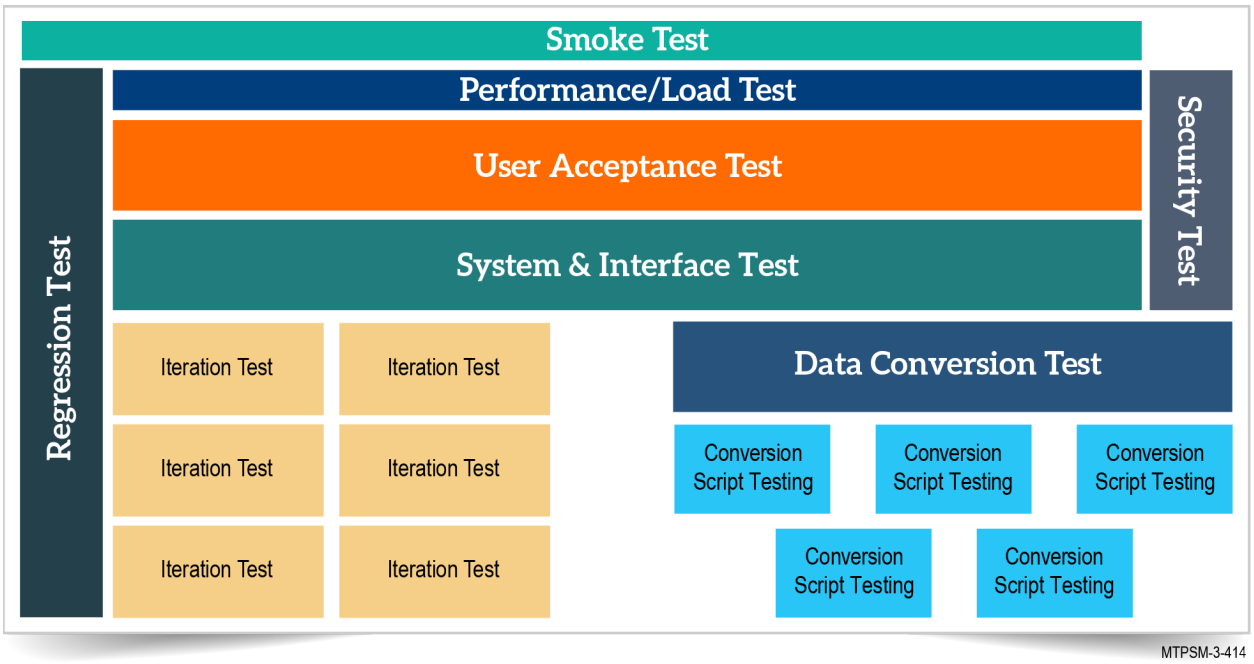


Figure 3.10.2-46. Team CNSI's Test Hierarchy. Team CNSI's layered testing approach builds from the smallest testable units to full system and user acceptance testing.

Team CNSI uses similar processes for each layer of testing. This consistent approach allows DPHHS to become familiar with our test processes and artifacts and prepares the participants for a similar approach to conducting UAT.

The Test Layers include:

- Iteration tests, also called unit/iteration tests: These are the smallest testable units of code and are tested using low-level scripts. Iteration/unit testing is conducted by Team CNSI's software engineering team.
- Conversion script testing: This is analogous to iteration/unit tests. It is used to test specific data conversion elements and rules. This testing is done by Team CNSI's data conversion team.
- Data conversion test: When sufficient progress has been made to reliably convert data and any necessary data cleansing has occurred, the data conversion process is executed to produce converted data for use in system testing.
- System and interface testing: When the features specifically configured for the MT PSM have completed iteration/unit test, and we have converted legacy data, we perform system testing with a concentration on the State-specific features including interfaces. The later phases of system testing are referred to as end-to-end (E2E) testing where a process, such as enrolling a provider, is executed from the beginning of the enrollment process all the way through application approval or denial.

- Regression testing: Regression testing is performed after every code release to ensure new features have not affected unchanged functionality.
- UAT: UAT is performed on the completely configured MT PSM using converted data. End-users who will operate the system post-deployment perform UAT.
- Performance and load testing: Performance and load testing verifies that non-functional requirements such as throughput service levels and concurrent usage requirement are met.
- Security testing: Security testing focuses on confirming all security features are functioning as expected and the State's responsibilities for maintaining secure control of personally identifiable information (PII) and protected health information (PHI) are met.
- Smoke test: Smoke testing is a final check performed to ensure that all features and functions are operating normally after a production deployment, or a deployment to UAT.

Throughout our responses to the State's requirements, we refer to these testing layers. We have also described them in more detail in our response to requirement TEST02.

Test Execution Approach

Figure 3.10.2-47 provides a visual showing the consistency of Team CNSI's approach across all testing activities from iteration tests through UAT. The horizontal right arrows in Figure 3.10.2-47 demonstrate how testing builds through each phase and benefits from re-using evoBrix PMIS module base test cases for MT PSM test case construction and regression testing in each phase. The horizontal left arrows in Figure 3.10.2-47 indicate how regression testing is completed.

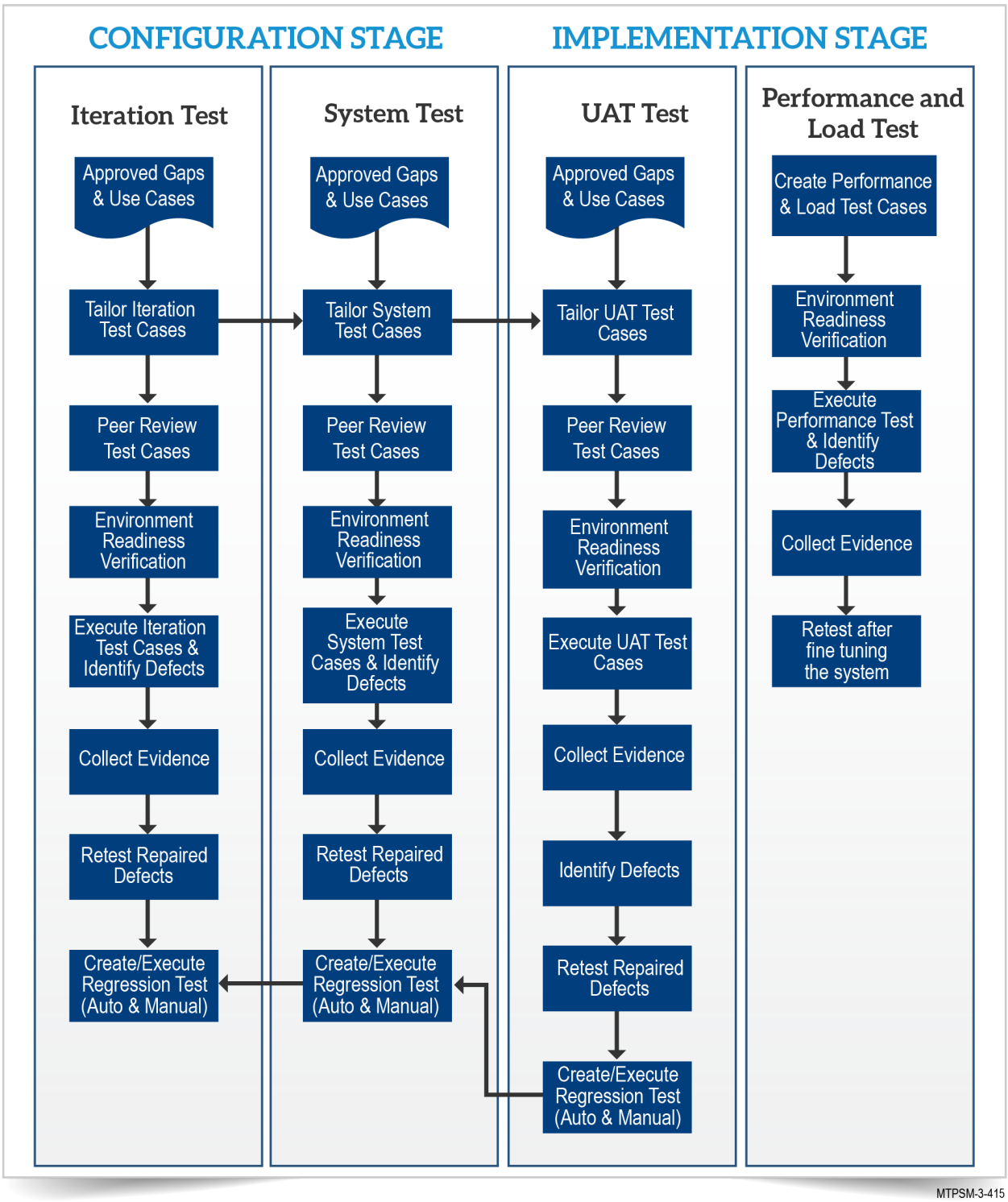


Figure 3.10.2-47. Foundations of the MT PSM Test Program. Team CNSI's System test program is composed of multiple layers of testing and structured test activities to ensure validation of the product and its capabilities before deployment.

As shown in Figure 3.10.2-47,Team CNSI follows a structured test process across all layers of testing. The steps and their benefits to the State are summarized in Figure 3.10.2-48.

Test Step and Description	Description	Benefits
Tailor Test Cases	Team CNSI reuses the base evoBrix PMIS module test cases and modifies them, where necessary, to test State-specific gaps.	■ Base test cases are being used to test production work in other state installations ■ Reused test cases are tailored to the State's gaps minimizing test case preparation ■ The effort necessary to create new test cases is minimized
Peer Review Test Cases	Team CNSI peer reviews any modified or newly developed test cases.	■ Peer reviews verify that the test case conforms to the approved DSDD ■ Peer reviews include Team CNSI test engineers, business analysts, developers promoting thorough review of the test case ■ Peer reviews offer the opportunity to correct errors in understanding that might otherwise lead to erroneous defect reporting
Environment Readiness Verification	Team CNSI confirms that the test environment is correctly configured and has all necessary resources to support test activity	■ This check, called a Test Readiness Review (TRR), ensures that testing activity is not derailed due to preventable errors in the test environment
Execute Test Cases and Identify Defects	Team CNSI executes each step of the test case recording any variance from the expected result	■ Our systematic method of test execution and documentation has been proven through our other PMIS implementation ■ Test results documentation provides the necessary pass or fail proof points and captures the critical information required to record a defect accurately ■ Test results are recorded and stored in the SharePoint documentation repository for review by Team CNSI and State team members ■ Defects are captured in Jira and are available for review by Team CNSI and State team members
Collect Evidence	Team CNSI builds test results over multiple weeks of test execution and provides monitoring and reporting of pass/fail rates, defects, and defect correction activity	■ Team CNSI's process provides transparency throughout the test process and feeds honest and accurate test progress reporting ■ The State is kept informed throughout the process because we provide test results evidence through aggregate status reporting as well as detailed test results reports
Retest Repaired Defects	Team CNSI's software engineers review reported defects, conduct analysis, correct the code where necessary and conduct unit/iteration testing to verify the defect is corrected. The corrected code is released ad retested to the environment where it was reported	■ Jira monitors the progress of defect correction from initial reporting through closure further supporting transparency throughout testing ■ Following the test process to where it was originally reported allows the tester to confirm that the defect is no longer appearing
Create/Execute Regression Test Automated and Manual	Team CNSI conducts full regression testing at the end of each test phase to ensure no defects have been inadvertently introduced through the configuration of defect correction processes	■ Regression testing uses a set of test cases and test data that has performed reliably in Team CNSI's production PMIS installations providing assurance that the system is stable and free of defects that would prevent moving to the next phase of testing

Figure 3.10.2-48. The Repeatable Steps of Team CNSI's Test Process. This figure shows an expanded view of the activities listed in Figure 3.10.2-47 including descriptions of the steps and benefits of our approach.

Throughout the test phases, Team CNSI's testers summarize and review the test results and compare them to the expected results per the approved solution. We involve our software engineers who are responsible for configuring the system for DPHHS. We also involve both State and Team CNSI business analysts. This ensures clear communications and understanding across all stakeholders involved in testing.

Test Case Construction and Traceability Approach

CNSI is privileged to have a core team of professional testers who have years of Medicaid testing experience and who are well-versed in the design and execution of testing activities. CNSI's Test Team operates independently of the development team and creates or tailors all test cases for the MT PSM solution testing. For the MT PSM solution, most of the test cases are preexisting. Iteration test cases are created during the configuration phase to conduct iteration testing. Upon successful completion of iteration testing, we progress to System test, where we re-utilize and combine Iteration test cases to create and adjust System test cases and E2E test cases. The key benefits to this approach include:

- Key traceability information to system level test cases, critical to identifying regression test sets
- Consistency in test execution from one test phase to another
- Reduction in time to create or adjust and review system test cases

Team CNSI also uses its libraries of E2E test cases that represent the day-to-day business scenarios of other healthcare agencies. While each state is unique in its implementation, these test cases represent those processes using the base PMIS solution. These tests may be re-used and modified to meet the needs of the DPHHS.

Team CNSI also incorporates system test-level test scenarios from DPHHS' legacy Provider system where applicable. Team CNSI can build updated versions of these tests using the project's standardized templates. This provides confidence that the newly configured MT PSM solution continues to meet the existing needs and functionality of the current system as these tests may identify flaws with the re-engineered business processes.

Team CNSI's experience with system testing has shown test case generation is best completed with our client to generate test scenarios that represent the real-life situations experienced with the actual work done by the users themselves. By engaging our clients in this process at the system level, we also prepare them for the upcoming UAT phase where they may re-utilize the system tests.

Team CNSI helps DPHHS to create UAT test cases by letting them leverage system test cases and E2E test cases. Team CNSI also works with DPHHS to ensure any unique scenarios not already covered are included. Team CNSI will help DPHHS testers in executing these tests in the UAT environment to validate the system.

For all types of testing, CNSI will ensure that all test cases:

- Are version-controlled
- Use the standardized test case form
- Use standard naming conventions to distinguish test cases by phase and subsystem
- Are tester-independent so that any tester can read and execute the test case
- Show the test objectives
- Provide traceability to the underlying use case and gap
- Address the required validation points to be used in the test
- Define the expected results of the test and the actual result of the test after it has been executed so that the two results may be compared easily
- Are searchable using electronic methods in event that an approved gap is changed enabling all related test cases to be quickly and easily identified for regression testing or modification
- Are data-independent where possible and make use of de-identified converted data

Test Automation Methods

Team CNSI will use Selenium to automate MT PSM browser interactions. Team CNSI plans to leverage the suite of PMIS automated test scripts that were developed for the previous State implementations. Team CNNSI will execute the suite of PMIS automated scripts regularly where and when applicable. The frequency of test execution renders immediate results, thereby identifying and addressing defects early. Using the available automated test scripts available and executing them regularly allows Team CNSI testers to focus on more complex testing scenarios that cannot be automated.

A continuous effort and focus on maintaining the suite of automated tests allows Team CNSI to measure quality at a faster pace. Automated scripts are carefully maintained and updated to ensure all DPHHS requirements are met.

Defect Management Process

All defects opened in Jira are assigned a defect severity level. The defect severity levels are defined in Figure 3.10.2-49. Defect resolution Service Level Agreements (SLAs) will comply with the response time described in the RFP.

Defect Severity	Defect Severity Description
Severity 1: Very High	Results in a complete System outage with no workaround. Action results in a system crash or in damage to data, such as wrong results or a loss of data.
Severity 2: High	System functionality is degraded with severe adverse impact to the user and there is no effective workaround.
Severity 3: Medium	System functionality is degraded with a moderate adverse impact to the user but there is an effective workaround.
Severity 4: Low	The actual results have a user inconvenience or other minor inconvenience, such as typographical errors, or alignment errors, or extra steps are needed to complete function. These include all other discrepancies, spelling errors, or minor/trivial errors.
Severity 5: Documentation	All documentation defects that do not require system changes because of the documentation update.

Figure 3.10.2-49. Defect Severity Definition. Team CNSI will assign every defect with the defect severity level based on these definitions

Team CNSI's development staff will review, assign, and open defects for resolution, as part of the defect management life cycle shown in Figure 3.10.2-50.

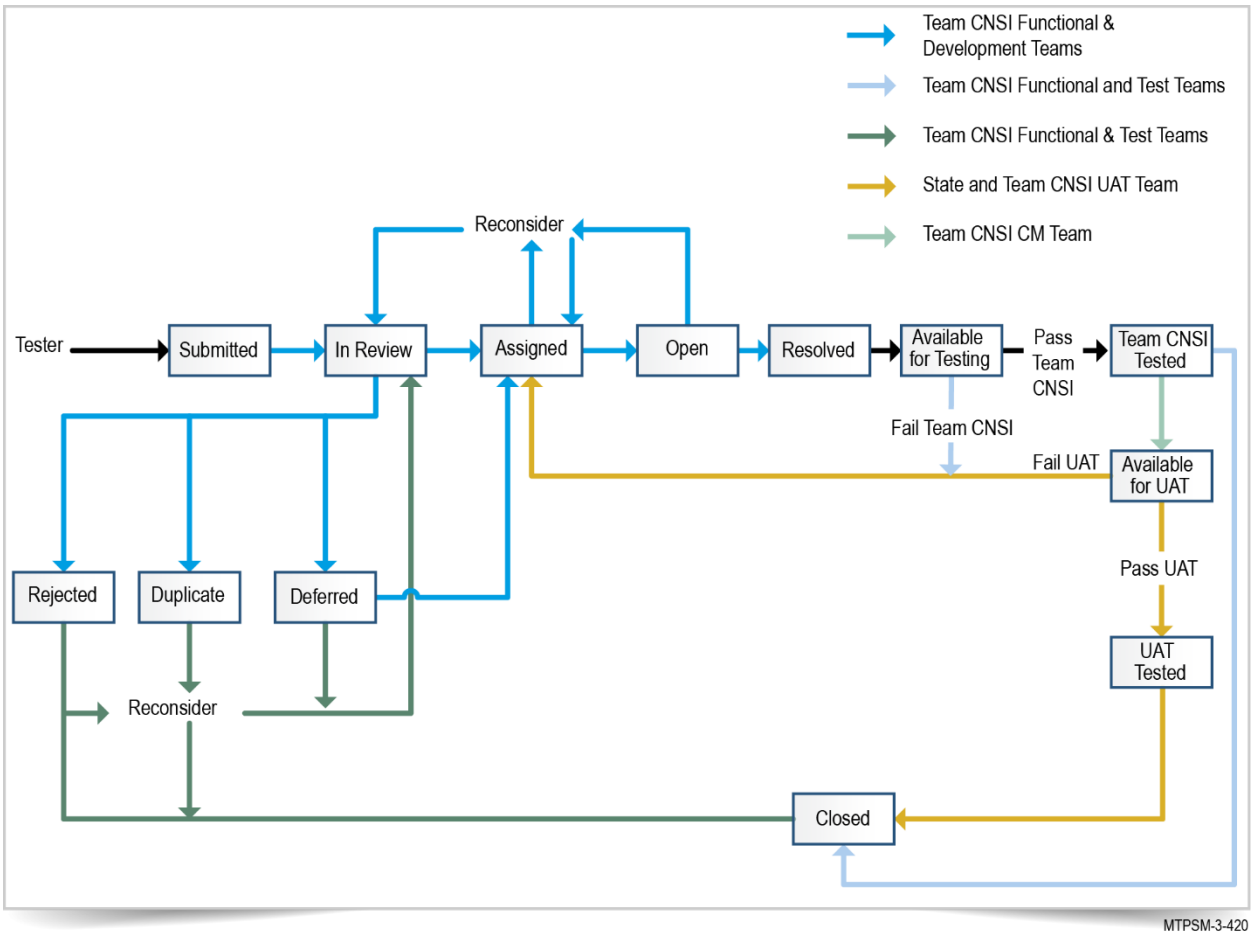


Figure 3.10.2-50. Defect Management Lifecycle. Atlassian's Jira provides defect reporting and management infrastructure.

After completing defect resolution using our standard practices, the Team CNSI Configuration Management (CM) team will deliver the "changed" software to the system test environment for verification. Team CNSI's Test team will verify that each defect has been properly resolved, and perform system and regression testing to ensure that the defect repair has had no adverse impact on the software. After Team CNSI is satisfied that the defect has been repaired successfully, the CM team will deliver the repaired code to the UAT environment. The CM team will include a report with each software delivery to the UAT environment that indicates what defects have been resolved and are ready for the UAT testers to retest and close. The procedures and guidelines concerning the use of Jira are included in the Test Plan.

Test Management Monitoring and Control

Project management processes are critical in establishing the controls necessary to maintain the expected performance levels of testing and identify corrective actions as needed. Team CNSI continually monitors progress of test case execution. Team CNSI management reviews test execution and defect rates to identify bottlenecks and possible complexities that require greater management visibility and attention. Team CNSI provides robust reports throughout each test phase providing detailed information such as test case execution and pass rates, defects open/closure rates, defect aging, and other key metrics for meaningful test progress tracking.

Team CNSI provides DPHHS with adequate test status to help them monitor the overall Testing progress as well as the quality of testing.

Test Execution Scheduling and Acceptance

Team CNSI executes the test strategy detailed above based on the dates identified in the project schedule. In parallel to Configuration, Iteration testing will be conducted followed by System testing, and then UAT. During the last stage of UAT, performance and load testing will be conducted to validate the MT PSM solution's performance against the RFP requirements.

Team CNSI's dedicated team of experienced PMIS testing professionals performs the proven, previously described, testing strategy as per the dates identified in the project schedule to ensure the MT PSM solution is successfully integrated and fully accepted by DPHHS.

TEST02

At a minimum, the Contractor shall provide sufficient segregated environments to support testing processes that are equivalent to the following:

a. Integration Testing: End-to-end testing performed to expose defects in the interfaces and in the interactions between integrated module components or other systems and validate the system's readiness to meet non-functional requirements.

b. System testing: The process of demonstrating that a program, function, or integrated system components meets its requirements and objectives as stated in the requirements specification.

c. Regression Testing: Testing of a previously tested function following modification to ensure that defects have not been introduced or uncovered, as a result of the changes made. It is performed each time the software or its environment is changed, and typically involves automated testing scripts.

d. Parallel Testing: Validates that the system achieves the same results as compared to another system (e.g., a legacy system) or previous software version.

e. Performance and Load Testing: Verifies the performance of a system will meet service level agreements and also measures the behavior of the system with increasing load (e.g. number of parallel users and/or numbers of transactions to determine what load can be handled by the system).

f. User Acceptance Test: Testing conducted by the user or customer to determine whether or not a system satisfies the defined use acceptance criteria in an isolated environment.

Team CNSI has successfully implemented provider systems for Michigan, Washington, Illinois, and Utah. This has provided Team CNSI rich experience in knowing what exactly it takes to perform effect testing of the system. Team CNSI will leverage this knowledge to ensure DPHHS requirements are met and the Montana solution is thoroughly tested.

After preparing an environment for testing, Team CNSI's development and test team members perform a readiness review to ensure the environment has been properly configured, code is properly deployed, and converted data set is properly loaded. Examples of items appearing on the Environment Readiness Checklist include the following:

- Is the latest code deployed into the environment?
- Is converted data available or data conforming to final specification created by testing teams available minimally for System testing? (Partial or preliminary converted data may be provided as early as Iteration testing.)
- Is interface connectivity verified?

- Can the hardware and software be accessed as defined by the roles and responsibilities of each team member?
- Is data synchronized between separate interfaced systems and verified for each interface?
- Is the batch scheduler configured as agreed per the test plan or training plan?
- Is security configured and validated with user IDs and roles as specified in the Test Plan?

The activities performed in these environments are described in detail in the following sections.

Team CNSI provides segregated test environments for:

- Iteration/unit testing which precedes system testing
- System and integration testing, including interface testing
- Regression test
- UAT
- Performance and load test
- Security test
- Parallel testing
- Post-deployment system change testing

The following sections outline some of the key characteristics of each environment and the activities performed in it.

Iteration/Unit Test

The iteration/unit test is designed to test business areas or stand-alone components, without dependency on any other business area, to demonstrate that they meet the approved documented solution. When an individual business area has dependency on data from another business area, Team CNSI's test team will create the data needed to perform the test. When external interfaces are involved, those interfaces will be tested using mocked up data. Full interface testing is completed later, during system testing and E2E testing.

Each test case is defined with input data, step-by-step testing procedures, and expected results. Each test case contains traceability to use cases and gaps based on the approved MT PSM solution Detailed System Design Document (DSDD). Successful completion of the Test Readiness Review at the end of the Iteration test phase allows the project to move to the System test phase.

System and Integration Test

System test concentrates on testing business processes using converted data. Team CNSI focuses on testing all system functions within scope for their completeness and accuracy. We tailor MT PSM solution test cases to meet specific system test case needs, using the common test creation process for individual iteration tests and leveraging the test cases previously created. System test cases are a combination of individual use case test cases and integration test cases as well as E2E test cases. E2E tests combine individual use case tests into a complete business goal flow. For example, filling a provider application, then reviewing the application for completeness, validating the application for data accuracy, followed by screening the applicant, and then approving or rejecting the application accordingly. E2E test cases build the use cases into a single stream leading to the business objectives of each function or process.

Ensuring that each use case and any related interfaces are present in one or more System test cases provides a way to ensure effective test coverage in an efficient manner. Utilizing actual data during System test supports our actual Scenarios and verifies the accessibility and functionality of converted data.

Creating DPHHS-specific system test cases for every possible permutation of functionality is neither realistic nor valid from the business perspective of operating the MT PSM solution. Team CNSI's test approach ensures that each DPHHS gap is tested, including interfaces, and that all standard PMIS solution functions continue to operate as expected. DPHHS and Team CNSI SMEs will participate in reviewing the test plans and test cases to ensure the State's business objectives are completely satisfied.

During System Testing, Team CNSI testers will conduct tests to:

- Verify that all DPHHS business policies are exercised. This encompasses testing use case alternate flows dependent on the State's business rules, error conditions, informational messages, and error messages.
- Confirm that the design documentation provided to DPHHS corresponds to the system's behavior.
- Verify that the online help and training materials match the developed system.
- Verify all reports and correspondences are tested, including formatting, data validation, generation (both batch and on demand), and printing.

Interface Testing

Interface testing is a critical element of System testing. The goal of Interface testing is to verify a successful transfer of data to entities external to the MT PSM solution and verify that the data are properly interpreted by the receiving system. Team CNSI understands the complexities of Interface testing. We work collaboratively with DPHHS to engage the external partner agencies and establish an approach for completing Interface testing prior to the start of System testing. Some of the key considerations for the interface test plan include:

- Identify key parties to complete the test activities for external interfaces
- Determine the availability of both human and computing resources for System Testing
- Identify the sequence of testing to be completed
- Coordinate common data that may be required to successfully complete the test
- Verify network connectivity has been established prior to conducting any test activities
- Test each interface completely, exercising all message protocols and responses, and capturing evidence of testing to include the files and messages used in testing, the operational reports, and the error messages and measures
- Test each interface to verify the data generation (outbound), transmission, and processing (inbound) can be completed per the design of the PMIS as configured for MT PSM solution

Figure 3.10.2-51 shows the common elements in each interface. During Interface testing, Team CNSI tests these common elements to ensure that they perform as expected.

Common Element	Description
Event Trigger Handling	Events to trigger interface processes (i.e., When an event occurs, the trigger for the interface is tripped, and a response is initiated)
Validating	Routines to validate the interface data and protocol structure and to ensure that they meet expected content and structure
Logging	Routines to record critical events and activities for the interface
Reporting	Routines to collect statistical information for reporting (e.g., number of times an interface is used, total number of errors, total amount of data transmitted)
Process Management	Routines to start and stop external programs that are used as part of the interface specification (e.g., secure File Transfer Protocol (FTP))

Common Element	Description
Error Handling	Routines to handle error conditions (e.g., logging the error condition and repeating a request for information when a timeout occurs)
Status Monitoring	Routines to continuously monitor the status of an interface connection

Figure 3.10.2-51. Common Elements of Interface Testing. These common elements have become part of Team CNSI's repeatable standard interface testing process.

Interface testing is considered complete when Team CNSI has executed all the interface test cases during system test and has validated the following with the external interface owners:

- An outbound interface was exercised as far as the successful transmission of data, form, and content to the external interface owner
- An inbound interface was exercised as far as the successful receipt and processing of data transmitted by the external interface owner

Regression Test

Team CNSI executes a regression test suite to validate the integrity of the MT PSM solution through the iteration, system, and user acceptance testing processes. The validation suite will identify, through manual and automated regression tests, any core functionality that is behaving differently than expected. Team CNSI will adjust its automation suite during the Iteration and System test phases to accommodate the DPHHS-specific use cases. By performing the regression testing at a regular interval, Team CNSI can identify changes to pre-existing functionality that may be an unintentional result of configuration changes.

After identifying the regression test scope, the test team selects a set of pre-existing iteration and system test cases created during earlier test phases. Criteria for selecting test cases are:

- The test case is representative of the core functionality of the subsystem being configured
- The test case specifically targets the areas within the subsystem that have been configured
- The test case specifically targets integration points of other subsystems that may be affected by the changes

Team CNSI will conduct a full regression test (automated and manual) prior to the end of each major set of testing objectives to ensure continued stability as testing proceeds through the layers.

User Acceptance Test

The purpose of User Acceptance Testing (UAT) is to confirm that the system is performing per DPHHS-approved design documentation and is accepted by DPHHS. The design documents include all applicable MT PSM solution functionality and approved changes for DPHHS.

Team CNSI provides inputs to the State to develops a comprehensive UAT plan to fully test all the operational elements of the MT PSM solution in the context of the related business operating procedures. During UAT planning, Team CNSI will work with DPHHS to identify UAT scenarios that will test MT PSM solution functionality logically and comprehensively. Refer to "Entry and Exit Criteria" in this section of our response for a complete discussion of conditions that must be met prior to starting UAT.

Operational procedures are developed for the MT PSM environment during the configuration phase of Implementation. Team CNSI works in close collaboration with DPHHS, and the Team CNSI operations

team to confirm that the UAT plan meets the State's needs and goals and conforms to industrial testing standards.

UAT is designed to ensure that all MT PSM solution functions are tested by personnel who have responsibility for using and executing the MT PSM solution following deployment. All UAT activities are designed to be performed within the security roles defined for the specific function. UAT test cases are constructed to fully exercise the business functions that will be performed following deployment, and testing is conducted in a production-like, controlled, and stable environment using converted data.

Team CNSI's UAT methodology examines the readiness of the system for full acceptance by DPHHS based on actual performance.

For the MT PSM, UAT will be conducted by the SMEs who will operate the solution following deployment. DPHHS will be responsible for UAT for the primary PMIS operations of provider enrollment, provider enrollment maintenance, and provider administration as well as management of the role-based security administration for provider accounts. Team CNSI will be responsible for UAT for Option B – the customer relationship management and SiteVisitPro modules. Team CNSI will work with DPHHS and its System Integration Contractor to confirm that UAT is comprehensive and includes all necessary activities to prove the MT PSM is ready for production.

Successful test results and defects are documented by the UAT testers who carry out the tests, the State SMEs who validate the results, and the end-users running business operations. Team CNSI functional and testing team members provide support for the UAT testers and perform evaluation of test throughput, pass/fail rates and defect correction activity. Throughout UAT we will assist individual users with using the MT PSM solution, identifying problems, and conducting root cause analysis to facilitate corrections needed. As defects are identified during UAT, Team CNSI will use our standard test defect management process and the Jira application to capture the defects. Team CNSI will train DPHHS users in the defect management process and use of Jira.

Performance and Load Tests

The final layer of testing is the Performance and Load test. This layer of testing is covered in Team CNSI's Test Plan as previously noted in Figure 3.10.2-45. Performance and load tests are executed in parallel with UAT in a dedicated environment to ensure that the required performance characteristics of the MT PSM solution have been met. The Test Plan outlines all test activities and processes necessary to complete these tests.

Performance and Load requirements are commonly classified as non-functional requirements and differ greatly from the functional gaps being tested in the System test and UAT. Testing non-functional requirements uses different test tools, techniques, and verification methods than those used for testing of functional requirements. Performance and Load tests provide the computing environment necessary for performance tuning. Team CNSI uses this test layer to establish baseline sizing and benchmarks for use in planning for future growth requirements.

Performance Test: For each test, Team CNSI works with DPHHS in the planning and construction of the test cases that are used to verify performance and load requirements are met. Team CNSI maintains responsibility for performance testing and may request information from DPHHS to ensure that the test cases represent the most realistic view of legacy system operations that is possible. We recognize that some information may not be readily available from DPHHS or its legacy MMIS provider due to the limited availability of system profiling tools. In such cases, Team CNSI works collaboratively with DPHHS to make a reasonable approximation based on data that is available.

Performance tests are designed to verify requirements that specify the need for the system to complete user-initiated operations and return control to the user within a specified period. This measurement is commonly referred to as response time and is a part of the SLAs provided by DPHHS.

All response times are based on the normal system user load distribution encountered during normal business hours. To design the test to simulate production system usage, additional parameters are obtained through a combination of collaborative design sessions with DPHHS and capturing additional production profile data from the legacy MMIS, when available. Some of this additional data include:

- Selecting screens and transactions to be used in the test
- Mixing operations between Record Search, Screen Edit, and Next Screen actions
- Randomizing lookup criteria to ensure realistic performance scenarios
- Providing think times between user actions

Team CNSI works with the State to design and construct a user profile to verify that performance requirements are met. Figure 3.10.2-52 represents sample user profiles that could be used for the design and development of Performance test cases.

Business Area	Number of Concurrent Users Using the Business Area	Number of Users Performing Inquiries	Number of Users Updating
Provider Management	288	54	234

Figure 3.10.2-52. Sample User Profile for Performance Testing. Team CNSI will work with the State to construct a user profile to verify that performance requirements are met.

After determining the user profile, Team CNSI selects the appropriate test cases and use cases to develop automation scripts and data pools to generate the response time tests.

Figure 3.10.2-53 shows an overview of the Performance and Load testing process.

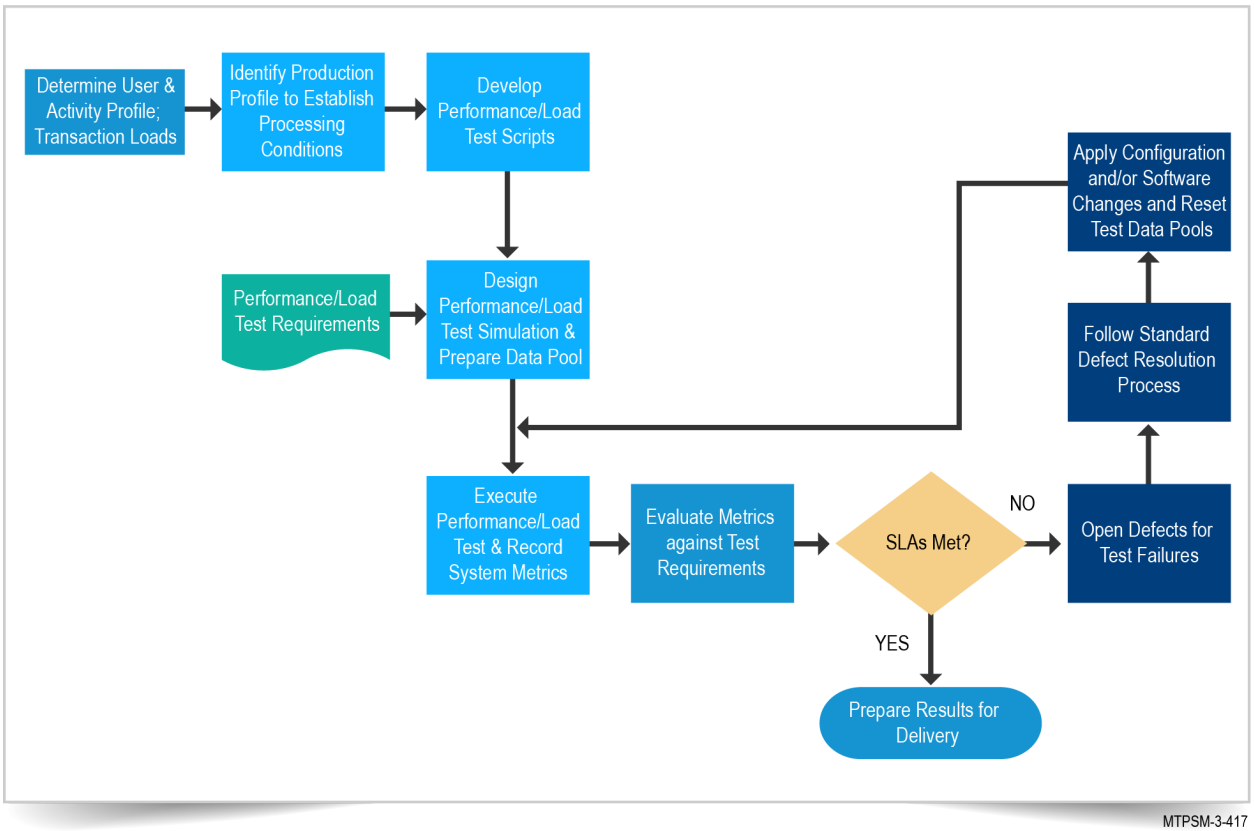


Figure 3.10.2-53. Performance and Load Test Process. Team CNSI ensures that the MT PSM solution responds to meet or exceed required MT PSM performance requirements.

Load Tests: Load tests are constructed to verify that the MT PSM solution meets the requirement to process volumes of enrollments over a specified period.

To construct Load tests that simulate production system usage, parameters for executing the tests require identification using a combination of collaborative design sessions with DPHHS and capturing additional production profile data from the legacy MMIS, where available. Ideally, some parameters may be used for more than one test. Some examples of parameters might include:

- Duration
- Daily hours of operation for provider enrollment and call center
- Daily hours of operation for user-driven provider application processing
- Competing processes during provider application processing
- Average number of provider calls per day
- Average daily peak (e.g., Are Mondays statistically heavier?)

Additional load parameters, such as the number and type of competing system processes, are established during the constructions of these tests. An example of a competing system process might be the processing of nightly batch license file or similar activities which are executed at the same time that Provider Screening is occurring. Team CNSI will complete the identification of competing processes as part of our development of the production schedule of jobs, and verify they are thoroughly tested.

Security Test

The MT PSM solution includes a robust role-based security model to facilitate control and access to PHI and PII. Our security system allows Team CNSI to configure operational roles at the screen and field level within the MT PSM solution.

Until the operational roles and access control rights are configured, Team CNSI tests using the pre-defined super-user role. As roles are configured and provided for each component, Team CNSI begins to test using those to verify that the data restrictions are enforced while confirming data that should be available is presented accurately. It is anticipated that these roles are available at the beginning of System testing so that all applicable roles are exercised as a part of System Testing. If the role definitions are provided earlier, Team CNSI will also test them during Iteration testing. This allows DPHHS to ensure that every role has access only to the data required to perform their job, safeguarding security and privacy in full HIPAA compliance.

Smoke Test

The Smoke test is a smaller subset of the Regression tests executed as part of the Configuration Management (CM) delivery process to ensure that the delivery of software to any environment is successful and that the software is functional. Team CNSI conducts Smoke testing using a library of test scripts that are both manual and automated. The test cases executed as a part of Smoke test validate the touch point between the various modules to make sure the integration is intact and communication between the modules are perfect.

Additional Testing

Team CNSI believes in testing as early and as often as possible. As detailed above, testing begins early in the Configuration stage (Iteration and System testing) and continues through the Implementation stage (UAT). In addition to the testing discussed earlier in this section, Team CNSI covers two other types of testing that require strong DPHHS involvement: Parallel Testing and Business-to-Business (B2B) Testing, both conducted during the UAT phase.

Parallel Testing

Parallel Testing primarily focuses on ensuring key functionality is working, processing, and producing outcomes the same way as compared to that in the legacy system. Parallel testing is most typically done in transaction-heavy applications where the parallel runs can be automated.

For the MT PSM parallel testing, Team CNSI will execute a set of test provider enrollment and maintenance activities in manual mode to confirm that the MT PSM is producing parallel results where expected. Team CNSI will work with DPHHS to identify the test set and the expected results.

Business-to-Business (B2B) Testing

B2B Testing is a State-run effort that focuses on the State testing the MT PSM solution with trading partners and other State agencies, and it typically begins two months prior to go-live. The purpose of the B2B testing is twofold:

- Validate the accuracy and acceptability of the MT PSM solution and related business processes
- Confirm DPHHS trading partners can effectively communicate with the MT PSM solution and related systems

In Team CNSI's implementations for Michigan, Washington, Illinois, and Utah, the states worked with their provider networks to identify a set of critical providers who they included in limited UAT activities. The selected providers participated in late-stage UAT testing by performing routine enrollment and maintenance activities on their converted account data. This is a viable option for DPHHS, but is not required for successful deployment.

Post-Operations System Changes Testing

Testing for changes made to the MT PSM after go-live falls into this category. It is necessary due to defect fixes or enhancements in response to State or Federal mandates. In the event of defect fixes, the testing will primarily focus on the changes made to a given feature(s) and regression testing. For changes made to the System because of a State or Federal mandates, Testing will primarily focus on the new feature(s) added and regression testing. Typically, automated test scripts are created and executed to cover the length and breadth of regression testing.

Once individual use case testing is completed successfully, interfaces and E2E/Integration testing will be conducted to uncover all the defects if any during interaction between different modules and accepting interfaces from other State and/or vendor agency modules.

TEST03

The Contractor must identify and resolve interdependencies that restrict or impede required testing of the Contractor's solution, other enterprise modules, or module components from performing required testing. Unless otherwise identified by the State strategies to resolve interdependencies must be reviewed and approved by the State prior to implementing the resolution strategy.

As a part of planning for the MT PSM, Team CNSI will identify the interdependencies that must be accounted for to verify the solution is comprehensively tested. These interdependencies are identified and listed in the integrated project schedule along with the owner(s) and a date when they need to be accomplished. These tasks are reviewed by the relevant stakeholders to make sure we get their buy in before the dates are baselined. Then the tasks are monitored and reviewed on a weekly basis to make sure they are complete on time. Should concerns about possible delays occur with interdependencies, Team CNSI will engage in collaborative discussion with DPHHS, its System Integration Contractor, and the other stakeholders involved to develop a mitigation strategy. If the interdependency impacts the project completion date, project scope, or budget, Team CNSI will initiate escalation to DPHHS.

TEST04

The Contractor shall perform testing and present the results for each of the following test levels: Performance Test results, System Test results, Parallel Test results, Regression Test results, Integration Test results. Test results shall be traced to the use case/user story and design documentation being tested.

Team CNSI prepares comprehensive test reporting for each layer of testing performed. This includes the reporting for performance test results, system test results, parallel test results, regression test results, and integration test results.

Each of the above test reports will have an Appendix with a bi-directional traceability matrix which will trace each Design Use Case to the Test Case and the Test Result.

Maintaining Traceability throughout Testing

Team CNSI maintains the DPHHS requirements in a gap traceability matrix that includes all approved gaps, their relationships to PMIS solution use cases, and related MITA business processes. Figure 3.10.2-54 shows an example test case traceability matrix. This matrix provides complete bidirectional traceability between the DPHHS requirements, MT PSM solution design documentation, related test cases, and MITA business processes. Team CNSI uses this matrix to ensure complete test coverage. When the project executes change management activity, the matrix is the tool we used to synchronize modifications to all impacted documentation and test cases.

State Requirement #	Gap Number	DSDD Part	Use Case/ Section#	Use Case/ Component Name	MITA Business Area	MITA Business Process #	Test Case Name
PE19	F-7-15 F-7-18	LG1A	2.3.1	Enroll As Individual Provider	Enroll Provider	EE06	CHAMPS_MICLOUD-STC-PE-LG1A-UC2.3.1- Enroll As Individual Provider
PE20	F-7-15 F-7-19 F-7-25	LG1A	2.3.2	Enroll As Group Provider	Enroll Provider	EE06	CHAMPS_MICLOUD-STC-PE-LG1A-UC2.3.2- Enroll As Group Provider
PE22	F-7-15 F-7-19 F-7-26	LG1A	2.3.3	Enroll As FAO Provider	Enroll Provider	EE06	CHAMPS_MICLOUD-STC-PE-LG1A-UC2.3.2- Enroll As FAO Provider
PE21	F-7-15 F-7-19 F-7-27	LG1A	2.3.4	Enroll As Contractor / MCO Provider	Enroll Provider	EE06	CHAMPS_MICLOUD-STC-PE-LG1A-UC2.3.2- Enroll As Contractor / MCO Provider

MTPSM-3-179

Figure 3.10.2-54. Sample Traceability Matrix. This matrix shows how requirements are tracked to completion from initial definition through testing to confirm all are met. Note: Requirement text has been redacted from this sample.

In keeping with Team CNSI's quality assurance standards, all new test cases undergo formal peer review. During peer review, each test case is reviewed in detail to ensure that the test steps, input conditions, output, and validation points are correct. Reviewers include CNSI team members from quality assurance, development, and functional areas. The peer review process minimizes the risk of misinterpretation of use cases as the test cases are predominantly based on the use cases.

Test Reporting

Team CNSI will present standard test output reports to the DPHHS as requested. Distributed to the development team leads, test team, and project management staff, the test progress report summarizes activities that have taken place during the test phase as well as the status of defects.

The weekly test progress report is generated once system testing begins and represents the progress of testing. The report contains two sections. The first section provides information for the current week being reported. The second section of the summary report provides cumulative (to date) summary statistics. The metrics available in both sections are reported by functional area with clear identification of the risks associated with each. Presenting the report in this manner, with historical weekly information and totals, may assist management in identifying any patterns in weekly and overall activity that may be used to make decisions regarding the project.

Team CNSI tracks the number of executed test cases. This allows the test team and project management to more accurately predict test completion. Low execution rates may indicate a problem with comprehension of the software being tested or the completeness of the software delivery.

Team CNSI also tracks the number of test cases being passed each week by comparing pass rates to execution rates, which provides an indicator of the quality of the software. This is measured over the entire scope of the project or within individual business areas. Pass rates provide a measure of software quality derived from the defect tracking system. Team CNSI follows a stringent process for creating and tracking defects. This process ensures that all defects are tracked to resolution and determines if the criteria for completion of a testing milestone have been met. The defect tracking process is documented, in detail, in the test plans.

In addition to providing defect reports, Team CNSI provides DPHHS with training and access to the Jira defect repository. Team CNSI can create customized reports or new testing reports at DPHHS's request, either on an ad hoc basis or as part of the regular reporting cycle throughout System and UAT testing.

Summarizing and Reviewing Test Results

Team CNSI conducts multiple rounds of Iteration testing, System testing, and Regression testing to correct defects discovered during testing. Once all test cases for the phase have met the acceptance criteria for exiting the test, a final assembly of all test results is created to demonstrate to DPHHS that the test has been completed successfully. Team CNSI submits all test cases and test scripts as part of the Test Results report.

Team CNSI creates a test results acceptance criteria document. This project artifact details the form and content of the test results delivery, which ensures a smooth delivery and assurance to DPHHS that the delivery itself meets their expectations. An outline of test results acceptance criteria is included in Figure 3.10.2-55.

Criterion	Description of Acceptance Criterion
Criterion # 1 Summary Test Results Report	Title Page Approvers Page Revision History TOC Preface (Purpose, Audience, Scope, Organization, Reference documents) Executive Summary Description of the test results report How to read the test results report Acceptance criteria for approving the test results from the Test Plan Test Results Summary Table Total Test Cases Executed Total Test Case Passed (P) Total Test Cases Failed (minor Severity 4/5 defect) Total Test Cases Failed (Severity 3 defect) Total Test Cases Failed (Severity 2 defect) Total Test Cases Failed (Severity 1 defect) Test Start Date & Test End Date Tests completed by (list of testers involved) Defect Summary Table Defects Opened/Closed by Severity Appendix A Test Case Result Tables which contains the test case #, the result, Defects addressed and Engineering Change Requests.

Criterion	Description of Acceptance Criterion
Criterion # 2 Test Results Evidence	Delivery of test cases and corresponding results Test case formats to be included are: Test Cases (includes traceability mapping to requirement) All Test cases to include detailed descriptions of input values used All Test Cases have a description of the test case within the name

Figure 3.10.2-55. Test Results Acceptance Criteria. The test results acceptance criteria document will ensure a smooth delivery and assurance to the State that the delivery itself will meet their expectation.

TEST05

The Contractor shall provide sufficient environments and resources for the following:

a. Synchronize the software and the data from the production environment and testing and impact analysis environment at a minimum on a quarterly basis or at the discretion of the Department.

b. Synchronize the software and the data from the production environment and training environment following software deployments.

c. Provide a fully functioning online test environment, which includes batch and online programs, files, and supporting systems.

d. Provide technical and functional support to create and analyze "what-if" scenarios and compare results between scenarios in the impact analysis environment. Provide an analysis of outcomes in impact analysis environment and another environment, such as production or test.

e. Provide State, Contractor, and IV&V staff a minimum of read-only access to all environments and tools.

f. Provide sufficient resources to support the execution of automated regression testing.

h. Provide comparative analysis support of regression testing results.

i. Conduct testing of approved system configuration changes, corrections or enhancements or before implementation.

j. Allow Department resources and contractors designated by the Department to create and edit appropriate data to support testing efforts, including provider, member, and reference data.

Following deployment, Team CNSI will maintain the environments resources necessary for ongoing production support and system enhancements.

- Team CNSI's experienced DBAs will ensure that the data between the production environment and the test environments are synchronized on a quarterly basis, or at the discretion of DPHHS, by refreshing test environment with production data.
- Team CNSI's experienced Lead Developer and the Configuration Management Analyst will ensure that the code and the data between the production environment and the training environment is synchronized with in a week after a new code has been deployment into production environment.
- After successful system testing, Team CNSI will provide DPHHS a fully functional online UAT environment which includes batch and online programs, files and supporting systems.
- Team CNSI will provide technical and functional support to create and analyze "what-if" scenarios and compare results between scenarios in the test environment. Team CNSI will also provide a detail comparative analysis of outcomes between test environment and production for the what-if scenarios.
- Team CNSI will provide State, Contractor, and IV&V staff a minimum of read-only access to all environments except development environment and all tools.

- Team CNSI will allocate experienced automation testers who have prior experience in PMIS automation testing to support the execution of automated regression testing.
- Team CNSI's experienced testers conducts system testing and regression testing of approved system configuration changes, corrections or enhancements or before implementation. The tested code will be deployed into UAT environment for the State to validate and pass before deploying it into Production environment.
- Team CNSI will allow DPHHS resources and contractors designated by the Department to create and edit appropriate data to support user acceptance testing efforts, including provider, member, and reference data.

TEST06

The Contractor shall ensure, in order to release code to UAT or production, it must meet the minimum acceptable defect levels:

• Critical: 100% have been resolved.

• High: 100% have been resolved.

Team CNSI has robust test entry and exit criteria for each layer of testing. Prior to promoting code to the UAT environment, Team CNSI verifies that the test exit criteria for system testing is met. We also verify that the test entry criteria for UAT has been met. We follow the same process for post-deployment code promotions from the lower system test environment to the UAT, training, and production environments. Team CNSI has provided a summary of the test entry and test exit conditions we monitor later in our response to this requirement.

Prior to deploying code to UAT and Production, Team CNSI must meet the exit criteria mentioned below.

- All Severity 1 (Critical category issues/bugs) must be fixed and resolved and regression tested successfully
- All Severity 2 (High Category issues/bugs) must be fixed and resolved and regression tested successfully

As noted in the introduction to this response section, all defects are recorded in Jira are assigned a defect severity level. For ease of reference, the defect severity levels are defined in Figure 3.10.2-56, which duplicates the table presented in Figure 3.10.2-49. Defect resolution SLAs will comply with the response time described in the RFP.

Defect Severity	Defect Severity Description
Severity 1: Very High	Results in a complete System outage with no workaround. Action results in a system crash or in damage to data, such as wrong results or a loss of data.
Severity 2: High	System functionality is degraded with severe adverse impact to the user and there is no effective workaround.
Severity 3: Medium	System functionality is degraded with a moderate adverse impact to the user but there is an effective workaround.
Severity 4: Low	The actual results have a user inconvenience or other minor inconvenience, such as typographical errors, or alignment errors, or extra steps are needed to complete function. These include all other discrepancies, spelling errors, or minor/trivial errors.
Severity 5: Documentation	All documentation defects that do not require system changes because of the documentation update.

Figure 3.10.2-56. Defect Severity Definition. Team CNSI will assign every defect with the defect severity level based on these definitions

Test Entry and Exit Criteria

Entry and exit criteria for each test phase and release is listed in Test Plan. At the start of each test phase, a Test Readiness Review (TRR) is conducted with DPHHS to document the project's readiness to begin testing activities for that phase. Each phase of test has a unique checklist that includes some common entrance criteria for testing.

Entry Criteria: Figure 3.10.2-57 lists the base entrance criteria for each phase of testing.

Iteration Test	System Test	User Acceptance Test
Review of the Test Plan specific to the Iteration Test phase has been approved	Review of the Test Plan specific to the System Test phase has been approved	Review of the Test Plan specific to the UAT phase has been approved
Defect tracking system (Jira) configured	Defect tracking system (Jira) configured	Defect tracking system (Jira) configured
Environment readiness review completed (Iteration)	Environment readiness review completed (System)	Environment readiness review completed (UAT)
Detailed System Design Document approved for all business area	DSDDs approved for all business areas	DSDDs approved for all business areas
	Iteration test completed	System test completed
	Converted data available in environment	Converted data available in environment
		Results for System test have been submitted to DPHHS

Figure 3.10.2-57. Entrance Criteria for Testing. The entrance criteria for each test level helps to ensure the project's readiness to begin testing activities for that phase.

The Test Plan outlines any additional criteria required for each phase of testing, including considerations for any elements unique to the DPHHS implementation of the MT PSM solution.

Test Exit Criteria: Exit criteria are used to establish when testing activities are completed for a given test phase. As testing progresses through each phase, the level of quality is increased and the corresponding exit criteria become more stringent. Figure 3.10.2-58 shows the exit criteria for each test phase and the severity level of open defects permitted at the end of each testing phase. These defect severities were previously shown in Figure 3.10.2-56.

Iteration Test	System Test	User Acceptance Test
All planned Iteration test cases are executed and a pass or fail determination has been established for each	All planned System test cases are executed and a pass or fail determination has been established for each	All planned User Acceptance test cases are executed and a pass or fail determination has been established for each
No open severity five defects	No open severity five defects	No open severity five defects
No open severity four defects	Mutually agreed up on number of open severity four defects permitted provided they are very cosmetic and aren't impacting the system usage.	Mutually agreed up on number of open severity four defects permitted provided they are very cosmetic and aren't impacting the system usage.
Open defects of severity three through two permitted	Mutually agreed up on number of open severity three defects permitted provided there are work around and system can still be used.	Mutually agreed up on number of open severity three defects permitted provided there are work around and system can still be used.
	No open severity two and one defects permitted	No open severity two and one defects permitted

Iteration Test	System Test	User Acceptance Test
	Results gathered and deliverable prepared for delivery to DPHHS	Results gathered and deliverable prepared for delivery to DPHHS

Figure 3.10.2-58. Exit Criteria for Testing. By defining exit criteria for each test level, Team CNSI documents the project's progress to move to the next phase of development or deployment.

TEST07

The Contractor shall plan and execute testing for all inbound and outbound interfaces, ensure accurate and secure data transmission between the solution and the ESB and coordinate with external entities as appropriate.

Team CNSI's test plan does plan for all the interfaces testing that are applicable for the MT PSM solution. All the sources for the inbound interfaces and outbound interfaces are identified and a secure mechanism for exchanging data between the solution and the ESB will be established contacting the relevant stakeholders.

Interface testing is typically executed at the end of the system testing phase after making sure the core system is working as per the requirements. Interface testing involves receiving and sending files between the MT PSM and other State agencies and organizations. This phase of testing requires careful coordination with the other State agencies and organization to make sure they are ready to test.

We have repeated following content on Interface Testing previously shown in our response to requirement TEST02 for the State reviewer's convenience.

Interface testing is a critical element of System testing. The goal of Interface testing is to verify a successful transfer of data to entities external to the MT PSM solution and verify that the data are properly interpreted by the receiving system. Team CNSI understands the complexities of interface testing. We work collaboratively with DPHHS to engage the external partner agencies and establish an approach for completing Interface testing prior to the start of System testing. Some of the key considerations for the interface test plan include:

- Identify key parties to complete the test activities for external interfaces
- Determine the availability of both human and computing resources for System Testing
- Identify the sequence of testing to be completed
- Coordinate common data that may be required to successfully complete the test
- Verify network connectivity has been established prior to conducting any test activities
- Test each interface completely, exercising all message protocols and responses, and capturing evidence of testing to include the files and messages used in testing, the operational reports, and the error messages and measures
- Test each interface to verify the data generation (outbound), transmission, and processing (inbound) can be completed per the design of the PMIS as configured for MT PSM solution

Figure 3.10.2-59 shows the common elements in each interface. During Interface testing, Team CNSI tests these common elements to ensure that they perform as expected.

Common Element	Description
Event Trigger Handling	Events to trigger interface processes (i.e., When an event occurs, the trigger for the interface is tripped, and a response is initiated.)
Validating	Routines to validate the interface data and protocol structure and to ensure that they meet expected content and structure
Logging	Routines to record critical events and activities for the interface
Reporting	Routines to collect statistical information for reporting (e.g., number of times an interface is used, total number of errors, total amount of data transmitted)
Process Management	Routines to start and stop external programs that are used as part of the interface specification (e.g., secure File Transfer Protocol (FTP))
Error Handling	Routines to handle error conditions (e.g., logging the error condition and repeating a request for information when a timeout occurs)
Status Monitoring	Routines to continuously monitor the status of an interface connection

Figure 3.10.2-59. Common Elements of Interface Testing. These common elements have become part of Team CNSI's repeatable standard interface testing process.

Interface testing is considered complete when Team CNSI has executed all the interface test cases during system test and has validated the following with the external interface owners:

- An outbound interface was exercised as far as the successful transmission of data, form, and content to the external interface owner
- An inbound interface was exercised as far as the successful receipt and processing of data transmitted by the external interface owner

TEST08

The Department plans to perform UAT on all software releases as part of the contract. The Contractor's approach to establishing testing environments should not impact the Department's ability to conduct continuous UAT in a separate, dedicated environment.

A dedicated User Acceptance Test environment will be established by Team CNSI a month before the start of UAT. DPHHS will use this environment to perform their acceptance testing. The environment will be up from 7:00 a.m. to 7:00 p.m. daily Mountain time, from Monday to Sunday except for planned outages approved by the State.

TEST09

The Contractor shall facilitate UAT as follows:

a. Provide test cases and scripts from previous test levels.

b. Assist the Department in developing UAT test cases.

c. Provide a dedicated UAT environment to the Department and maintain the environment as needed to support continuous UAT throughout design, configure/build and testing.

d. Refresh data, execute processes, and migrate releases or code fixes as requested or on an agreed-upon schedule.

e. Provide test data.

f. Provide a mechanism for the Department to enter defects into the online defect-tracking tool.

Team CNSI will provide DPHHS all the test cases and scripts that were created and utilized during system testing, integration testing, E2E testing, and regression testing. Most of the test cases are reused from evoBrix PMIS base module testing. Some are developed specific to gaps identified and configured specific to the MT PSM. The State can leverage these already created test cases rather than having to create them from the scratch. Team CNSI will also help the State in creating new UAT test scenarios that the State identifies to verify their requirements are met.

As previously noted in our response to requirement TEST02, Team CNSI will establish a dedicated UAT environment a month before the UAT start date. The UAT environment will be configured with converted data and code that has been promoted from system testing. The UAT environment will be maintained to ensure that it closely parallels the production environment. After go-live UAT Code and data updates will be conducted in accordance with a State-approved schedule. data is refreshed with production data on a mutually agreed upon timeline. The UAT environment will be maintained through the end of the contract.

Team CNSI will help the DPHHS in creating adequate test data that will help them to smoothly perform use acceptance testing.

As previously discussed in our response to requirement TEST06, Team CNSI uses Atlassian's Jira to record defects. This tool facilitates submission of defects and tracking them to resolution. Jira is used to capture defects or errors found in deliverables, documentation, and software that are under test. Jira provides defect reports throughout the entire test life cycle. This tool, and the process governing its use, allows Team CNSI and DPHHS to organize and automate the process of submitting, assigning, tracking, releasing, and testing defects until they are closed. Jira's built-in reports deliver real-time, relevant information in a convenient format and convenient location. These reports provide clear visibility into project progress. Jira provides reports that show statistics by person, projects, versions, or other fields within issues, and custom reports can be created in Jira if required by DPHHS.

Team CNSI will provide access to Jira for the State User Acceptance Testers to log in defects or issues uncovered during user acceptance testing of MT PSM solution.

TEST10

The Contractor shall provide Department resources or their designee access to test cases, test results and defect tracking via online tools. The Department reserves the right to inspect artifacts and results at any time.

Team CNSI will store all test cases and test results in the SharePoint Project Documentation Repository. DPHHS resources or their designees will be provided access to SharePoint to access the test cases, test scripts and Test Results Reports. Test Results Reports are formal deliverables presented to DPHHS for review and approval as a part of the MT PSM project execution.

As previously noted in our response to requirement TEST09, DPHHS will have access to Jira to review reported testing defects to reconcile the Test Results Report defects and the defects logged in Jira.

TEST11

The Department reserves the right to conduct independent testing of the solution at any time. The Contractor must cooperate with the Department or its designee, and provide environments, data, and technical support for independent testing.

DPHHS will be provided with the UAT environment one month before UAT begins. The environment will not be loaded with system tested code and converted data until the test exit criteria has been met for system testing. Testing of the MT PSM cannot begin until these milestones have been met. Team CNSI has committed to providing a sandbox environment early in the project to allow State users to familiarize themselves with the interface and system functions. The State can perform independent testing in the sandbox at any time with the understanding that it represents the base evoBrix PMIS and not the configured MT PSM.

Once UAT is established, Team CNSI will maintain and support the environment until the end of the contract to make sure State has access to it to test the system at any point of time. Team CNSI will support DPHHS with UAT test data and technical support to perform User Acceptance testing throughout the length of the contract.

TEST12

The Contractor's testing environments shall be sized to be capable of mirroring the production System in its infrastructure, files, databases, processing, and reporting.

Team CNSI will build System Test environment, Regression Test environment, and User Acceptance environment with capacity enough to hold at least one-years' worth of production data to replicate and mirror production system.

Data in these test environments will be refreshed at mutually agreed upon intervals to bring the data in line with the production data.

The test environments will have all the capabilities of generation letters and reports, receiving inbound interfaces and transmitting outbound interfaces just like the production environment.

TEST13

The Contractor shall work proactively with the State's designated testing resources to review all test results and provide the necessary system and functional information to create verification procedures and user acceptance test cases.

Team CNSI will share the results of System testing, Integration testing, and E2E testing with DPHHS designated testing resources. This documentation will be placed into the SharePoint Project Documentation Repository and made available for designated testing resources to review.

Team CNSI and the DPHHS designated testing resource will collaborate to develop detail verification procedures and UAT test cases. Because UAT is a shared responsibility between DPHHS and Team CNSI, a high degree of collaboration will be needed. In our previous PMIS implementations in Michigan, Illinois, Washington and Utah, the states relied heavily of the Team CNSI's test cases to develop their

UAT test cases. Team CNSI will support DPHHS to develop appropriate test cases for additional test scenarios defined by the State testers.

TEST14

The Contractor shall coordinate with the Department and specific module component vendors to conduct integration testing.

Team CNSI will identify all the agencies and organizations engaged with DPHHS in the implementation of the MT PSM. This includes all data exchange partners who send data to, or receive data from, the MT PSM.

During system test and integration test planning, Team CNSI will identify all the dependencies and make sure they are entered in the schedule as a task with due date. Team CNSI monitors the planned activities against the schedule to make sure all dependent tasks are complete prior to the start of system and integration testing.

Prior to System testing and UAT, Team CNSI will work with DPHHS and the module component vendors refine the schedule for conducting integration testing. As a part of the activity, Team CNSI will also confirm the sequence and scenarios that need to be tested as a part of the integration testing. The schedule is reviewed by all the stakeholders and baselined before execution. The schedule is revised and adjusted during execution based on the need of the project. Standard project change control will be applied in the event of a significant change. Significant, in this context, means a change to scope or schedule that puts the phase or project completion date at risk.

TEST19

The Contractor shall develop test criteria and algorithms for expected outcomes prior to production of reports.

Team CNSI test cases are based on the functional design documents. The design use cases have outcome for every single action. Hence the test cases/scripts will have expected outcome for every single step.

Because we start with a completed evoBrix PMIS module, most outcomes are predefined in the test cases and test scripts we use as the starting point for MT PSM-specific gap testing. Criteria for MT PSM-specific test will be discussed with the DPHHS as a part of test planning and preparation activity. Team CNSI and DPHHS follow the mutually agreed upon test criteria throughout the project and contract.

TEST20

The Contractor shall ensure that the Project Work Plan allocates sufficient time to the State's user acceptance testing activities relative to the detailed scope of work, requirements and gaps, the number of manually executed test cases, and the complexity. of module integration. The Contractor' will be responsible for extended user acceptance testing if the proposed testing duration is not sufficient for the State to validate the module.

During initial planning for the MT PSM, Team CNSI will work with the State to develop the UAT schedule. As noted previously, the team having responsibility for operating the solution will perform the

related UAT activities. DPHHS will be responsible for testing the provider enrollment, maintenance, management and both provider and security administrative activities. Team CNSI will perform UAT for the customer relationship management system and SiteVisitPro. There are coordination points between our UAT test activities throughout the UAT test period.

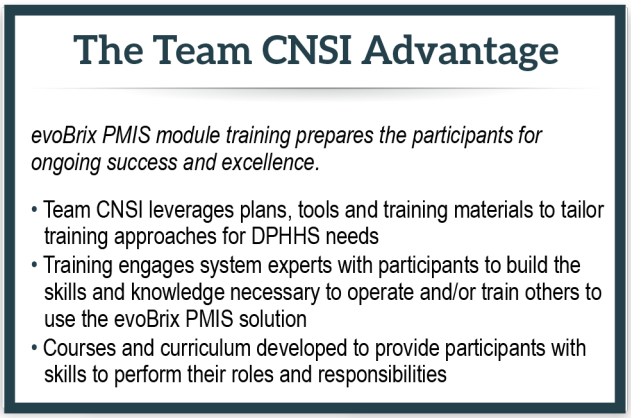
MT PSM is an SCI implementation rather than a DDI implementation. MT PSM will be configured from working production system code in use in Michigan, Illinois, Washington, and Utah. The base code is the same as the CMS-certified systems in operation in Michigan and Washington with minimal change tailor the evoBrix PMIS solution for DPHHS. Owing to both the short implementation time frame and the reuse of existing code already in operation in other states, the time required for UAT will be proportional to the changes being made to address DPHHS gaps, and regression testing, rather than testing the entire system as we would need to do with a conventional DDI project.

Team CNSI will work in collaboration with DPHHS to scope and plan the UAT effort in accordance with the schedule and to help the State to develop its test cases and test data to support completion of UAT within the planned timeframe. Should the State require additional time to validate the module it will be managed as a standard change request to the schedule and will follow the agreed upon change management process to make any necessary adjustment to schedule.

3.10.2.7 Training

The Contractor must provide training to designated MPATH team members, DPHHS training staff and other staff responsible for training to achieve an understanding of the new system, services, or release. The training will incorporate a train-the-trainer model so that participants can, in turn, provide training to additional users. Users must become proficient in using and viewing information in the Contractor's solution in order to ensure effective and efficient business operations and service delivery. The Offeror must describe their approach to meet each of the detailed training requirements defined in Attachment F, Requirements Matrix.

Team CNSI recognizes that well-trained users are a critical component of the overall success of our evoBrix PMIS solution. New or changed functionality can enhance organizational performance when users are confident and competent performing their assigned roles as they interact with the system. Team CNSI has an extensive history of successfully providing training for staff, clients, providers, and stakeholders. In our more than 50 years of commercial, federal, and state health care service and administration, we have trained more than 3,500 staff and offered education and outreach to more than 340,000 providers and suppliers.



MTPSM-3-195

The evoBrix PMIS solution has a core set of training and materials that is applicable to all implementations and can be tailored if needed for an implementation that has some unique needs. Team CNSI uses a training calendar in conjunction with a training curriculum to organize and schedule the training courses included in the approved training plan. We collaborate with DPHHS to further tailor the suite of learning objectives and arrange them into sets of classes with targeted participants, recommended delivery methods, and recommended timing based on role and responsibility. Our approach to establishing a curriculum provides a linear progression beginning with a high-level overview of the

DPHHS solution and moving into participants' respective roles and responsibilities, so each course in the curriculum can be arranged to build on the courses before it until all skill and knowledge targets for the given role and responsibility have been reached. Once the curriculum is set, we work with DPHHS to align the training calendar with the project schedule to provide sufficient time for participants to complete the training prior to UAT activities.

evoBrix PMIS is designed to be easy to learn and use. Once initial positive momentum is achieved through a basic understanding of the system, users are soon able to navigate and use features that are consistent throughout the system. To provide users with a baseline understanding of the system, Team CNSI provides both instructor-led training for trainers and computer based eLearning for the base evoBrix PMIS solution.

Instructor-led Train the Trainer segments:

- Provider/State User Access Management – Authentication & Authorization
- Provider Administration Services
- Legacy Provider Data Validation
- New Provider Enrollment and Screening
- Enrollment Modifications and Screening
- Provider Revalidation and Screening
- Associated COTS product training (as applicable)

Computer-based eLearning segments geared toward providers:

- User Account Registration and Enrollment Process
- Legacy Provider Data Validation
- Enrolling as a New Individual Provider
- Enrolling as a New Group Provider
- Enrolling as a Special Provider – Facility/Agency/Organization (FAO), Clearinghouse, and other State Specific enrollment types
- Enrollment Modifications – Individual
- Enrollment Modifications – Group Practice
- Enrollment Modifications – FAO, Clearinghouse, and other State-specific enrollment types

This training will provide trainers and users with what they need to use the system confidently. In addition, Team CNSI will provide a user guide/manual organized by procedures and roles to facilitate use of the system. The procedures in the guide/manual are formatted as job aids that provide end users with the steps needed to complete each procedure for their role. The classes and procedures in the user guide/manual make it very easy for users to understand how the system can help them complete their jobs.

Team CNSI can arrange our packaged courses and any additional courses identified in the approved implementation training plan into a final curriculum with the associated learning objectives, audience, and method of delivery. To facilitate effective management of the courses, Team CNSI utilizes Cornerstone Learning Management System to administer, deliver, and track the curriculum. The training in this proposal includes packaged training modules for the Core functionality which can be tailored to the solution as well as Options A and B (reference Requirements TRN15 and TRN16).

For tailoring the base training materials or developing new modules beyond the standard package, Team CNSI follows an established and proven Analyze, Design, Develop, Implement, Evaluate (ADDIE) life cycle framework. As shown in Figure 3.10.2-60, we use the industry-standard ADDIE method to guide

training development, as recommended by the Association for Talent Development. ADDIE provides a common platform for collaboration to determine the audience, necessary skills, required knowledge, and delivery methods for the PMIS solution training.



Figure 3.10.2-60. The ADDIE Cycle. ADDIE is the industry standard model for development and delivery of training for adult audiences.

In the analysis phase, the instructional context is clarified, goals and objectives are established, and the learning environment and learner's existing knowledge and skills are identified. The design phase deals with learning objectives, assessment instruments, exercises, content, subject matter analysis, lesson planning, and media selection. The development phase is where the developers create and assemble the content assets that were created in the design phase. During the implementation phase, a procedure for training the facilitators and the learners is developed. The evaluation phase consists of two parts: formative and summative. Formative evaluation is present in each stage of the ADDIE process. Summative evaluation consists of tests designed for domain specific criterion-related referenced items and providing opportunities for feedback from the users. Lessons learned from the full cycle are then incorporated back into our standard process as appropriate.

TRN01

The Contractor shall provide technical training to agency project resources and designated contractors to develop an understanding of how to monitor the system using available tools and dashboards while leveraging technical and functional documentation and/or reports.

Team CNSI will provide technical training to assist designated persons to perform system monitoring responsibilities using available tools and reporting capabilities. Team CNSI will collaborate with project resources to establish the scope of training required and incorporate it into the Training Plan deliverable. The training plan deliverable will include all training to be conducted on the project, including system monitoring.

One of the system monitoring tools provided with the solution is Team CNSI's innovative dashboard application called HealthBeat. This tool provides access to real-time or near real-time measures within the evoBrix PMIS solution. Figure 3.10.2-61 shows trends for two sample metrics. Once set up, monitoring can be simplified and transparent for any user whether they have technical training or not.

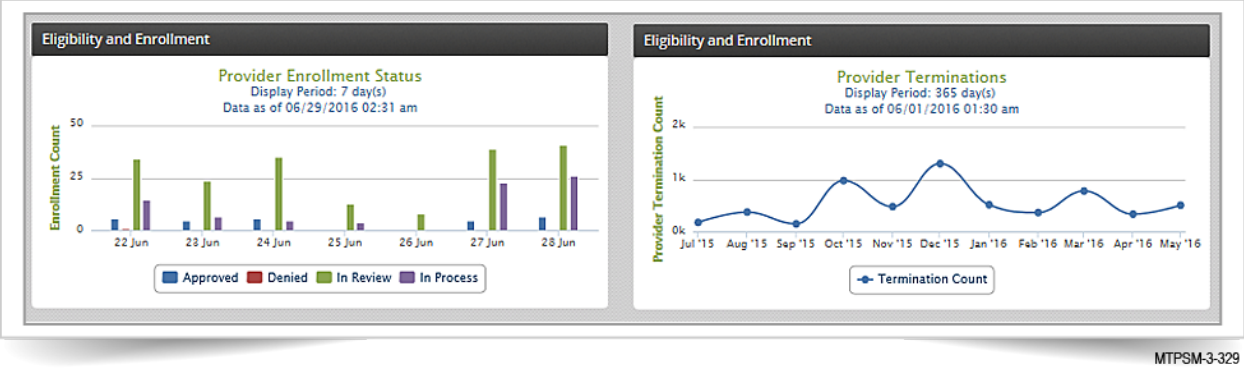


Figure 3.10.2-61. HealthBeat Dashboard Sample. HealthBeat dashboard functionality provides transparency for critical metrics.

TRN04

The Contractor shall update training materials when changes occur.

A critical success factor for any initiative is the ability to successfully identify and manage change. Team CNSI will work with DPHHS to assess the impact of changes to the system using the change management process established for the project. One of the necessary elements to be considered with any change is the degree and level of training that may be required to accompany changes to the system. When a change is identified and introduced through the change management process, Team CNSI will assess each aspect of the change's impact to the environment including the impact upon communication, training, and publications related to system functionality. The change management process and the training plan will be used to coordinate timing and approvals that verify changes required to revised artifacts are updated to coincide with approved system changes.

TRN05

The Contractor shall collaborate with the agency to finalize a training schedule.

Team CNSI will collaborate with DPHHS to develop and maintain a training schedule that meets the needs of the stakeholders as part of the training plan deliverable. The training plan is a living document that will continue to be updated as the project progresses through its lifecycle.

TRN06

The Contractor shall maintain and update the training environment with training data to use during user training.

Team CNSI will set up, maintain, and update a training environment with de-identified data which will be used to provide training necessary for DPHHS and other stakeholders. Team CNSI will work with DPHHS to establish a training schedule to ensure coordination of the training environment's use by various stakeholders and to establish support needs for the environment. Team CNSI has learned through experience that coordination is key to establishing and maintaining adequate support for any environment, including the training environment.

TRN07

The Contractor shall provide train-the-trainer sessions for Agency resources or designated agency resources and other staff responsible for training.

Team CNSI will plan and conduct Train the Trainer (TTT) sessions for State and State-approved resources in a location provided by the State. The TTT courses will be instructor-led and consist of the following training modules:

- Provider/State User Access Management – Authentication & Authorization
- Provider Administration Services
- Legacy Provider Data Validation
- New Provider Enrollment and Screening
- Enrollment Modifications and Screening
- Provider Revalidation and Screening
- Associated COTS product training (as required)

evoBrix PMIS is designed to be easy to learn and use. All TTT modules are offered to trainers prior to go-live based upon the approved training plan.

TRN08

The Contractor shall utilize a variety of delivery methods to best meet the training objectives. Examples include online self-paced training presentations, in-person classroom setting, written material, and demonstrations.

Team CNSI's training approach covers a spectrum of methods to accommodate all learning types, staff locations, and preferred formats of training. This includes the following possible methods:

- **eLearning courses** are pre-recorded and available 24 hours a day, 7 days a week via any standard LMS or by download. Team CNSI brings a standard set of courseware that can be utilized. Team CNSI will offer these through its Cornerstone Learning Management System if the DPHHS does not have one available. We can develop our tutorials for use on any modern LMS which provides for multiple types of media including static content such as slides, forms, audio recordings, and video with screen-capture technology. This enhances the learning experience by associating real situations with training materials.

- **Webinars/Demonstrations** provide online training and video sharing, simulating "face-to-face" and "in person" training sessions and meetings without the costs associated with travel. Webinars allow for activities such as real-time interactive conferences, sharing training presentations, application demonstrations, and web tours.
- **Instructor-led, hands-on training** uses a dedicated training system that replicates the actual evoBrix PMIS solution to ensure the highest degree of direct application from the classroom to the functional work area. Team CNSI uses presentations, distributable curriculum, tutorials, and hands-on application training. Staff and DPHHS personnel receive general overview training in the use of the solution as well as training specific to their security profile, functional role, and system usage needs.
- **Train the Trainer (TTT)** model is a training strategy widely used in the workplace. The trainer, a subject-matter expert, trains other employees and simultaneously teaches them how to train others in the use of the system. The method offers distinct advantages over other training models because it allows rapid expansion of knowledge and skills into larger populations.

TRN09

The Contractor must provide training necessary to support new functionality and/or major software releases that materially change the user interaction.

Team CNSI will provide training necessary to support new functionality and/or major software releases that materially change user interaction. As part of our change management process, we analyze whether additional training or updates to training materials are needed. Any updates are incorporated into the analysis of the total impact.

TRN10

The Contractor shall provide training to Agency staff and other designated module vendors on the overall data management strategy and investigating data or process issues related to module integration.

Users who need to investigate data or process issues related to module integration will need to possess some background knowledge and skills in the domain. As a result, we will work with DPHHS to identify the data experts and power users who should be candidates for training as opposed to those who can accomplish their analysis using canned reports or simple ad hoc query capabilities available through existing tools.

Team CNSI believes that data is the lifeline of a Medicaid enterprise and the timely availability of data that is both reliable and secure is key for successful business and technical operations. Team CNSI's evoBrix PMIS solution is designed with a sound data management strategy that is key for managing the current and future data needs of MT PSM. We understand that it is not only sufficient to have a good data management strategy, but also, and more importantly, to be able to provide appropriate role-based access to data for users, encompassing both business and technical communities, so that they could make effective decisions for investigating data or process issues during day-to-day operations. Training and knowledge transfer is designed for specified agency staff to familiarize them with the basic data governance methods and processes to handle the set of systems and applications, interfacing and interoperating both within the evoBrix PMIS solution and with the partner/vendor systems that comprise the broader DPHHS MPATH enterprise. Toward that end, agency staff and other designated module vendors will be provided with relevant training and knowledge transfer to understand the evoBrix

models/processes that support data inquiry, data analysis, and ad hoc reporting, as shown in Figure 3.10.2-62.

Knowledge Area	Topics Team CNSI will address…
Data Origin, Collection, and Frequency	■ Where does the data come from? For example, from an upstream State-managed system, from another module vendor, from CMS? ■ What is the mechanism for collecting the data? For example, is the data keyed in through the application screens, received and loaded via a web service or batch interface, received as a paper form that is scanned and loaded? ■ How frequently is the data collected? For example, is the data created/updated on a daily or weekly basis?
Data Dependency	■ Is the transactional/operational data dependent on master/reference data? ■ How is the master/reference data setup and periodically maintained in the system?
Data Models	■ How is the solution structured and configured to address the needs of the users? ■ How is the data organized? ■ How are the entities and attributes defined and used? ■ How are the entities related? ■ What is the format and size of the attributes within the entities?
Data Usage	■ How is the data processed and stored? ■ In what business processes are the data used? ■ How is the data transmitted among the various components within and outside the MT PSM solution? ■ What should be done should there be an issue during the submission or receipt of a file to/from MT PSM? ■ How to differentiate between a data and a process issue? For example, a certain field in a file that is in an invalid format could be categorized as a data issue, while a file that hasn't been Ftp'd successfully could be attributed to a process issue related to a discrepancy in the file exchange.
Data Inquiry	■ Can the data be directly accessed in the database and queried? ■ What tools are recommended to be used for querying the data? ■ How to develop basic queries to interact with the data in the backend? ■ How to export the data for analysis? ■ What are the do's and don'ts while querying the data?
Data Reporting and Visualization	■ What are the different types of reports available to users to support agency operations? ■ Users can create ad hoc reports and visualizations.

Figure 3.10.2-62. Data Management Knowledge Areas. Knowledge areas needed to understand the evoBrix models/processes that support data inquiry, data analysis, and ad hoc reporting.

TRN11

The Contractor shall develop and maintain electronic training guides and materials to support the Train the Trainer instruction.

The training materials referenced under TRN07 will be provided in electronic format. Team CNSI will collaborate with DPHHS to tailor these materials to support Train the Trainer instruction.

In addition, Team CNSI will provide a base system user guide organized by procedures and role to facilitate use of the system. The procedures in the guide/manual are formatted as job aids that provide end users with the steps needed to complete each procedure for their role. The classes and procedures in the user guide make it very easy for users to understand how the system can help them complete their jobs. These materials can be utilized by trainers to support their training sessions on the PMIS solution.

TRN13

The Contractor shall provide training and support to State staff and individuals designated by the State (e.g., IV&V, QA/QC vendor), on the use of DDI tools provided by the contractor. This may include traceability tools, document repositories and testing tools.

Team CNSI will provide the necessary training for State staff and the State's designees to function efficiently on the project. Areas typically covered for the project training include:

- Project Orientation to Tools and Processes
- Use of Tools and Methods/Technologies
- Overview of Documentation Repository, Change, and Configuration Management
- Records Management

TRN14

The Contractor shall provide training on the system for UAT testers. The Contractor shall provide updated User and System Documentation to UAT testers to support the UAT effort.

Team CNSI recognizes that training is necessary to ensure that team members are prepared to begin UAT and move seamlessly into the operations. Team CNSI's evoBrix solution is packaged with a set of standard eLearning training modules covering the base functionality of each module. The eLearning modules are tailored for unique situations applying to a specific state's requirements.

During implementation training, we have two primary focus areas:

- Training DPHHS trainers to develop the training necessary to deliver pre-go-live training to providers and DPHHS staff who will be performing specific activities after the system is in operations
- Training the DPHHS and other stakeholders to support UAT activity

3.10.2.8 Implementation and Acceptance

Prior to implementation, the Contractor must demonstrate readiness to implement the solution and to provide operational support and maintenance of the proposed solution(s) for the remainder of the Contract term. The Contractor is responsible for managing the end-to-end implementation of the proposed solution. DPHHS expects the Contractor to help formulate strategies for a successful transition.

DPHHS must formally approve the implementation of the solution based on pre-defined acceptance criteria. DPHHS's acceptance of the solution will initiate the Operations, Maintenance and Configuration phase of the contract. The Offeror must describe their approach to meet each of the implementation and acceptance requirements defined in Attachment F, Requirements Matrix.

Team CNSI understands that transitioning the evoBrix PMIS Solution to operations is a major factor in achieving DPHHS' goals and objectives for the project. There are many moving parts in the transition to a SaaS system, including the infrastructure, application software, updated business processes and training the users, certification readiness, provider outreach, and overall readiness. Meeting the needs of DPHHS and provider communities while maintaining future upgrade paths is a result of careful planning and a clear understanding of the solution that is being transitioned.

As the project progresses through its life cycle, all parallel tracks will be orchestrated and scheduled to converge into a tightly woven fabric of dates and interdependencies that will be centrally tracked and

managed to ensure that all components are ready for system deployment and the "pre-go-live" state at the same time.

During the Transition phase (Implementation to Operations), Team CNSI will configure the production environment, support acceptance testing, perform a final conversion of data, prepare the production facilities and business services, and provide written assurance to the State that the MT PSM solution is ready for production.

The Team CNSI Advantage

Team CNSI utilizes low risk transition and implementation techniques.

- Implementation Plan checklists assist stakeholders in assessing the readiness of the technical, business, and information architectures
- Integrated implementation approach facilitates seamless transition to production
- Our value-add provider readiness testing ensures providers can submit claims day one of production
- Well defined service validation and testing activities including verification of test plan and design
- Team CNSI utilizes the ITIL approach to service validation testing, as well as iVision360 methodologies

MTPSM-3-123

Management Activities

Team CNSI's Project Management Office (PMO) supports all phases of the evoBrix MT PSM project beginning on the contract effective date. The PMO is Team CNSI's management control center for each phase of the contract. It ensures that all contract, development, quality, and business process operations are performing to the service levels stipulated in the contract. For transition activities, the PMO continues to maintain the project schedule and report status to DPHHS, collaboratively tracking and mitigating issues and risks, and monitoring implementation and cutover checklists. The PMO also oversees contingency planning and contingency plan execution, if needed.

Implementation Activities

The initial Implementation planning process and Implementation plan is a key input to a successful evoBrix implementation. The planning process produces a complete list of activities that must be completed to ensure successful deployment of the system and related business operations activities. The activity list spans technical and business readiness from provisioning the production environment though ensuring providers and business operation staff have successfully completed training. The activity list is a collaborative product of Team CNSI, DPHHS, and other organizations involved in the deployment. Collaboration activities include collaborative planning sessions and operations readiness reviews. We will leverage our extensive practical knowledge of the activities required to successfully deploy the system and initiate system and business operations to ensure a smooth, low-risk, implementation and production cutover using our implementation checklist and our implementation calendar.

Using our proven framework tailored for the DPHHS implementation is much more efficient and reduces the risks associated with implementation of the evoBrix solution. The MT PSM Implementation Plan is based on Team CNSI's highly successful implementation plans from our other MMIS implementations in Washington and Michigan and provider implementations in Illinois and Utah.

Working with the DPHHS, MPATH interface partners, legacy MMIS and data warehouse vendors, agencies and systems that interoperate with the DPHHS MPATH core system, and shared services and stakeholders, Team CNSI develops implementation plans that include a final implementation calendar and production cutover checklists. The checklists provide a consolidated and integrated set of critical milestones and activities that lead to the deployment. We have proven the effectiveness of the checklist on our prior implementations allowing which have allowed a smooth transition to operations. We also include implementation readiness metrics, such as provider, staff, and organizational readiness metrics for use in the readiness assessment checkpoint meetings.

©2017 CNSI

The checklists include the following items:

- Verification of UAT progress and objectives
- Confirmation of hardware and software installation for Production and Disaster Recovery (DR) sites
- Confirmation of network infrastructure and single sign on integration
- Confirmation of database setup and configuration
- Confirmation of hardware, software, and facility security procedures
- Execution of initial and final data conversion and population of the production environment
- Monitoring of training progress and confirmation of training completion
- Demonstration of backup and recovery features
- Monitoring staff readiness metrics
- Monitoring provider readiness metrics
- Monitoring organizational readiness metrics

The implantation plan also includes activities that must be orchestrated for a smooth transition to operations. We collaborate with DPHHS and other stakeholders to have business activities stop as close as possible to the production cutover date. This is to ensure that the disruptions are minimal. Please refer to Section 3.10.2.2 System Development Methodology, for implementation planning and activities.

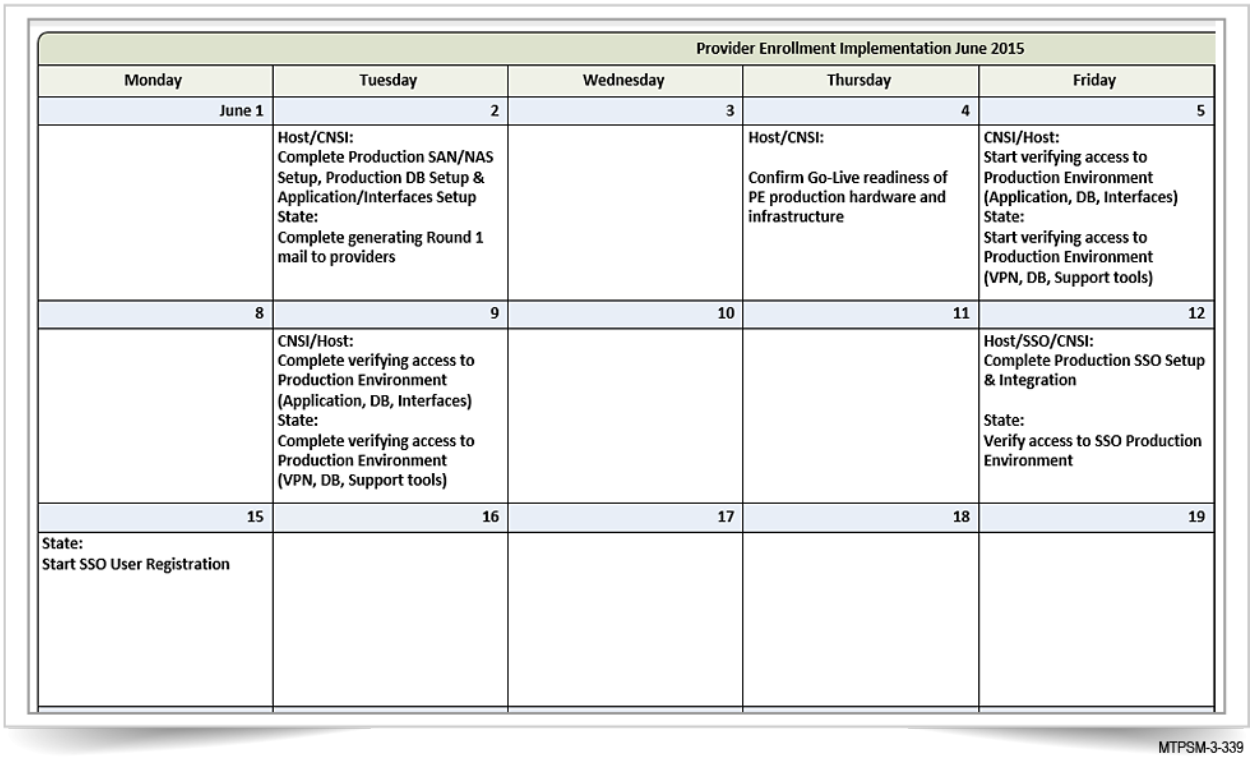
Figure 3.10.2-63 provides an excerpt sample from a prior PMIS implementation. Figure 3.10.2-64 provides a sample calendar page from a prior PMIS implementation.

Provider Enrollment Project Implementation Checklist

Task ID	Task	Oranization: Actor	Planned Start Date	Planned End Date	Actual Completion Date	Approver	Approval Date	Status Description
LEGEND								
	Green - Task is completed							
	Red - Task is delayed							
	White - Task is open							
Infrastructure Setup and Readiness for Go-Live								
1	Verify the readiness of [redacted]/State PE production hardware and infrastructure, including Application servers, DB Servers, networking and firewall rules	Team CNSI: GS, DK, AM Host: BG, AMM	1/26/2015	5/28/2015		CNSI: JH Host: BG, AMM		
2	Verify License and Maintenance agreements for software used in deployment	Team CNSI: GS Host: BG	3/2/2015	3/6/2015	3/6/2015	CNSI: JH Host: BG	3/6/2018	Completed
3	Verify appropriate storage (SAN/NAS) have been created and installed for WebSphere, Oracle, Interfaces, conversion	Team CNSI: GS Host: BG	3/23/2015	5/28/2015		CNSI: JH Host: BG		
Transition Tasks								
130	State stops accepting provider applications & paper-based updates	State: JRH, JRH, AC, NG, LR, RR	5/29/2015	5/29/2015		State: JRH, JRH, AC, NG, LR, RR		
136	Deploy State PE (Application and Interfaces) Code in Production Environment	Team CNSI:AM, MB	7/11/2015	7/16/2015		CNSI: JH		
[redacted] State PE Go-Live - (12:00AM) July 20 2015								
Management Gate Meeting - Sponsor Meetings								
144	Management Gate Meeting - Program Leadership Meeting (Gate-1) "Approve entry to 14-day implementation activities"	Program Leadership	7/2/2015	7/2/2015		N/A		
145	Sponsor Meeting "Status Update"	Sponsors & Program Leadership	7/15/2015	7/15/2015		N/A		
146	Management Gate Meeting - Executive Leadership/Sponsor Meeting (Gate-2) "Final Go/No-Go Decision"	Executive Leadership/Sponsors	7/16/2015	7/16/2015		N/A		

MTPSM-3-338

Figure 3.10.2-63. Sample Excerpt of Implementation Checklist. The implementation checklist includes all the details necessary to complete implementation of the PMIS module. This example shows a few tasks from three of the many areas tracked in the checklist.



Provider Enrollment Implementation June 2015				
Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**
June 1	2	3	4	5
	Host/CNSI: Complete Production SAN/NAS Setup, Production DB Setup & Application/Interfaces Setup State: Complete generating Round 1 mail to providers		Host/CNSI: Confirm Go-Live readiness of PE production hardware and infrastructure	CNSI/Host: Start verifying access to Production Environment (Application, DB, Interfaces) State: Start verifying access to Production Environment (VPN, DB, Support tools)
8	9	10	11	12
	CNSI/Host: Complete verifying access to Production Environment (Application, DB, Interfaces) State: Complete verifying access to Production Environment (VPN, DB, Support tools)			Host/SSO/CNSI: Complete Production SSO Setup & Integration State: Verify access to SSO Production Environment
15	16	17	18	19
State: Start SSO User Registration				

MTPSM-3-339

Figure 3.10.2-64. Sample Implementation Calendar. Team CNSI creates a complete calendar of activities leading up to deployment of the system. This excerpt shows sample activities for a single month. The Implementation Calendar for MT PSM will cover all months included in the implementation period.

Production Cutover Execution and Maintaining Service

In preparation for final data conversion activities, the legacy vendor completes the processing of data in the current MMIS system so that the final data extract can be performed. This activity is dependent upon the current operational cycles, and Team CNSI and DPHHS will need to determine collaboratively how those processes will be completed during the implementation planning activity while maintaining SLAs. While the preparation and ongoing readiness activities start during the implementation phase, we begin the readiness assessment 90 days prior to the go-live date and include two additional planned checkpoints, one each at 60 and 30 days prior to the planned go-live date.

Once the decision is made to proceed with the final implementation and confirmation is made for final readiness prior to go-live, Team CNSI and DPHHS monitor key processes to ensure that the final data conversion extract from the current MMIS system is executed on time and the data are loaded to the conversion staging area. Team CNSI then deploys the latest production software, proceeds with final data conversion, and performs validation and verification testing.

Team CNSI and the DPHHS meet daily the last two weeks before the go-live date so that DPHHS staff members are kept up-to-date with the most recent progress. The final cutover period usually takes one to two weeks to complete, depending on the business needs, and is determined by the planning process. Our implementation approach focuses on minimizing disruption of payment to providers and external parties by optimizing the sequence of events in the final cutover period, based on the operational cycles of the legacy system. Team CNSI completes an Operational Readiness Review Checklist and obtains written approval from the State to start operations. Please refer to Section 3.10.8 Performance Standards, and our

response to requirement SLA67, which requires the Contractor to receive Implementation Acceptance from DPHHS.

For interfaces, Team CNSI, the State, and the external interface partners monitor the final interface executions to and from the current MMIS system to ensure completion of those data exchanges. Most interfaces from the evoBrix Solution usually begin running after the system go-live. Exceptions where interfaces must run prior to the system go-live are documented in the Operational Readiness Review Checklists (ORR) checklist and executed per the Implementation Plan.

Risk Mitigation - Contingency and Rollback Planning

The contingency scenarios are developed jointly with the State, legacy vendors, and stakeholders during the Implementation planning period, and are captured in the checklist. The most common scenarios and mitigation examples are highlighted in Figure 3.10.2-65.

Common Risk Scenario	Risk Mitigation Strategy
Provider community is not ready as measured by the readiness metrics	Mitigation strategies may include providing additional communication to providers, offering additional online training classes, or adding additional testing periods so that providers can test the new system test environment.
Data conversion data quality issues during cut-over	By using an iterative approach during the initial data conversion period, Team CNSI ensures that the data exceptions are resolved, and changes to the conversion rules and programs are made prior to the cutover period, minimizing the risks during the final implementation.
Code deployment issues	In addition to the checks in the configuration and deployment process, we have scheduled the validation and verification testing period to identify and correct any possible code deployment issues.
Business process contingency scenarios	Team CNSI assesses business functions that may fail and need mitigation actions in production. Working with the DPHHS and the legacy MMIS vendor, Team CNSI is responsible for documenting the business contingency scenarios so that they can be included in the Implementation Plan. Team CNSI has examples and templates that can be tailored to DPHHS-specific scenarios.
State staff or State organizations are not ready as measured by the readiness metrics (Staff, Provider and Organizational Metrics)	The mitigation includes additional training and coaching sessions. DPHHS may consider rolling out the functionality in stages. For example, Provider PMIS can be rolled out first, followed by Siebel and others. The evoBrix Solution functionality is available at go-live, but the staff access can be restricted so that rolling out is more manageable from the DPHHS staff and State organization perspective.

Figure 3.10.2-65. Possible Risks Related to the evoBrix Solution and Services Implementation and Cutover. Based on successful implementations in Washington and Michigan, Team CNSI is well-prepared to mitigate any potential risks during implementation and cutover.

Team CNSI's contingency planning also includes planning for operation contingencies that could occur early in production. We recognize that failures can occur which would require a rollback to partial or full legacy operations. These failures can be instantaneous or may develop gradually over time. The former must be addressed, as needed, to restore required functionality, and our planning allows for that with State approval. But Team CNSI contingency planning attempts to identify the symptoms of a potential failure early in the life cycle, so that pre-planned mitigation can occur prior to reaching the point where rollback to legacy functionality is required. Team CNSI's contingency planning is included in the implementation plan.

IA01

The Contractor shall follow the following process for deploying each proposed solution(s) to production:

a. Submit an implementation letter to the State confirming that the solution is ready for

implementation.

b. Receive the State's approval of the implementation letter, accepting the Contractor's confirmation.

c. Deploy the solution according to the approved Implementation Plan.

d. Provide confirmation that the solution has been deployed to production and the Contractor has completed three (3) calendar days of operations without significant operational issues defined as no critical or high defects.

e. Receive the State's acceptance of the system implementation.

With daily DPHHS involvement from 30 days prior to go-live and throughout the final cutover period, the Operational Readiness Review Checklist is the culminating proof of what Team CNSI has already demonstrated and DPHHS has already reviewed. Due to the tight timeframes during the final implementation, the Operational Readiness Report is compiled by Team CNSI, and reviewed by DPHHS on a regular basis during the cutover period. Once Team CNSI formally submits the final version of the Operational Readiness Review Checklist, the DPHHS will be able to quickly provide written approval to start operations.

Team CNSI will follow the process defined by DPHHS for deploying the evoBrix PMIS solution to production:

- Team CNSI will submit an implementation letter to the State confirming that the solution is ready for implementation
- Team CNSI will receive the State's approval of the implementation letter
- Once the signed implementation letter is received, Team CNSI will deploy the solution according to the approved Implementation Plan
- Team CNSI will then provide confirmation that the solution has been deployed to production without significant operational issues defined as no critical or high defects within three calendar days of operations
- Team CNSI will then receive the State's acceptance of the system implementation per the exit criteria identified in the Operational Readiness Review Checklists (ORR)

IA02

The Contractor shall monitor the initial operation of the solution to ensure that there are no immediate or ongoing adverse effects on the Department's programs according to the performance expectations identified in the Contractor's scope of work.

Team CNSI's strategy for monitoring operations and ensuring services levels are met during the initial operations period includes our 24x7 Network Operations Center located in Rockville, Maryland, our HealthBeat tool, iTOP Configuration Management Database (CMDB), Oracle Ops Center, and Oracle Enterprise Manager. Team CNSI uses this toolset to measure, monitor, and report performance against the SLAs on an ongoing basis throughout the life of a contract. Refer to Section 3.10.8 Performance Standards & 3.10.4 Operations, Maintenance, and Configuration for more detail regarding service level tracking and reporting.

Team CNSI also utilizes an ongoing systems operations group that consists of team leads representing the business, functional, and system areas. This team is the hub for incident management and reporting across the system, including defect tracking and management, test management, and release management.

Similarly, the business operations team meets to assess the transition activities during cutover and works with the systems team to address concerns and ensure implementation is as smooth as possible. As the system stabilizes, they meet less frequently, arriving at a final interval of weekly.

Prior to commencement of routine operations, annually thereafter, upon the implementation of a change that affects existing SLAs, and/or at the request of the State, Team CNSI reviews the SLAs to determine if revisions are needed. If so, such changes follow the change control process to identify and evaluate any potential impacts and are subject to mutual agreement of DPHHS and Team CNSI based on that assessment.

IA03

The Contractor shall demonstrate that the System infrastructure (hardware, software, and interfaces) is operational and meets federal and State architectural, technical, security and privacy requirements as well as the business and functional requirements.

Team CNSI will demonstrate that the evoBrix solution infrastructure is operational and meets federal and State architectural, technical, security, and privacy requirements as well as the business and functional requirements. As part of the Operational Readiness Review checkpoint, Team CNSI will review hardware, software, and interfaces to ensure that they are in compliance by completing system performance and loads as well as a complete smoke test prior to go live. Please refer to Section 3.10.2.6 Testing for Functional Test Execution Methodology.

Performance Test: For each test, Team CNSI works with DPHHS in the planning and construction of the test cases that are used to verify performance and load requirements are met. Team CNSI maintains responsibility for performance testing and may request information from DPHHS to ensure that the test cases represent the most realistic view possible of legacy system operations. We recognize that some information may not be readily available from DPHHS or its legacy MMIS provider due to the limited availability of system profiling tools or expertise. In such cases, Team CNSI works collaboratively with DPHHS to make a reasonable approximation based on data that is available.

Performance tests are designed to verify requirements that specify the need for the system to complete user-initiated operations and return control to the user within a specified period. This measurement is commonly referred to as response time and is a part of the SLAs provided by DPHHS.

All response times are based on the normal system user load distribution encountered during normal business hours. To design the test to simulate production system usage, additional parameters are obtained through a combination of collaborative design sessions with DPHHS and capturing additional production profile data from the legacy MMIS, when available. Some of this additional data include:

- Selecting screens and transactions to be used in the test
- Mixing operations between Record Search, Screen Edit, and Next Screen actions
- Randomizing lookup criteria to ensure realistic performance scenarios
- Providing think times between user actions

Team CNSI works with the State to design and construct a user profile to verify that performance requirements are met. Figure 3.10.2-66 represents sample user profiles that could be used for the design and development of Performance test cases.

Business Area	Number of Concurrent Users Using the Business Area	Number of Users Performing Inquiries	Number of Users Updating
Provider Management	288	54	234

Figure 3.10.2-66. Sample User Profile for Performance Testing. Team CNSI will work with the State to construct a user profile to verify that performance requirements are met.

After determining the user profile, Team CNSI selects the appropriate test cases and use cases to develops automation scripts and data pools to generate the response time tests.

Load Tests

One of the final layers of testing is the Load test. These tests are executed in parallel with UAT in a dedicated environment to ensure that the required performance characteristics of the MT PSM solution have been met. As with all test activities, Team CNSI begins the process by preparing the Test Strategy and Plan. This plan outlines all test activities and processes necessary to complete these tests.

Load requirements are commonly classified as non-functional requirements and differ greatly from the functional gaps being tested in the System test and UAT. Testing non-functional requirements uses different test tools, techniques, and verification methods than those used for testing of functional requirements. Load tests provide the computing environment necessary for performance tuning. Team CNSI uses this test layer to establish baseline sizing and benchmarks for use in planning for future growth requirements. Team CNSI will perform a load test and provide the results as called out in the Operational Readiness Review checklist.

Interface Readiness

Interface testing is a critical element to a successful implementation. The goal of Interface testing is to verify a successful transfer of data to entities external to the MT PSM solution and verify that the data are properly interpreted by the receiving system. Team CNSI understands the complexities of interface testing. Team CNSI work collaboratively with DPHHS to engage the external partner agencies and establish an approach for completing Interface testing prior to the start of operations and the activity will be called out as part of the Operational Readiness Review Checklist.

Some of the key considerations for the interface pre-go-live test include:

- Identify key parties to complete the test activities for external interfaces
- Determine the availability of both human and computing resources for Testing
- Identify the sequence of testing to be completed
- Coordinate common data that may be required to successfully complete the test
- Verify network connectivity has been established prior to conducting any test activities
- Testing each interface completely, exercising all message protocols and responses, and capturing evidence of testing to include the files and messages used in testing, the operational reports, and the error messages and measures
- Testing each interface to verify the data generation (outbound), transmission, and processing (inbound) can be completed per the design of the PMIS as configured for MT PSM solution

Figure 3.10.2-67 shows the common elements in each interface. During Interface testing, Team CNSI tests these common elements to ensure that they perform as expected.

Common Element	Description
Event Trigger Handling	Events to trigger interface processes (i.e., When an event occurs, the trigger for the interface is tripped, and a response is initiated.)
Validating	Routines to validate the interface data and protocol structure and to ensure that they meet expected content and structure
Logging	Routines to record critical events and activities for the interface
Reporting	Routines to collect statistical information for reporting (e.g., number of times an interface is used, total number of errors, total amount of data transmitted)
Process Managing	Routines to start and stop external programs that are used as part of the interface specification (e.g., secure File Transfer Protocol (FTP))
Error Handling	Routines to handle error conditions (e.g., logging the error condition and repeating a request for information when a timeout occurs)
Status Monitoring	Routines to continuously monitor the status of an interface connection

Figure 3.10.2-67. Common Elements of Interface Testing. These common elements have become part of Team CNSI's repeatable standard Interface testing process.

Interface testing is considered complete when Team CNSI has executed the identified interface test cases and validated the following with the external interface owners:

- An outbound interface was exercised as far as the successful transmission of data, form, and content to the external interface owner
- An inbound interface was exercised as far as the successful receipt and processing of data transmitted by the external interface owner

Smoke Test

The Smoke test is a smaller subset of the Regression tests executed as part of the Configuration Management (CM) delivery process to ensure that the delivery of software to any environment is successful and that the software is functional. Team CNSI conducts Smoke testing using a library of test scripts that are both manual and automated. The test cases executed as a part of Smoke test validate the touch point between the various modules to make sure the integration is intact and communication between the modules are perfect.

Architecture, Technical, and Security Compliance

Team CNSI's proposed solution is hosted in Oracle's FedRAMP and HIPAA compliant Government Cloud. This hosting platform has all the cloud features in-built to support any future expansion based on workloads.

For security and regulatory compliance, the hosting platform is flexible enough to integrate with other solutions that can be installed on a temporary or permanent basis. Team CNSI's hosting platform allows IT resources (infrastructure components), that are of the same type, to be added or removed quickly. This flexibility is because all infrastructure components are either built using Platform as a Service (PaaS) services, Infrastructure as a Service (IaaS) services or Software as a Service (SaaS) services, thereby creating a highly flexible and elastic environment. Additional PaaS or IaaS services in Team CNSI's private cloud can be subscribed to or cancelled, on an ad hoc basis, using the "Pay as you go" subscription model. Please refer to Section 3.10.1.3 Hosting and Environments for more details on hosting.

Team CNSI's system is also built on a multi-layered security approach that protects the backend client data from unauthorized access. Team CNSI's FedRAMP and HIPAA compliant Data Centers perform annual audits to comply and achieve certification with Statements on Standards for Attestation Engagements/Service Organization Control (SSAE/SOC) and HIPAA standards. All these certifications will remain in place for the duration of the contract and Team CNSI can provide DPHHS with the most recent version of compliance certificates and audit reports. The following certifications are in place to provide for the confidentiality, integrity, and availability of the information systems:

- SSAE 16 SOC 1 Type II
- SSAE 16 SOC 2 Type II
- HIPAA/HITECH
- Federal Risk and Authorization Management Program (FedRAMP)

Additionally, Team CNSI's proposed solution includes security and privacy controls that are compliant with the most current version of the CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E) and National Institute of Standards and Technology (NIST) standards. Team CNSI's proposed solution adheres to the following security standards:

- Federal Information Security Management Act (FISMA)
- Internal Revenue System (IRS) Publication 1075
- Patient Protection and Affordable Care Act (PPACA) or (ACA)
- NIST Special Publication 800-66 Revision 1
- NIST Special Publications 800-53 and 800-53A
- NIST Special Publication 800-47
- NIST Special Publication 800-88 Revision 1
- NIST Special Publication 800-111

IA04

The Contractor shall provide Operational Readiness test results demonstrating that the solution meets all Service Level Agreements for system performance as defined in the scope of work.

Team CNSI uses ITIL best practices and processes in our approach to service validation testing and operational readiness, as well as iVision360 methodologies to ensure strong quality management and a solid testing approach to ensure performance standards are met. To ensure operational readiness, Team CNSI will call out readiness test activities in the Operational Readiness Review Checklist and provide test results for each test milestone. Please refer to section 3.10.2.6 Testing for testing details and results and 3.10.8 Performance Standards, SLA 15 for determining overall production readiness.

Team CNSI will store all the system testing, integration testing, end-to-end testing, regression testing, and performance/load testing test cases and test results in SharePoint. DPHHS resources or their designee will be provided access to the SharePoint to access all the test cases, test scripts, and test results. Since the Test Results Report is a formal deliverable, DPHHS reviews and approves it as a part of the MT PSM project execution. DPHHS can store their UAT Plan and test cases and test results in SharePoint as well. DPHHS will also have access to Jira to review Team CNSI's testing issues or defects to reconcile the Test Results Report defects and the defects logged in Jira.

Team CNSI will create the following mentioned detailed test reports.

- System Test, including Integration/End-to-End Test Report

- Performance Test Report
- Regression Test Report
- Each of the above test reports will have an Appendix with traceability matrix which will trace each Design Use Case to the test case and the test result.

System Non-functional Testing

Along with the Functional test results, Team CNSI will provide test results for performance load and stress testing to ensure that the evoBrix PMIS Solution meets performance and system service level requirements and is ready for operations. Non-functional testing requirements differ greatly from the functional requirements being tested in the system integration and UAT phases. Testing non-functional requirements uses different tools, techniques, and verification methods than those used for testing of functional requirements. After each test milestone results are presented to DPHHS for review and approval as part of steps defined in the Operational Readiness Checklist. Figure 3.10.2-68 provides an overview of how each of the capacity requirements will be validated. Refer to Section 3.10.2.6 Testing and Section 3.10.8 Performance Standards, for more detail on Team CNSI's testing strategy and Performance Standards.

Type	Description	Test Methodology/Tool
Performance Testing	Production Capacity – Refers to the need to test and demonstrate that the evoBrix PMIS Solution will maintain its demonstrated performance, including response times, throughput, and integrity as volume scales up and down. The State expects that the capability of the evoBrix PMIS Solution far exceeds the actual production demands placed on it by the State's historic and projected volumes.	Team CNSI proprietary capacity test framework
Load and Stress Testing	Peak Query Volume – Refers to the need to test and demonstrate the ability of the evoBrix PMIS Solution to handle larger query volumes and prioritize queries.	Automated Testing and Profiling
Load Testing	File Sizes – Refers to the need to ensure, via tests and demonstrations, that the evoBrix PMIS Solution handles files of size; including very small files and very large files (i.e., files in the gigabyte size and larger and files smaller than 1 kilobyte).	Manual Test Cases
Load Testing	Throughput – Refers to the need to test and demonstrate that the throughput of the evoBrix PMIS Solution is not impacted negatively by scaling volumes, processing, or any other function within the evoBrix PMIS Solution. The term throughput in this requirement refers to all aspects of evoBrix PMIS Solution functionality, in addition to throughput constraints of network and hardware components of the evoBrix PMIS Solution.	Automated Testing and Profiling Team CNSI proprietary capacity test framework
Stress Testing	Volume Integrity – Refers to the need to ensure, via tests and demonstrations, that as volume scales up and down, the integrity of the evoBrix PMIS Solution is maintained, and that components of the evoBrix PMIS Solution do not fail when volume is at its peak.	Automated Testing and Profiling Team CNSI proprietary capacity test framework
Performance Testing	System Availability – Refers to the need to ensure, via tests and demonstrations, that the evoBrix PMIS Solution is reliable and will remain available for operations even if one or more components fails. This is accomplished via load balanced systems or fault tolerant architectures.	Operations demonstration

Figure 3.10.2-68. Capacity Testing. Team CNSI will use a variety of testing methods and tools to validate non-functional capacity requirements have been met.

Team CNSI works with DPHHS during the design and construction of test cases and methods to verify that non-functional testing requirements are met. We request information from DPHHS to ensure that the tests designed for non-functional testing represent as realistic a view of the production system as possible. It is recognized that some information may not be readily available from the legacy MMIS due to the limited availability of system profiling tools or expertise. Furthermore, if the legacy system architectures are radically different, the data collected may not map well to the evoBrix PMIS Solution system

architecture. In such cases, Team CNSI works collaboratively with DPHHS to make a reasonable approximation based on data that is available.

Non-functional testing also provides the opportunity to reconfigure components and features of the system to maximize its overall throughput. Unlike functional tests that simply pass or fail, capacity tests will often be repeated against revised configurations until they achieve the best possible performance above and beyond the requirements or until the test fails to determine the point at which the system can no longer handle additional load. Our approach to non-functional tests takes advantage of this opportunity to optimize the system configuration in addition to meeting the State's non-functional requirements. Having determined the optimal configurations, the same conditions used to successfully meet the non-functional capacity requirements will be applied to the production systems.

Problems identified during non-functional testing that require changes to software components, configurations, or hardware configurations, developed by Team CNSI, will follow the same process for analysis, correction, retest, and regression testing.

IA05

The Contractor shall conduct an Operational Readiness Walkthrough with the Department to validate the operational readiness of the Contractor, the solution, and the Department. The Department must formally sign off on the Operational Readiness Checklist prior to proceeding to implementation.

While the preparation and ongoing readiness activities start during the implementation phase, we begin the readiness assessment 90 days prior to the go-live date and include two additional planned checkpoints, one each at 60 and 30 days prior to the planned go-live date. The checkpoints include discussion on status of work and whether the project can proceed as scheduled (go/no go). Theses checkpoints ensure milestones are achieved and the system is ready so DPHHS can provide formal final sign-off on the Operational Readiness Review Checklist prior to implementation. For streamlined and rapid communications, there will be joint daily meetings with Team CNSI, MT PSM, external interface partners, and stakeholders from the 30-day checkpoint to the go-live date. These daily meetings help keep all parties current on the progress of implementation activities and help expedite the decision to move from implementation to production cut-over.

Figure 3.10.2-69 shows the decision timeline for each checkpoint.

Checkpoint	Assessment Start	Decision
90 days prior to go-live	At 90 days prior to go-live (or next business day if it is a weekend or holiday)	Walkthrough 3 business days after the Assessment start
60 days prior to go-live	At 60 days (or next business day if it is a weekend or holiday) prior to go-live	Walkthrough 3 business days after the Assessment start
30 days prior to go-live	2 business days ahead of 30 days prior to go-live	Walkthrough 30 days prior to go-live or the next business day

Figure 3.10.2-69. Implementation Checkpoints. Team CNSI schedules checkpoints on regular intervals to support successful implementation.

At each checkpoint, Team CNSI and DPHHS PMOs examine the Operational Readiness Review Checklist and additional supporting checklist(s) and thresholds presented in the metrics to determine if the implementation can:

- Proceed as planned, and no remediation is needed
- Remediation required

Team CNSI recommends joint daily meetings two weeks prior the go-live date, so that State staff members are kept up-to-date with the most recent progress across all of the parties with responsibility for operational readiness. Team CNSI and the State implementation leads will lead these daily meetings with the support of the project management team from the State and Team CNSI and other involved entities.

The additional checklists are included as part of the plan to transition from implementation to operations, and Team CNSI collaboratively finalizes the metrics for each of the readiness areas for which they are responsible as part of the implementation planning process.

Readiness checklists concentrates on four core areas:

- **Organizational readiness:** Ensuring that the State and operational teams are trained on their jobs, have appropriate documentation and procedures for their role, and, when possible, have had an opportunity to practice those procedures. Team CNSI onboard support staff required to operate the system well in advance of the go-live date. Team CNSI ensures that the team members who will be responsible for running the system are trained to do so – that they have been trained in the processes and procedures, have documentation of both the system and processes, and an understanding of the system's day-to-day lifecycle.
- **User readiness:** Ensuring the users (Team CNSI staff, business operations staff, providers, and the State) have been trained and supplied documentation on how the system functions, and thereby know how to use the system, and that they know how to contact help when they need it.
- **System readiness:** Confirming that the system has been fully tested both functionally and for performance. Team CNSI ensures system readiness via two mechanisms. First, applying robust performance, stress, and load testing processes to verify the completed production infrastructure will fully meet and exceed the needs of the deployed evoBrix PMIS Solution. Secondly, by applying rigorous software testing across the entire system, end-to-end.
- **Operations readiness:** Confirming that the facilities and infrastructure are ready (e.g., phones on desks and functioning correctly, system connectivity established from the desktops), as well as ensuring that the operations processes and procedures are in place. Team CNSI also ensures operational readiness by testing the disaster recovery process, verifying system performance monitoring and alerting components are in place, and confirming the business facility is ready for production.

IA06

The Contractor shall develop Operational Readiness Review Checklists (ORR) that will examine the actual solution characteristics and the procedures of the product's operation to ensure that all hardware, software, resources, procedures, and user documentation accurately reflect the deployed state of the system.

In the final months leading up to system cutover and implementation, Team CNSI will assemble the Operational Readiness Review (ORR) checklists which identify each task, the owner, the readiness area, and the date by which it must be completed. These checklists are then used to manage overall implementation readiness, including producing metrics at each readiness gate for the percentage of work complete versus percentage of work expected to be complete. At each readiness gate, a meeting is held with the State to report readiness metrics and to review any outstanding items. The checklist will examine the actual solution characteristics and the procedures of the product's operation to ensure that all

hardware, software, resources, procedures, and user documentation accurately reflect the deployed state of the system.

Alongside the readiness checklists, Team CNSI includes detailed cutover tasks as part of the solution implementation and transition to operations plan. This artifact provides information concerning when legacy systems and operations processes terminate and when corresponding processes in the new system begin.

When, at the final readiness checkpoint, all checklists are showing "green," meaning ready for operations, then approval to continue with the cutover and assume operations is granted and the final countdown to go-live starts.

In preparation for go-live, Team CNSI and the DPHHS plan coverage for the final days of cutover and the first few days following go-live.

Team CNSI utilizes an ongoing systems operations group that consists of team leads representing the business, functional, and system areas. This team is the hub for incident management and reporting across the system, including defect tracking and management, test management, and release management. Similarly, the business operations team meets to assess the transition activities during cutover and works with the systems team to address concerns and ensure implementation is as smooth as possible. As the system stabilizes, they meet less frequently, arriving at a final interval of weekly.

Additionally, a core team of DPHHS and Team CNSI management and program representatives are assembled to ensure availability for any issues encountered during implementation. If issues are encountered, the key leads for the impacted area report to the joint State and Team CNSI management team with details so that the joint team can quickly determine next steps, communication, and other activities, as necessary. As issues become less common, typically within the first few days, if not hours, this team resumes their normal roles and the operations group manages day-to-day events, escalating to the core management team as necessary.

As the transition to operations is carried out, the PMO begins to support ongoing operational support functions including change management. This minimizes the volume of procedural changes to be absorbed at go-live, ensures continuity, and ensures that future changes and product priorities are captured and tracked. This process continuity also allows staff familiar with the environment to continue to transition into the next phase of the life cycle.

3.10.3 Certification

The Contractor must work with DPHHS and other contractors as necessary to ensure that all solutions provided by the Contractor meet requirements specified in the Mechanized Claims Processing and Information Retrieval Systems (90/10) Final Rule (CMS 2392-F) and relevant federal certification requirements as described in the most current version of the MECT Toolkit available at https://www.medicaid.gov/medicaid-chip-program-information/by-topics/data-and-systems/mect.html.

The Contractor will be responsible for providing and maintaining a solution that meets all applicable checklist items in the most current version of the Medicaid Enterprise Certification Toolkit (MECT), and supporting the review and validation of those items by the Department, IV&V Contractor, and CMS. The Contractor must become knowledgeable of all MECT-related items associated with the solution offered. The MECT Mapping document, found as Attachment D, contains the most current version of the MECT checklist items applicable to the Contractor's scope of work, mapped to the associated business requirements.

The Contractor must provide staff and other resources to support and to participate in MECT milestone reviews and other Certification activities that occur before, during and after implementation of the proposed solution(s). The Offeror must describe their approach to meet each of the Certification requirements defined in Attachment F, Requirements Matrix.

The Team CNSI Advantage

The evoBrix PMIS solution and implementation methodology has been built with the goal of certification in mind.

- Reuses previously certified evoBrix module components
- Leverages knowledge from previous successful certifications
- Allows early identification of checklist requirements in Solution Analysis
- Allows early remediation of potential gaps in Solution Modeling
- Facilitates early and ongoing collaboration with IV&V vendor to populate certification checklists and complete the steps in the MECL from MECT 2.2

MTPSM-3-124

System certification from CMS is one of the highest priorities for Team CNSI because we understand that it is essential to realize the Federal matching funds needed to complete other program objectives. Implementing the evoBrix PMIS solution that has been previously certified reduces DPHHS' risk for obtaining certification and facilitates the shortest path toward certification. Our experience obtaining system certification on the first pass with no findings in both Washington and Michigan has allowed us to refine our approach into a proactive and effective process for meeting the requirements of the Medicaid Enterprise Certification Toolkit (MECT). We understand what is needed to certify a system because we have gone through the process ourselves. When we implement, we expect the MT PSM solution to be certified as soon as possible after the required six months of operation is met because we prepare throughout the life cycle of the project. Our preparation, tangible experience on actual certification teams, as well as providing the evoBrix PMIS base module that has been previously certified by CMS in Michigan greatly reduces risk of not obtaining matching funds when the system is finally implemented.

To ensure success, Team CNSI will create a Certification Plan based upon guidance from the current version of the MECT version 2.2 and the guidance provided in the Medicaid Enterprise Certification Lifecycle (MECL). The MECL defines the roles each stakeholder is expected to play.

Team CNSI's unique SCI methodology, as detailed in Section 3.10.2.2 of our proposal response, reduces DPHHS' certification risks by providing:

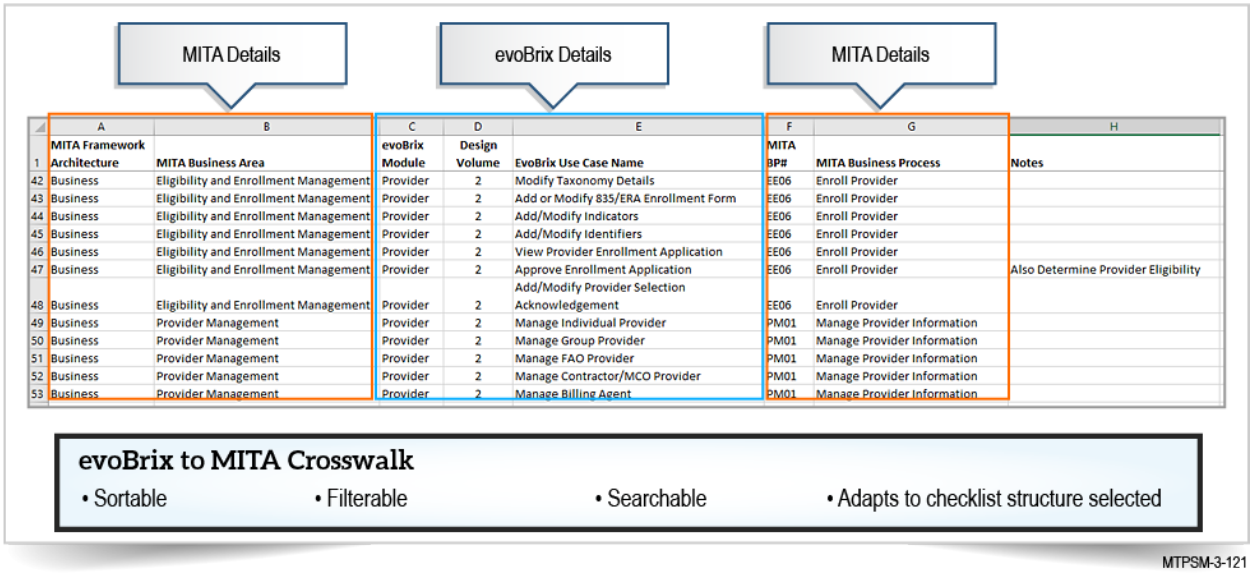
- Tracking and status reporting of system and business operations certification preparation activities from start to finish
- Early collaboration with the IV&V vendor to capture certification readiness status using our evoBrix to Medicaid Information Technology Architecture (MITA) crosswalk
- Early identification of possible certification gaps through Solution Analysis
- Early remediation of certification gaps during Solution Modeling
- Training in certification data collection activities, and use of the electronic certification data collection repository, necessary after production implementation
- Examples of CMS certification checklist responses and related validated documentation from our other successful certification activities

In the period of operations leading up to the CMS Certification Review Meeting, Team CNSI will support or manage certification and data collection activities as requested by the state. Based on progress toward meeting certification requirements, we will advise DPHHS and IV&V of the earliest possible time to request certification. We will provide DPHHS with the content to be included in their Certification Review Request letter upon request.

Once the Certification Review Meeting date is set, Team CNSI will provide logistics services for the meetings. Throughout the Certification Review Meetings, Team CNSI will provide the technical and/or business operations personnel and/or support needed.

Team CNSI's certification lead will be the central point of contact for DPHHS, its IV&V vendor, and other organizations that will be involved in the certification effort.

Team CNSI's certification efforts begin early in the project and are based on the experiences and lessons learned in prior certification events. One positive lesson learned is that to minimize risk, we provide a traceability crosswalk between the evoBrix solution modules and the MITA at the beginning of the Implementation phase of the project. A sample of the evoBrix to MITA functional crosswalk is shown in Figure 3.10.3-1.



	A	B	C	D	E	F	G	H
1	MITA Framework Architecture	MITA Business Area	evoBrix Module	Design Volume	evoBrix Use Case Name	MITA BP#	MITA Business Process	Notes
42	Business	Eligibility and Enrollment Management	Provider	2	Modify Taxonomy Details	EE06	Enroll Provider	
43	Business	Eligibility and Enrollment Management	Provider	2	Add or Modify 835/ERA Enrollment Form	EE06	Enroll Provider	
44	Business	Eligibility and Enrollment Management	Provider	2	Add/Modify Indicators	EE06	Enroll Provider	
45	Business	Eligibility and Enrollment Management	Provider	2	Add/Modify Identifiers	EE06	Enroll Provider	
46	Business	Eligibility and Enrollment Management	Provider	2	View Provider Enrollment Application	EE06	Enroll Provider	
47	Business	Eligibility and Enrollment Management	Provider	2	Approve Enrollment Application	EE06	Enroll Provider	Also Determine Provider Eligibility
48	Business	Eligibility and Enrollment Management	Provider	2	Add/Modify Provider Selection Acknowledgement	EE06	Enroll Provider	
49	Business	Provider Management	Provider	2	Manage Individual Provider	PM01	Manage Provider Information	
50	Business	Provider Management	Provider	2	Manage Group Provider	PM01	Manage Provider Information	
51	Business	Provider Management	Provider	2	Manage FAO Provider	PM01	Manage Provider Information	
52	Business	Provider Management	Provider	2	Manage Contractor/MCO Provider	PM01	Manage Provider Information	
53	Business	Provider Management	Provider	2	Manage Billing Agent	PM01	Manage Provider Information	

Figure 3.10.3-1. Sample of evoBrix to MITA Crosswalk. Team CNSI's evoBrix to MITA crosswalk provides the details necessary to identify where each piece of the MITA Architecture is met.

The evoBrix to MITA crosswalk allows DPHHS to begin the project with an understanding of how Team CNSI's PMIS solution aligns with certification checklists. The evoBrix to MITA crosswalk enables DPHHS to use their preferred certification checklist format, either the MITA checklist format or the Module checklist format.

CMS certification is achieved through the combination of business processes enabled by system features that together provide the complete picture needed for CMS to certify the MT PSM solution. Team CNSI's evoBrix solution provides the technology to continue to provide award-winning service to achieve CMS certification.

CERT01

The Contractor shall develop a Certification Crosswalk that describes how the Contractor's deliverables and other documentation align with federal certification requirements and MECT milestone reviews.

The Medicaid Enterprise Certification Life Cycle (located in MECT 2.2) provides specific and detailed guidance to states by defining a workflow which is composed of four phases containing 27 major

activities to be completed by CMS (Central and Regional offices), the State (PMO and Contractors), and an IV&V contractor. This workflow is intended to be completed in parallel with the system development life cycle used by the project as identified in the Project Management Plan.

Team CNSI will develop a comprehensive Certification Plan that aligns stakeholders with the activities required to complete the certification life cycle specified by CMS in the MECL as efficiently as possible. The artifacts and deliverables required for certification are identified in Appendix B of the MECT. As part of the planning process, Team CNSI will map a crosswalk from the required artifacts in Appendix B to the project's deliverables and documentation in accordance with the milestone review requirements in Appendix B.

The following is an example Certification Plan used by Team CNSI in the past which represents how we would provide a road map and logistics to follow the MECT certification workflow with associated deliverables in parallel with the project life cycle. A sample of Certification Plan outline is shown in Figure 3.10.3-2.

Table of Contents

1. Introduction 1
1.1 Document Purpose 1
1.2 Document Organization 1
1.3 Reference to Other Documents 2
1.4 Audience 2
2. Certification Overview and Assumptions 7
2.1 Certification Definition 7
2.2 Relationship between Certification Plan and MECT 8
2.3 Roles and Responsibilities 8
3. Certification Approach and Methodology 9
3.1 Draft and Final Certification Plan 9
3.2 The Process 9
3.2.1 Initial Assessment 9
3.2.1.1 Identification of SCI Certification Stakeholders 9
3.2.1.2 CHAMPS to MITA Crosswalk Evaluation 10
3.2.1.3 Initiating Preemptive Remedation for SCI Phase 11
3.2.2 Activities During SCI 12
3.2.2.1 Managing Crosswalk Updates 12
3.2.2.2 Managing Certification Checklist Reevaluation 13
3.2.2.3 Pre-implementation Certification Readiness Review 14
3.2.2.4 Establish the Certification Evidence Repository 15
3.2.3 Preparation for formal Certification Request 16
3.2.3.1 Identify Critical Success Factors 16
3.2.3.2 Commission Certification Team 17
3.2.3.3 Construct Initial Certification Schedule 17
3.2.3.4 Conduct Certification Team Orienation 18
3.2.3.5 Data Collection, and Monitoring 18
3.2.3.6 Perform Periodic Progress Reporting 19
3.2.3.7 Conduct Certification Readiness Review 19
3.3 Request to CMS for Certification Review 20
3.4 Review Preparation 20
3.5 CMS Certification Review 21
3.6 Certification Disposition 22
3.6.1 Potential Remediation Activity 22
3.6.2 Final Certification Disposition 22
4. Appendices 23
4.1 Appendix A – Acronyms and Terms 23
4.2 Appendix B – Deliverable Acceptance Criteria 24

MTPSM-3-122

Figure 3.10.3-2. Sample Certification Plan. Team CNSI's approach is proven and provides an effective, efficient path toward the earliest possible certification of the system.

CERT02

The Contractor shall complete quarterly and milestone updates of the CMS Certification Checklists as requested by the State.

Team CNSI will complete all the quarterly and milestone updates of the certification checklists as required. Certain Team CNSI deliverables will be developed with Certification in view so that they are prepared to fulfill the intended requirement for Certification. Team CNSI will include this activity in the comprehensive Certification Plan that is intended to align stakeholders with the activities required to complete the certification life cycle specified by CMS in the MECL as efficiently as possible.

CERT03

The Contractor shall validate the system against the CMS Certification Checklists

Team CNSI will validate the system against applicable CMS Certification Checklist criteria. We understand that the checklist criteria form a major portion of the core requirements for the system certification component. Team CNSI's certification efforts begin early in the project and are based on the experiences and lessons learned in prior certification events. As a result, we emphasize early collaboration with the IV&V vendor to capture certification readiness status using our evoBrix to MITA functional crosswalk, early identification of possible certification gaps through Solution Analysis, and early remediation of certification gaps during Solution Modeling.

Ultimately, CMS certification is achieved through the combination of business processes enabled by system features that together provide the complete picture needed for CMS to certify the MT PSM solution. Team CNSI will validate system related certification checklist items against the system to ensure compliance and work with DPHHS or their representatives to support completion of non-system related checklist requirements.

CERT04

The Contractor shall contribute to the quarterly IV&V certification reports.

Team CNSI is prepared to forge a strong working relationship with the IV&V vendor to ensure successful certification as early as possible and will work collaboratively with the IV&V vendor to establish clear expectations and roles to ensure all efforts are synchronized. As such, Team CNSI will contribute relevant information required to complete the quarterly IV&V certification reports to CMS. Team CNSI's certification lead will be the central point of contact for DPHHS, its IV&V vendor, and other organizations that will be involved in the certification effort.

CERT05

The Contractor shall provide staff resources to support MECT milestone review and certification activities including participating in planning activities, meetings and other activities as required by CMS.

Team CNSI will establish a certification lead to be the central point of contact for DPHHS, its IV&V vendor, and other organizations that will be involved in the certification effort. The certification lead will coordinate other Team CNSI members as required who will begin the project already prepared to support MECT milestone reviews, certification planning activities, meetings, and activities required by CMS based upon MECT 2.2. Team CNSI supports the project certification lead by engaging other resources, with both technical and functional expertise, to support checklists item completion. The certification lead will also consult with certification subject matter experts within the company to provide the project with the all the support necessary to meet the objective of an efficient and timely certification.

CERT06

The Contractor shall assist the Agency in preparing certification artifacts, evidence and presentation materials, e.g., Requirements/ user stories and/or use cases for functional and non-functional

requirements, data, business, capacity/performance, security/privacy/HIPAA compliance, usability, maintainability, interface, 508 compliance, disaster recovery, traceability to test plans or test cases.

Team CNSI is committed to assisting DPHHS in preparation of materials to support certification. Team CNSI understands the MECL workflow as well as the required infrastructure and coordination of each resource required to complete the MECL. For this proposal, it is assumed that the first 15 activities of the MECL have been performed per CMS direction and have been completed prior to the award of the MT PSM contract. At award, CNSI will immediately perform a review of the status of activities 1-15 in the MECL to determine if there are any gaps that need to be remediated, and work with the State and the IV&V contractor to ensure the project is ready to proceed to activity 16. This may include completion of certain activities and/or working with the State, IV&V contractor, and CMS to customize the activities for the MT PSM where appropriate. Assuming there are no remedial activities required, Team CNSI will develop a plan to complete the remaining MECL Activities 16 through 27. Based upon roles defined by CMS in the MECT, CNSI will develop a plan using the following approach:

- For MECL Activities 16, 21, 22, and 25, CNSI will collaborate with DPHHS to schedule and prepare all tasks required to complete the activities per the State's specifications and the MECT. This includes planning, communications, logistics, issue and action item follow-up, completion of key system documentation, coordination and completion of MMIS CSFs and supporting collection, and reviews of critical documentation identified in Appendix B of the MECT.
- For MECL Activities 17, 18, 20, 23, and 26, CNSI will work with the State's IV&V contractor to assist in the creation of their deliverables and completion of the tasks assigned to them by the State and CMS.
- For MECL Activities 19, 24, and 27, Team CNSI will perform either up front activities or the behind-the-scenes coordination, as requested, to allow the State to successfully coordinate with CMS to review status and certification requirements.

The MECL, as published in MECT 2.2, is shown in Figure 3.10.3-3.

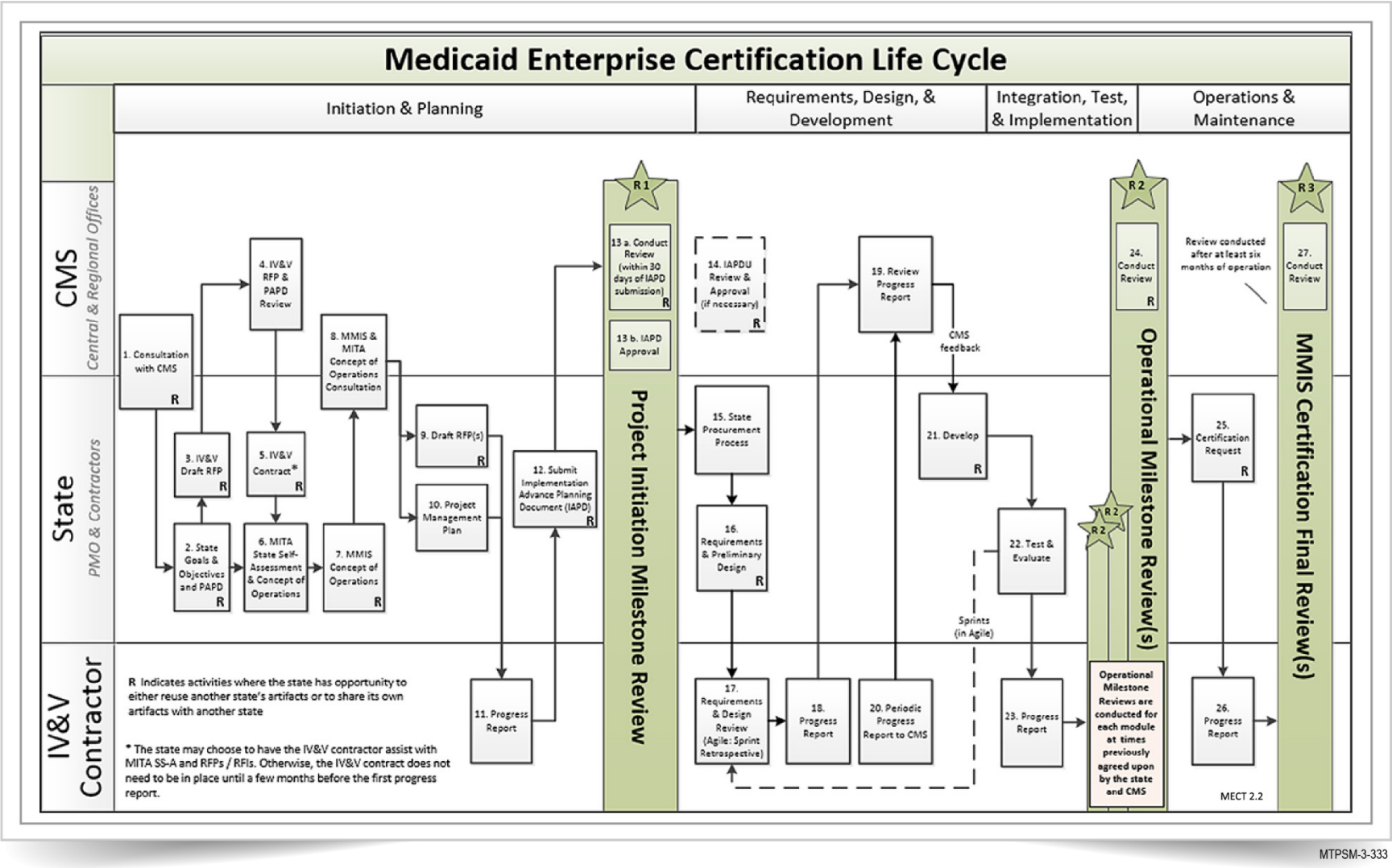


Figure 3.10.3-3. Medicaid Enterprise Certification Life Cycle (MECL). Diagram shows the MECL as published in MECT 2.2.

CERT07

The Contractor shall participate and support as needed in CMS certifications of the other modules.

Team CNSI will participate and support certification of the Medicaid enterprise and work collaboratively with all vendors where requirements overlap with the scope of work included in the MT PSM solution. Team CNSI has historically enjoyed strong relationships with other vendors in the states where they do business. We recognize that collaboration and mutual respect increase everyone's potential for success and strive to bring that culture to bare on all our engagements.

CERT08

The Contractor shall expeditiously correct, all required remediation activities related to certification findings on a schedule to be approved by CMS and the State.

Team CNSI understands the need to correct any findings that would inhibit achieving certification. Team CNSI approaches certification proactively to avoid any need for remediation, but as an unknown, we account for any potential remediation activates up front as part of our planning process. Then, throughout the SDLC, we seek to ensure that certification criteria are being met. When remediation is necessary, the corrective actions necessary to fix the finding receive the highest priority as early in the process as the issue can be identified. This approach has been successfully used by Team CNSI and resulted in systems in both Washington and Michigan that were certified on the first pass with no findings to correct.

CERT09

The Contractor shall use appropriate testing, configuration and change control procedures for all changes made to the solution during the certification process.

As part of Team CNSI's established process set, appropriate testing, configuration, and change management are standard operating procedures for changes to the system throughout the lifecycle of the project and maintained through operations. Changes made to the solution during the certification process will follow the same rigorous process established at the outset of the engagement. As noted under CERT08, if remediation is necessary, the corrective actions necessary to fix the finding will receive the highest priority. Reference Section 3.10.2.6 for more details regarding testing, and Section 3.10.4 for more details regarding configuration and change management.

CERT10

The Contractor shall update system, user, and training documentation as necessary to support the certification process and to reflect changes that have been made to the solution during the certification process.

Team CNSI will update system, user, and training documentation at logical, established intervals as defined in the project schedule to reflect updates and changes made to the solution throughout the solutions life cycle depending on the intended use of the document. Team CNSI will make accommodation for changes specifically required to achieve or maintain certification outside of the

normal update process as necessary. These changes will be made using change control as noted in CERT09 and with sensitivity to the need for certification requirements.

CERT11

The Contractor shall ensure system CMS Certification through correct design, implementation, documentation and certification support.

evoBrix PMIS, which forms the core of our MT PSM proposed solution, is built on the Provider Management solution certified in Michigan. This benefit provides the DPHHS with a significant advantage in terms of reduced time to validate compliance with federal requirements and realizing the associated matching funds. Based on the groundwork laid by taking advantage of a previously certified solution, significant portions of the design, implementation documentation, and certification effort can be leveraged from the previous experience.

CERT12

The Contractor shall coordinate with the State to develop CMS Certification Checklist documentation for each MECT Checklist requirement.

Team CNSI will coordinate the development of documentation, as well as the identification and collection of evidence required for each applicable MECT Checklist requirement with DPHHS.

Team CNSI understands the activities required to complete the MECL (MECT 2.2, Figure 3.10.3-3) and that a significant portion of the CMS checklist criteria are allocated to core requirements of the system components. Team CNSI will establish a Certification Plan with DPHHS to ensure that completion of each MECT checklist requirement is assigned. For this proposal, the MECL assumes that first 15 activities are performed prior to the arrival of the solutions provider, therefore, at award, Team CNSI will perform a review of the status of activities 1-15 in the MECL to determine if there are any gaps that need to be remediated. Assuming there are no gaps, Team CNSI will develop a plan to complete the remaining Activities 16 through 27 in accordance with the guidance provided by CMS and direction of the State as follows:

- For MECL Activities 16, 21, 22, and 25, CNSI will collaborate with DPHHS to schedule and prepare all tasks required to complete the activities per the State's specifications and the MECT. This includes planning, communications, logistics, issue and action item follow-up, completion of key system documentation, coordination and completion of MMIS Critical Success Factors (CSFs) and supporting collection, and reviews of critical documentation identified in Appendix B of the MECT.
- For MECL Activities 17, 18, 20, 23, and 26, CNSI will work with the State's IV&V contractor to assist in the creation of their deliverables to the State and CMS.
- For MECL Activities 19, 24, and 27, CNSI will perform the behind the scenes coordination to allow the State to successfully coordinate with CMS to review status and certification requirements.

CERT14

The Contractor shall populate the certification document repository, as each required item/artifact is completed and approved.

Team CNSI has previous experience organizing and leading certification efforts. The certification document repository should be set up with careful consideration for its intended use. Since certain evidence for certification may be protected under HIPAA rules, Team CNSI will work with DPHHS to establish guidelines around access and usage to ensure that the repository is set up for long term use and facilitate CMS reviews. Team CNSI will follow the procedures for populating the repository as artifacts needed for certification are finalized and approved. The policy and procedures governing the use of the Certification repository should be completed with the Certification Plan.

CERT16

The Contractor shall present at milestone reviews and other certification meetings as directed by the State.

Team CNSI will present at milestone reviews and other certification meetings as directed by the State.

3.10.4 Operations, Maintenance, and Configuration

The Contractor shall provide Operations support, Maintenance, and ongoing Configuration of the provided Solution(s) throughout the life of the Contract. This includes providing Operations support as described in the scope of work as well as providing Maintenance and Enhancements to the provided Solution(s). The Contractor will follow project management and system development processes throughout the life of the Contract.

Team CNSI's Operations, Maintenance, and Configuration strategy is designed to effectively and efficiently conduct system operations to enable DPHHS to achieve its goals and objectives. Team CNSI continually focuses on strategy by looking at the big picture, monitoring usage trends and alignment to goals and objectives. We carefully considered how our ITIL-based strategy can meet DPHHS objectives such as "increase DPHHS agility by increasing the speed with which routine changes can be made," "increase the use of business measurements consistent with Medicaid Information Technology Architecture (MITA)," and "improve consistency of application of program requirements." In reviewing these objectives, three key phrases stood out: agility, business measurements, and consistency. Hence, we selected the following three elements as the central themes of our ITIL-based operations management strategy to align with DPHHS objectives and to consistently deliver our services:



- **Agility.** The ability to respond rapidly to change is a necessity for today's programs. It enables us to *collaborate* more effectively with DPHHS and other vendors. Team CNSI's operations management processes are designed to be nimble and responsive in order to better deliver operations phase services for DPHHS. Agility is woven into all aspects of our operations**.**
- **Metrics-driven approach**. Team CNSI establishes SLAs and other metrics to implement quantitative managed techniques as a part of our ITIL continuous improvement activities. Our metrics strategy is also about monitoring performance measures, which are aligned to MITA business processes through HealthBeat and other operations monitoring tools and reports. Focusing on metrics enables Team CNSI to make data-driven decisions and be accountable for our performance. Near real-time

operational and SLA dashboards are made available using our HealthBeat system to Team CNSI leadership as well as DPHHS. The insight, visibility, and *transparency* resulting from our approach are key ingredients to establishing trust between our organizations and DPHHS.

- **Process excellence**. Team CNSI has an extensive library of process assets, procedures, best practices, and templates to implement our operations management strategy and subsequent processes. We blend the discipline of service delivery of ITILv3, and quality management systems to orchestrate and manage our activities during operations. The key benefit of our process excellence-based operations strategy is that it enables Team CNSI to streamline administration activities, enabling us to focus on outcomes.

Figure 3.10.4-1 provides a visual description of our operations management strategy. It describes our ITIL-based operations management focus areas, key elements of our strategy, and the expected results and benefits.

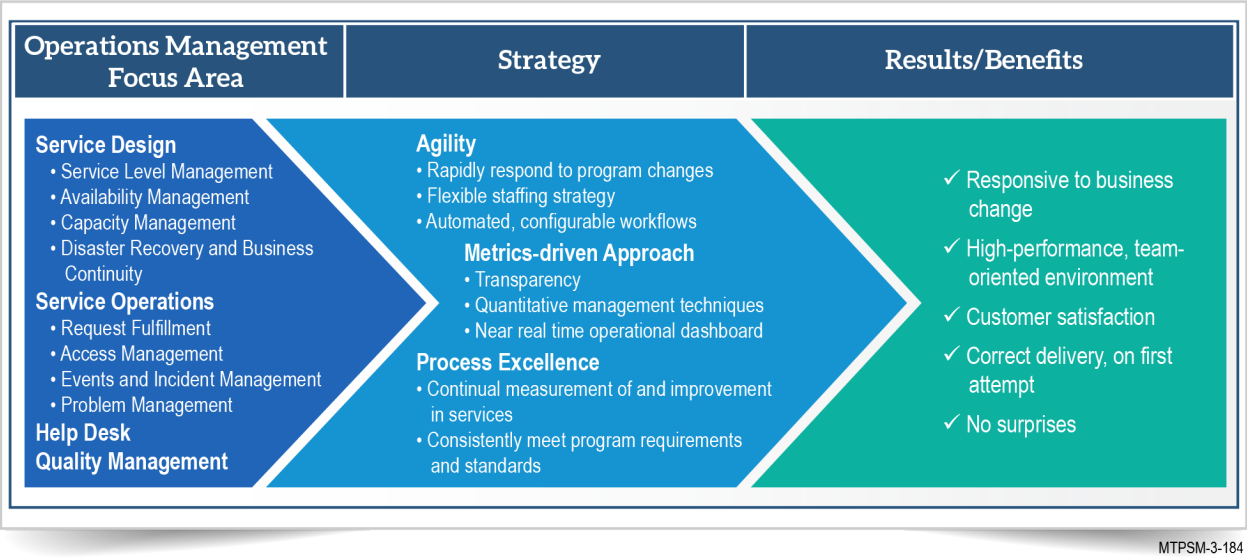


Figure 3.10.4-1. Team CNSI's Operations, Maintenance, and Configuration Strategy. Team CNSI's Operations, Maintenance, and Configuration management strategy helps DPHHS achieve goals and objectives for the Medicaid enterprise.

In designing our Operations, Maintenance, and Configuration management approach, we implemented our strategy in each of these areas:

- Service Design
  - Service Level Management
  - Availability Management
  - Capacity Management
  - Disaster Recovery and Business Continuity
- Service Operations
  - Request Fulfillment
  - Access Management
  - Events and Incident Management
  - Problem Management
  - Help Desk

Figure 3.10.4-2 describes our strategy and the results of decisions that drive our proposed operations management solution.

Operations Management Focus Area	Themes Driving Team CNSI Operations Management Strategy		
	Agility	**Metrics-Driven Approach**	**Process-Excellence**
Service Design	■ Proven SaaS process model ■ Designed for scalability and elasticity to meet SLA and capacity demands ■ Robust set of tools to monitor business, application, and infrastructure operations	■ Microsoft Project Schedule continually updated for project-based activities ■ Measures track effectiveness of business operations	■ ITIL-based DevOps processes for new or modified systems capability to support business operations ■ Focus on certification requirements ■ One formal review conducted before any new process or function is implemented ■ Well-planned and tested disaster recovery and business continuity
Service Operations	■ Responsive, flat organizational structure ■ Comprehensive operations manual ■ Continual focus on cross training staff for flexibility ■ Continually focus on "sharpening the saw" through continual training and evaluation	■ Establish measurable objectives for all operational areas ■ Daily production readiness meetings to review prior day's results versus goal against today's demands including escalations and issues ■ Each operational area establishes thresholds for green, yellow, and red flags ■ Defined contractual and management SLAs	■ Continue well-honed planning and scheduling processes from the implementation phase into operations ■ Operating procedures that are the foundation for training, production, and quality ■ Use of metrics data to monitor performance
Help Desk	■ Automated tools to auto-assign tickets to streamline workflows and eliminate manual processes ■ Continual focus on cross training staff for flexibility	■ Defined contractual and management SLAs ■ HealthBeat dashboard for near real-time view into operations	■ Multi-channel access points

Figure 3.10.4-2. Team CNSI's Operations, Maintenance, and Configuration Management Strategy. Our strategy themes are woven into all elements of operations to meet DPHHS goals and objectives.

Service Design

Team CNSI is has established robust and proven ITIL-compliant SaaS processes from implementations in Michigan, Illinois, and Utah. These processes enable a DevOps model to maximize system capability and, more importantly, productivity with business operations. IT services and new capability are designed, transitioned, and operated in a manner that avoids disruptions of system capability. A key part of ITIL involves designing processes or "services" such that changes are introduced to an operations environment in a controlled and systematic manner with a focus on Service Level Management, Availability Management, and Capacity Management.

Team CNSI's system architecture is equipped with load balancing, automatic failover, and redundancies to reduce the risk and exposure to unplanned outages. It is designed to minimize risk and ensure that DPHHS service and availability requirements are met. CNSI minimizes system maintenance periods, upon the State's approval, for major system releases, emergency system releases, and regular maintenance downtimes.

Team CNSI's extensive operational system and support infrastructure is composed of well-documented processes and procedures. Our approach is built on a combination of ITIL processes and augmented by

our own best practices refined over years of collective corporate health care administration operations experience in managing large, complex projects of similar size and complexity. A key value of aligning with ITIL involves designing services so changes are introduced to an operations environment in a controlled, low-risk manner. ITIL services represent a comprehensive set of practices, policies, procedures, and processes that enable us to focus on business and system value by providing consistent, predictable, and measurable results. SLA and performance metric reporting and management are integrated in the ITIL framework core to ensure that Team CNSI and DPHHS have the necessary visibility to monitor system performance and to provide course corrections when necessary. Refer to the Service Level Management Section below for more information.

Team CNSI's proven processes are implemented upon project initiation and throughout the Operations Phase. Our tiered approach efficiently and effectively allows Team CNSI to manage operations processes for technical, programmatic, and operational changes across the evoBrix PMIS solution. Team CNSI's support is structured into four main areas (network operations center, operations support, application services, and infrastructure support) to monitor and support the day-to-day operational activities. Together they represent a comprehensive set of practices, policies, procedures, and processes that will enable us to focus on business value by providing consistent, predictable, and measurable results.

Service Level Management

Team CNSI's evoBrix PMIS solution offers essential services to Medicaid providers and state staff. A disruption to its operations can adversely affect providers and other stakeholders. Therefore, it is critical to ensure continuous access and create a highly available infrastructure to support the business operations of the system, and to ensure that service levels are being met. Refer to Services Operations below for Event and Incident levels (OTRS Tickets).

There are three key components at the center of healthy operations that our operations staff monitor to ensure continuous operations and prevent disruption, as follows:

- Measures are designed to track effectiveness of support (e.g. ticket volumes, ticket response times)
- Application operations and health, which are measures that track performance of the application in performing the tasks for which it was built (e.g., CRM Service Request per hour)
- Infrastructure, which is made up of the hardware and software components that form the backbone of the system and support the application and business operations (e.g., the servers, the network)

Team CNSI's evoBrix platform has successfully demonstrated in production the key architectural tenets outlined in the State's vision for the evoBrix PMIS solution. The evoBrix solution architecture was conceived with the following core principles:

- J2EE technology
- Browser-based user interface
- Multi-tiered scalable architecture that is highly available, eliminates single points of failure, and enables transparent failover
- Relational databases
- Integrated evoBrix PMIS solution

Team CNSI's proposed solution is highly elastic and scalable. As the Medicaid entity grows, the system is designed for scalability and can easily have capacity added on demand. Team CNSI will work with the DPHHS to ensure sufficient capacity – based on performance requirements, user data, and transaction metrics provided by the State – for the evoBrix PMIS solution at system implementation and ongoing as proactive performance monitoring indicates is necessary and as business needs expand.

Currently, Team CNSI's system support uses a set of tools (e.g., HealthBeat, SLA Dashboard, Automation Oracle Enterprise Manager, Building Management System, and Data Center Infrastructure Management) to monitor the system and assist in the day-to-day operations activities to meet SLAs. Our quality support service provides transparency in reporting, fulfilling user requests, resolving service failures, fixing problems, and carrying out routine operational tasks.

SLA Automation Tool and Operational Performance Standards

Team CNSI's SLA automation solution provides DPHHS with configurable SLA management capabilities. It is one of the tools that allow Team CNSI and DPHHS to track and ensure that SLAs are being met. Figure 3.10.4-3 shows the SLA automation tool architecture. Our solution uses an SLA Automation Engine which is configured to automatically or manually track various SLAs related to system and business functions, such as interfaces and report generations. Our solution allows Team CNSI and DPHHS to have visibility into daily system and business functions and their corresponding SLA performance. The tool is also equipped with tracking, reporting, and management capabilities using Team CNSI's HealthBeat as the front-end application. This allows Team CNSI the necessary visibility to monitor performance and provide SLA course correction when necessary.



The SLA Automation engine runs on a configurable interval to generate service transactions based on the configured SLA's frequency schedule. The system retrieves data input from various source systems via REST or SOAP web service requests for multiple service configurations at any given time. The retrieved data – such as process start/end times and status codes – is matched to the SLA transaction based on unique criteria linked with the reference number, and automatically updated with the provided data. In the event of a non-compliant transaction, notification alert emails are generated and sent to email addresses linked to that service configuration.

Business Operations Monitoring

Indicative of Team CNSI's commitment to service and transparency, we are including HealthBeat, which provides DPHHS with configurable, automated, and real-time visibility into business operations, SLA compliance, and system monitoring. This section provides an overview of HealthBeat's business operations monitoring. HealthBeat for system monitoring is covered in detail in Availability Management, subsection Monitoring and Reporting High-Availability, below.

HealthBeat enables the setup of a hierarchy of MITA business, system, and application objectives or goals that can be linked with metrics to events and services. This will allow Team CNSI and the states using evoBrix to monitor the health of business and system processes not only in the short term but also over the long term to track historical trends. Such an approach allows Team CNSI to use real-life data in the business process configuration and ensures continuous business process improvement across all business process areas.

HealthBeat, upon contract award, comes configured with most of the SLAs identified in the Solicitation. We say most of the SLAs since many SLAs by their nature are not candidates for real-time monitoring (i.e., deliverable submissions). See Figure 3.10.4-4, SLA History View in HealthBeat. Currently, HealthBeat contains over 130 metrics and is continuously evolving to provide meaningful metrics to business operations users.

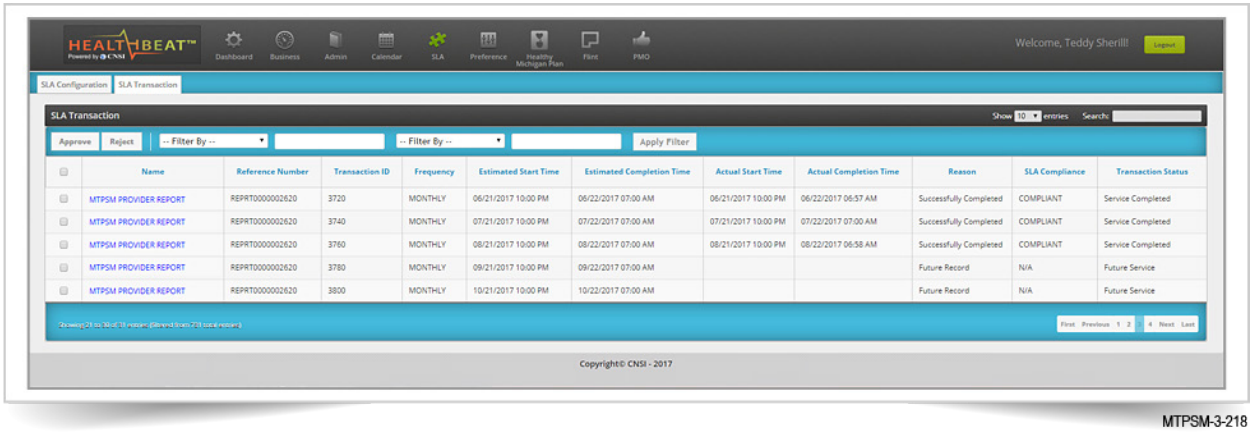


Figure 3.10.4-4. SLA History View in HealthBeat. HealthBeat provides SLA configuration, management, and monitoring capabilities for transparency of operations.

HealthBeat provides a comprehensive application activity monitoring framework along with the capability to facilitate continuous process improvement. As the system handles each process, it collects process-related data in the data store. This data is then used to display the process dashboard and provide visibility to the process metrics and the health of the operation. The system uses workflow-based analytics to provide feedback on potential bottlenecks and application performance issues. Thresholds are configured to display performance in the traditional "red," "yellow," and "green" dashboard status. Team

CNSI operations staff set appropriate thresholds during service design. Thresholds that have DPHHS visibility will be reviewed with DPHHS to meet our commitment for transparency.

Related to system monitoring, HealthBeat reports accurate data on items such as end-user response time, CPU utilization, and hourly load averages on different servers. This allows DPHHS and Team CNSI to see the system from a higher point of view and help make informed, strategic decisions on daily operations or future changes in policy and programs. Application management and monitoring, web services management, systems management and monitoring, network management and monitoring, performance monitoring, and event monitoring are all managed via the framework of HealthBeat. Figure 3.10.4-5 shows how HealthBeat monitors system resources of real application clustered (RAC) databases.

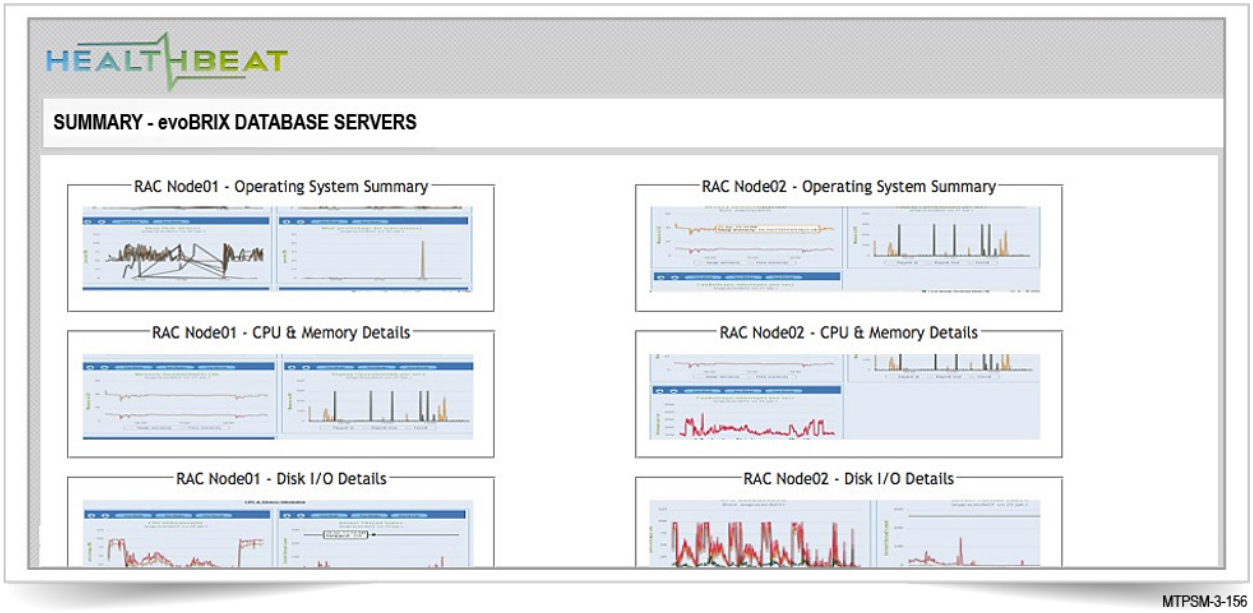


Figure 3.10.4-5. HealthBeat for System Monitoring. This screen illustrates monitoring of clustered databases.

HealthBeat also provides various reporting mechanisms, including dashboards and graphs that can be used to report on the metrics associated with performance standards. Team CNSI uses the HealthBeat tool to collect and report on final performance measures and standards. HealthBeat uses automation to extract, analyze, and report data from various business processes and systems, and to provide a centralized reporting database. This tool provides a robust interface to the various DPHHS MT PSM components for gathering and compiling data, allowing near-real time access to workload and system performance information.

Operational management staff regularly monitor data displayed through the dashboard and can proactively respond if performance indicators begin to decline. In this way, Team CNSI can implement corrective actions before a “red flag” situation occurs. In addition, email alerts are established to notify appropriate Team CNSI and State staff based on configured exception thresholds. Team CNSI also compiles information collected through HealthBeat and summarizes it in our regular reporting mechanisms, including statuses and required workload reports.

The tool produces visualizations of data in various formats, including dashboards and graphs that provide quick summaries for trending. Figure 3.10.4-6 shows the HealthBeat architecture that is configurable and automated.



Proactive System Performance Monitoring and Maintenance

Team CNSI's SLA governance processes establish and document all performance measurement criteria, along with the processes and procedures for monitoring, reporting on, and correcting any deficiencies discovered during operations.

Team CNSI will proactively monitor all defined performance standards to ensure that we meet contract SLAs and performance metrics, using evoBrix HealthBeat where applicable.

Team CNSI technical resources also have a tool suite used to monitor system components. For example, Team CNSI database administrators rely heavily on Oracle Enterprise Manager (OEM) to maintain, monitor, and configure proactive alerts for the evoBrix databases. Team CNSI's Network Operations Center (NOC), located in our Center of Excellence (COE), provides non-stop monitoring of infrastructure and applications. The NOC triages issues to the appropriate operations team for corrective action. Refer to the Availability Management section for full details on our monitoring framework for the evoBrix PMIS.

Team CNSI's proactive monitoring enables us to determine when issues may arise in the future. By monitoring trending data, we can determine whether a system may have issues down the road. For example, if we see that a system is spiking on central processing unit (CPU) usage and memory on a regular basis, then that system may require a hardware upgrade or optimization to remove capacity concerns.

Team CNSI's systems team is regularly informed by alerts from various vendors of the need for proactive patching and maintenance. Team CNSI database administrators, system administrators, and COTS specialists receive notifications of security patches, operating system patches, database patches, and COTS patches that resolve issues. These patches are evaluated to determine whether they apply to the evoBrix PMIS solution. All maintenance activities are scheduled via the formal change management process.

Team CNSI's operational approach is built on a culture of continual process improvement. This is not only an operational principle that dictates our ongoing business processes but is also consistent with ITIL continual service improvement principles. We will continually review all performance measurements and SLAs, and recommend changes – such as system upgrades or database reorganization – when needed to remediate performance-related deficiencies. In this way, the State can expect Team CNSI to continue to adapt via the implementation of innovative solutions and processes that enhance customer service and bring efficiencies while increasing business process and MITA maturity.

Monitoring evoBrix

The purpose of Team CNSI's comprehensive monitoring approach during the post-implementation period is not only to perform quality control, but also to provide feedback for process improvement. Team CNSI's monitoring approach includes three tiers:

- Team CNSI NOC monitoring on a 24x7x365 basis
- Application monitoring
- Business area monitoring

In addition to monitoring system performance and processes, we also monitor application throughputs to identify areas of improvement, either from the system or process perspective. For example, backlogs in the imaging system could arise from a variety of issues from infrastructure to application to human error. By analyzing the throughputs and backlog, we can make changes to the system when needed to remedy performance deficiencies. We are also able to make improvements to the application processes or provide feedback to state business staff, resulting in improved performance of the system and associated business processes.

During the SCI Phase, Team CNSI will identify operational performance measures and the associated reports that generate or contain data relevant to system and operational performance to be monitored and reported through the evoBrix HealthBeat performance tool. Team CNSI's NOC is responsible for generating system and workload reports.

Availability Management

Team CNSI reviews business process availability requirements and aligns them with our ITIL framework. This ensures that cost-effective contingency plans are in place and tested on a regular basis to ensure that the business needs of DPHHS are met. Team CNSI's Availability Management plan includes but is not limited to the following aspects:

- Designing high-availability, redundant systems to support mission-critical applications

- Testing system availability to meet all DPHHS MT PSM project SLAs
- Monitoring and reporting high-availability to ensure that SLAs are being met

High Availability Architecture Design

Team CNSI's evoBrix PMIS solution addresses challenges related to additional volumes and new programs anticipated for the future, as well as issues related to performance, maintenance, and availability. In addition, the solution leverages virtualization technologies to logically partition physical servers, leading to a lower total cost of ownership.

Team CNSI's high-availability architecture includes:

- Clustering at physical host level to provide for physical host failure
- Application server cluster with load balancing
- Web server load balancing
- Oracle Database real application cluster for database high availability
- Oracle Data Guard solution for database replication
- Oracle Recovery Manager (RMAN) for database backups
- Flashback technology for point-in-time recovery
- Data Recovery Advisor for performing recovery analysis

Figure 3.10.4-7 depicts the high-level availability architecture covering clustering at the application server and database server level as well as web server load balancing.

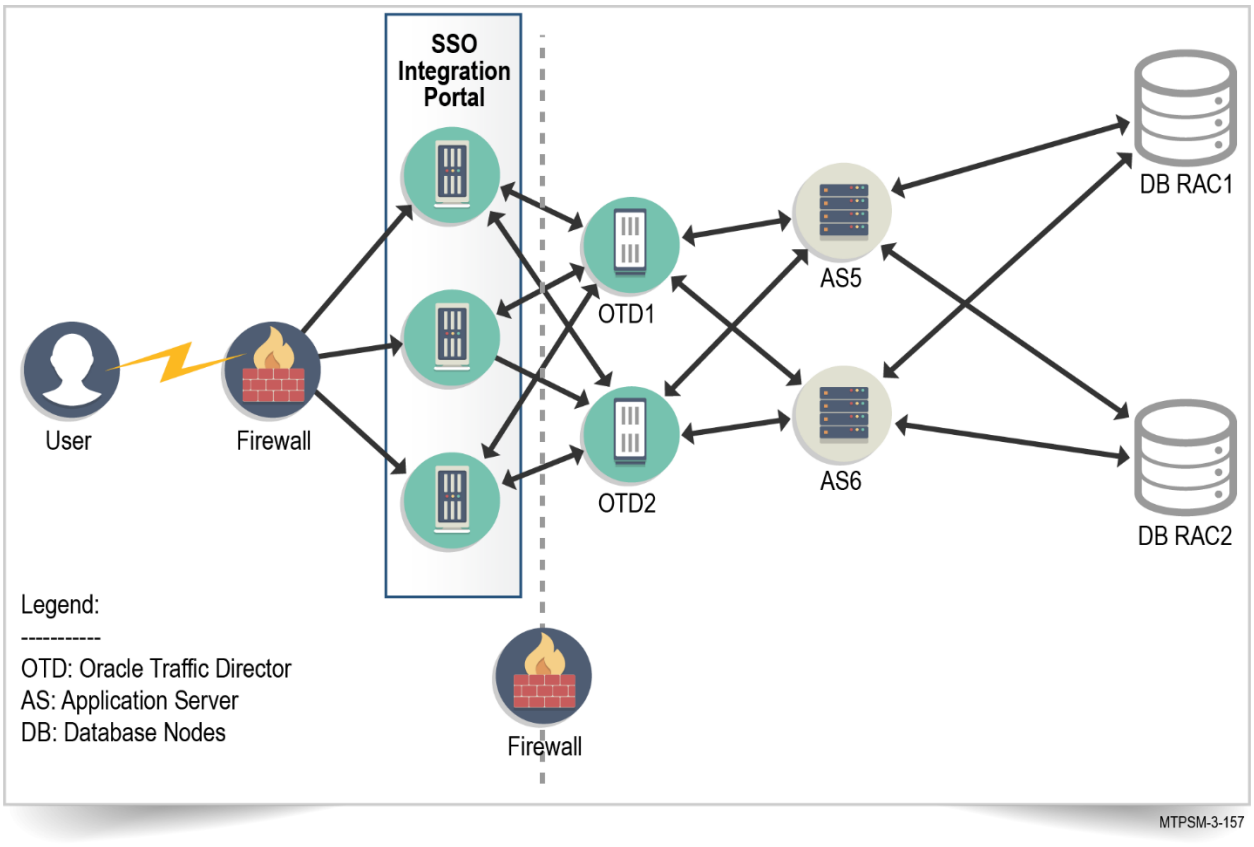


Figure 3.10.4-7. High Availability Architecture. Clustered architecture at the application server level and database server level provides load balancing and high availability capabilities.

There are three types of maintenance windows:

- Scheduled Maintenance (no downtime)
- Scheduled Maintenance (with downtime)
- Unscheduled Maintenance

Scheduled Maintenance (No Downtime)

This type of maintenance covers all regular maintenance activities such as system modifications and changes. This type of maintenance does not require downtime because high availability is achieved via multiple redundant services, resulting in no interruption to operations. Figure 3.10.4-8 contains a list of components that provide redundancy and scalability needed to support 99.9 percent availability and the goal of minimal disruption to providers, members, and other users of the solution.

System Components	Built-in Redundancy
Telecommunications	The telecommunication circuits have redundancy with diverse paths.
Network	Firewalls, switches, and other network equipment are configured in redundant load balanced pairs to eliminate any single point of failure.
Application Servers	Pairs of load balancers interface with application servers that serve end users.
Database Servers	Oracle Real Application Cluster along with Database Backups and Data Guard Replication ensures high availability for databases

Figure 3.10.4-8. Redundancy of System Components. Team CNSI's solution provides redundancy to maximize availability for business operations.

Scheduled Maintenance (with Downtime)

This type of maintenance covers all regular maintenance activities that require downtime. There are some configuration parameters that cannot be altered online and hence require a downtime window. CNSI will collaborate with DPHHS to develop a regular monthly maintenance schedule and plan during the implementation planning phase. The maintenance plan is accompanied by an impact analysis plan as well as a timeline required for the downtime.

Unscheduled Maintenance

This type of maintenance covers high priority changes that cannot wait until the next scheduled maintenance window or release. Unscheduled maintenance is not typically a common occurrence; however, we have processes in place to address it. In such cases, CNSI will plan an ad hoc maintenance schedule in collaboration with DPHHS and will seek formal approval before executing the same. This ad hoc maintenance plan will also be accompanied by an impact analysis plan along with the timelines and contingency plans.

System Availability

Team CNSI's evoBrix PMIS solution architecture undergoes varied levels of high-availability testing in test and performance environments before propagating the changes to a production environment. High-availability testing ensures designing for tolerance, recoverability, and reduced occurrence of high-severity faults. It measures business impact from faults and helps in planning for reducing impact. The testing activities include stress testing, load testing, and distributed denial-of-service (DDoS) attack testing, as well as testing individual hardware component failure and cluster failover capabilities.

OEM, HealthBeat, Building Management System (BMS), and Data Center Infrastructure Management (DCIM) solutions in combination help to provide the necessary monitoring and reporting capabilities for this high-availability architecture. This monitoring and reporting framework will monitor, detect, and report any loss in the high-availability functionality across various layers of hardware and software components. This combination of testing, monitoring, and reporting framework will ensure that Team CNSI's evoBrix PMIS solution complies, 99.9 percent uptime system availability requirement (except for DPHHS-approved maintenance timeframes for production systems).

Team CNSI's solution is also reinforced by a high-performance load balanced application framework and a robust monitoring framework. CNSI developed a configurable tool to monitor SLAs.

Figure 3.10.4-9 depicts one of the reports coming out of the SLA Automation Tool. This report provides details on the number of transactions as well as their response times in each day.

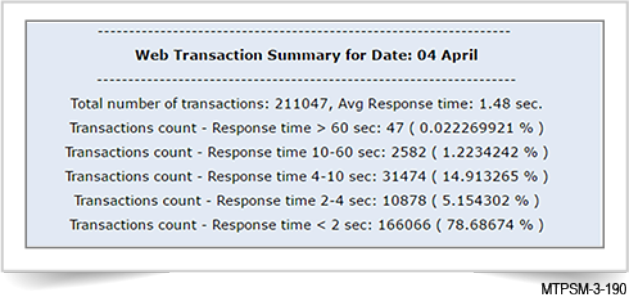


Figure 3.10.4-9. SLA Automation Tool Report. Web Transaction Summary report provides details on the response times of the web transactions across different buckets.

Monitoring and Reporting High-Availability

Team CNSI's evoBrix PMIS solution includes a comprehensive and complete system monitoring and reporting framework. This framework ensures that the high-availability components are working properly across the system. OEM, HealthBeat, BMS, and DCIM provide monitoring and reporting capabilities covering all layers of hardware and software components. Figure 3.10.4-10 provides a classification of monitoring tools and their respective infrastructure modules. These tools are discussed in sections that follow, with the exception of HealthBeat, which was discussed earlier.

Monitoring Tool	Infrastructure Modules
Oracle Enterprise Manager	Databases and Database Servers SOA Suite Application Servers
HealthBeat	Application Interfaces/Web Services Servers
Building Management System	Data Center Power and Cooling
Data Center Infrastructure Management	Infrastructure

Figure 3.10.4-10. Monitoring and System Performance Reporting Tools. This classification of monitoring tools and their associated infrastructure modules forms the backbone of the monitoring framework.

Oracle Enterprise Manager

Team CNSI's database administrators and system administrators rely on OEM to maintain, monitor, and configure proactive alerts for Oracle databases, SOA Suite, and Application Servers. Oracle Management Service (OMS) monitors various targets and collects the performance metrics. These metrics are then

uploaded to the Repository through a Java Database Connectivity (JDBC) API. The OEM Console and Enterprise Manager Command Line Interface (EMCLI) enables administrators to access and manage OEM functionalities, which in turn sends notifications and alerts to the NOC. The NOC triages issues to the appropriate operations team for corrective action. Team CNSI's proactive monitoring enables us to predict when issues may arise in the future. By monitoring trending data, we can determine whether a system is likely to have issues. For example, if we see that a system is spiking on CPU usage and memory on a regular basis, that system may require a hardware upgrade or optimization to remove capacity concerns.

Figure 3.10.4-11 shows the OEM architecture. Various alerts are configured in OEM to issue immediate notifications as soon as an issue occurs. Alerts are sent to the necessary teams and a NOC team that monitors the system 24x7x365 and communicates the same to the respective teams. Figure 3.10.4-12 shows the OEM database load map showing the health of all the registered clustered databases in a single pane of view.

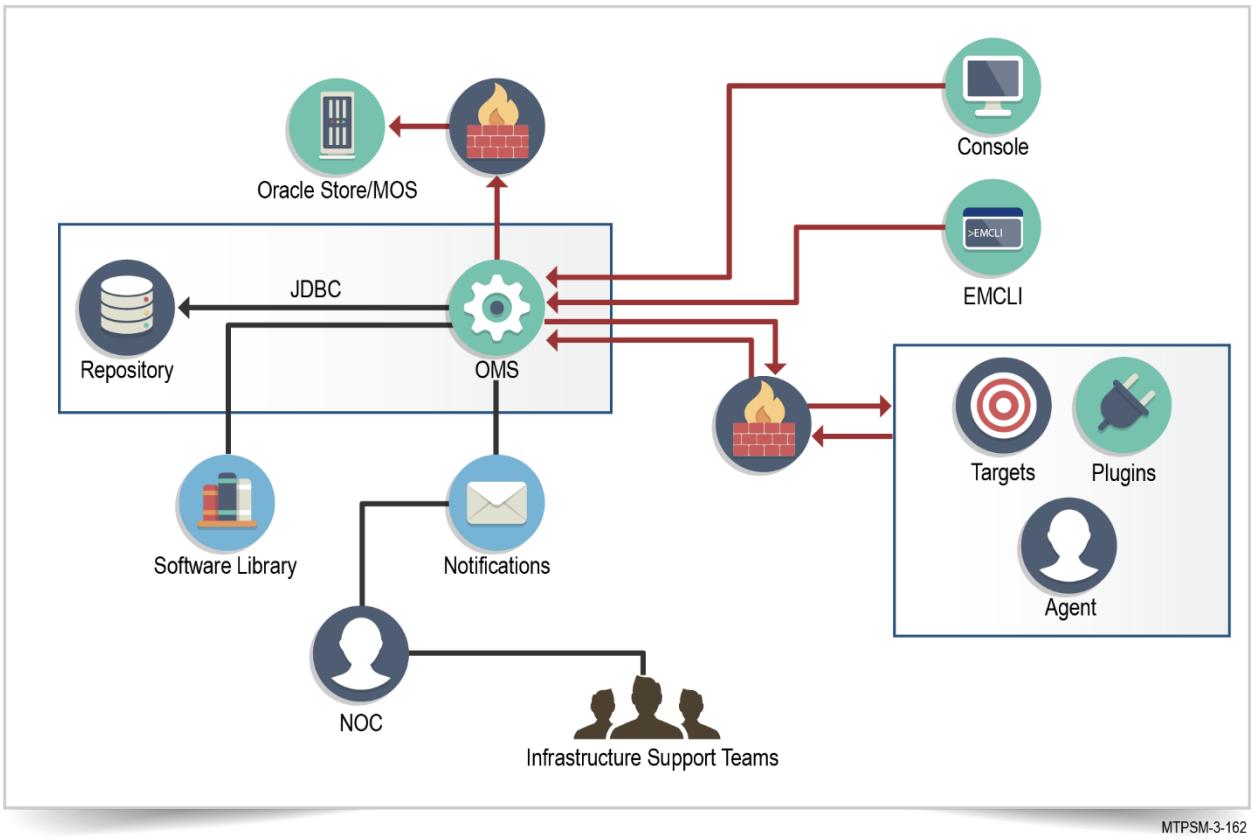


Figure 3.10.4-11. OEM Architecture. OEM monitors the availability and performance of the database and application servers and alerts the necessary teams.

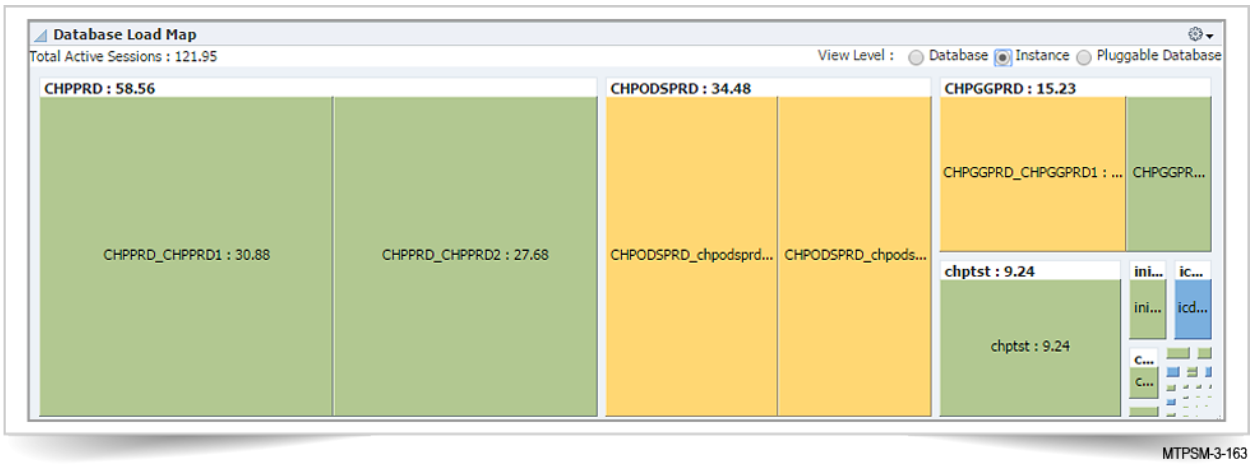


Figure 3.10.4-12. OEM Database Load Map. Portrays the health of all the registered clustered databases in a single pane of view.

Building Management System and Data Center Infrastructure Management

BMS alerts critical facilities staff and engineers of any issues. Depending upon priority, a ticket is executed and staff resolve or assign vendors for ticket completion and issue resolution. The BMS handles monitoring of power and cooling.

DCIM monitors all environmental systems (e.g., temperature, humidity, power usage, leakage, efficiencies of equipment and systems). Additionally, DCIM monitors all video and door access surveillance from a central NOC, staffed 24x7x365. Together, BMS and DCIM help to monitor and report any loss in high-availability functionalities across hardware and software components in the data center layer.

Capacity Management

Team CNSI adheres to the ITILv3 approach for capacity management. Team CNSI has broad and deep experience in various state MMIS implementations and will leverage its success and lessons learned to ensure that the hardware and software infrastructure for the evoBrix PMIS solution fully addresses DPHHS identified requirements. Our solution architecture is fully scalable, both horizontally and vertically, and is intrinsically designed for high availability. We use real-time operational metrics from production implementations for capacity planning. This enables Team CNSI to provide a low-risk, cost-effective infrastructure for managing and operating the evoBrix PMIS solution.

Team CNSI conducts performance testing that demonstrates the ability of the product to scale and captures capacity planning statistics to ensure that adequate resources are available during implementation. Post-implementation, our team deploys real-time and historic statistical analysis to ensure continued compliance with SLAs. Figure 3.10.4-13 shows the workflow for capacity planning.

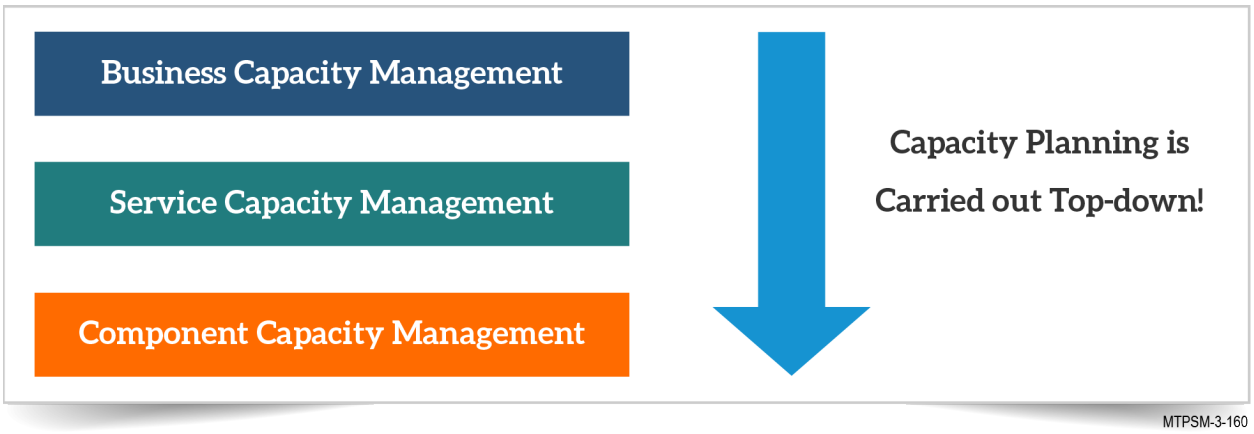


Figure 3.10.4-13. ITIL V3 Capacity Planning Flow. CNSI's solution adheres to ITIL v3 for capacity planning of all major components of the system.

Team CNSI uses the following tools and methods to support ongoing resource capacity use during operations:

- HealthBeat constantly reports all areas including applications and OS resources and generates reports, which helps to monitor and plan the future resource needs
- OEM provides a single pane for managing and monitoring various components, such as databases, middleware, and servers

Capacity Planning is divided into three dimensions:

- Component Capacity Planning
- Service Capacity Planning
- Business Capacity Planning

Component Capacity Planning

Team CNSI uses metrics such as claim volumes, enrolled providers, and concurrent business operations staff to size the recommended hardware and software components. This sizing also considers the amount of data that must be stored by the evoBrix PMIS solution, ensuring that the system is sized sufficiently to maintain and retain all data and imaged and electronic documents for the retention timeframes specified by DPHHS.

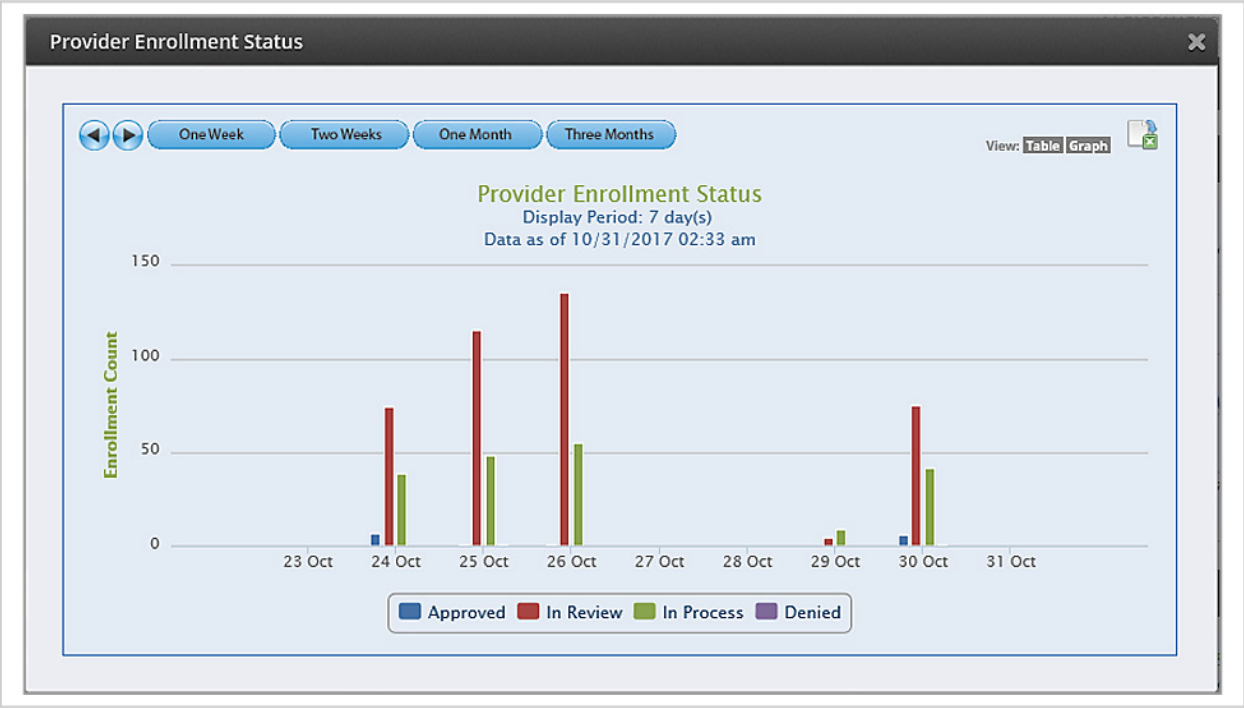
Team CNSI's Component Capacity Management looks at additional metrics such as:

- Number of users and transactions
- Type of transactions
- Data retention
- Database size
- Location of system compared to location of users
- Expected transaction performance, for both transactions and overall system uptime
- Duration parameters for maintenance windows
- Disaster recovery requirements

Team CNSI then uses this data to determine the appropriate sizing and type of technology elements that is required to support those metrics at specified performance levels, taking into consideration:

- Network bandwidth and structure (i.e., type of network connectivity)
- Data storage, both speed and size
- Input/output operations per second (IOPS)
- Server performance, including CPU
- Failover needs (e.g., if clustering is required to meet the requirements)

Applying this approach, Team CNSI looks at the baseline performance with the existing capacity and uses the projected additional data (e.g., users and transactions) metrics in the requirements to accurately predict the additional capacity that is needed to support the expansion. Once these metrics are gathered and the technology elements to support them are considered, Team CNSI arrives at an appropriately sized and scalable infrastructure solution to meet the needs of the system, both at implementation time as well as years to come. Figure 3.10.4-14 shows a HealthBeat screen in the system – one of the key drivers of infrastructure capacity sizing.



MTPSM-3-154

Figure 3.10.4-14. HealthBeat Provider Eligibility and Enrollment Screen. HealthBeat tracks business metrics which identify trends driving capacity needs.

Figure 3.10.4-15 shows a HealthBeat screen displaying the active users that are connected to the system. This is part of component capacity planning that portrays the system load, which is a key input to capacity sizing.

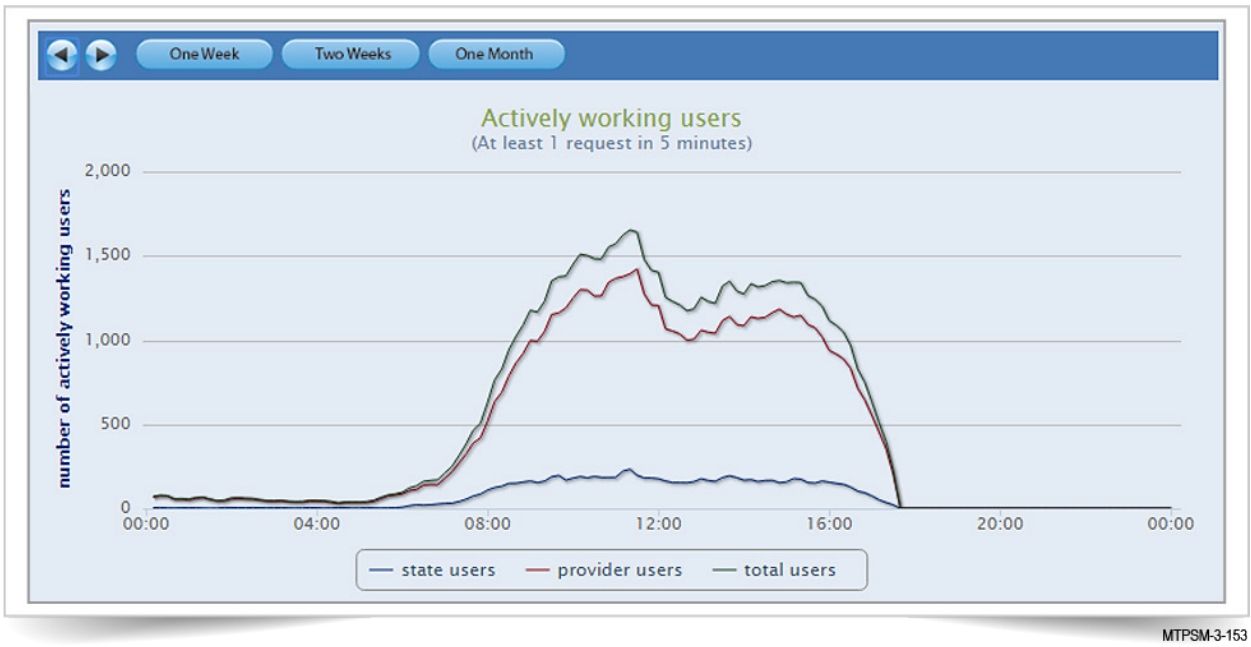


Figure 3.10.4-15. Active Working Users. HealthBeat tracks and reports Daily Periodic active users, which benefits the future planning of the hardware/software.

Service Capacity Planning

During operations, Team CNSI proactively monitors all hardware and software components. Team CNSI looks for trends that indicate capacity and performance issues that may occur in the future. In the event of a trend that indicates a risk, we take proactive steps to resolve capacity issues before the problem occurs. Our process for analysis is to:

- Identify monitoring touch points, frequency, and schedule
- Prioritize the monitoring metrics to identify the most relevant and applicable
- Collect metrics from various monitoring tools throughout the system
- Identify subsystems, processes, components, or system functionality that are not performing optimally
- Generate performance deficiency reports and distribute them to analysts for assessment

To optimize operations, the following infrastructure components are monitored:

- Internet Boundary Routers
- Network Switches
- Demilitarized Zone (DMZ) Firewalls
- Protected Network Firewall
- Content and Load Balancers
- Web Servers
- Application Servers
- Database Servers
- COTS Application Software Configurations
- Storage Area Network (SAN)
- Rules Engine Servers
- Physical Network

Reports that are generated by using the monitoring tools are analyzed for any capacity issues. Figure 3.10.4-16 shows an OEM screen displaying the current load of the database separated by various processes. This is part of service capacity planning that portrays the system load, allowing us to refine capacity sizing.

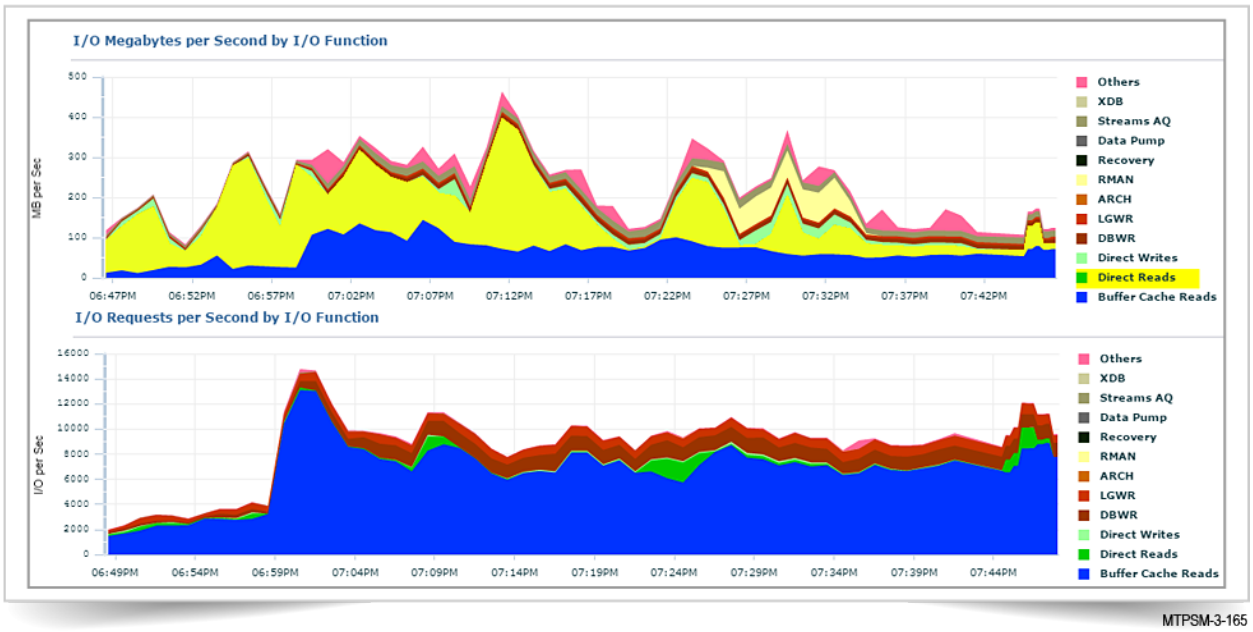


Figure 3.10.4-16. OEM IO Graph. OEM is configured to report the Database and related processes' load which helps to monitor/maintain the performance of the system.

Figure 3.10.4-17 shows a HealthBeat screen that displays the server memory usage. This is part of Service capacity planning, and it helps us estimate the load on the server.

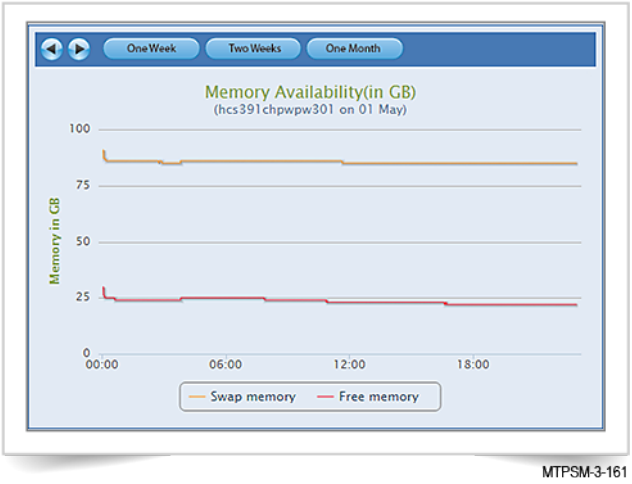


Figure 3.10.4-17. Memory Availability. A HealthBeat screen which shows the memory usage of the server monitored throughout the day.

Business Capacity Planning

Team CNSI's business capacity solution addresses challenges related to the volumes of providers, and new programs anticipated for the future, as well as issues related to performance, maintenance, and availability.

The hardware platform for the evoBrix PMIS solution has been designed to allow future expansion without impacting operations. Servers used for the system are implemented in a load balanced/cluster configuration allowing for horizontal and vertical expansion. Team CNSI offers the options of adding more CPUs, memory, or input/output (I/O) boards to existing servers, or adding newer equipment and decommissioning the older servers to achieve higher levels of performance, if necessary.

Team CNSI's evoBrix PMIS solution, in alignment with ITIL v3 framework:

- Is well-managed, utilizing the highly domain experienced database/network/system administrators to ensure efficient, proactive, and effective infrastructure monitoring and maintenance
- Includes a proven load, stress, and performance testing approach that ensures that SLAs are met
- Is architected and sized using sophisticated capacity modeling techniques
- Is easily scalable to accommodate necessary capacity changes based on the outcomes of monthly utilization reports

Figure 3.10.4-18 shows a HealthBeat screen displaying the Customer Relationship Management (CRM) requests per hour in the system. This is part of business capacity planning, which portrays the system load, allowing us to refine capacity sizing.

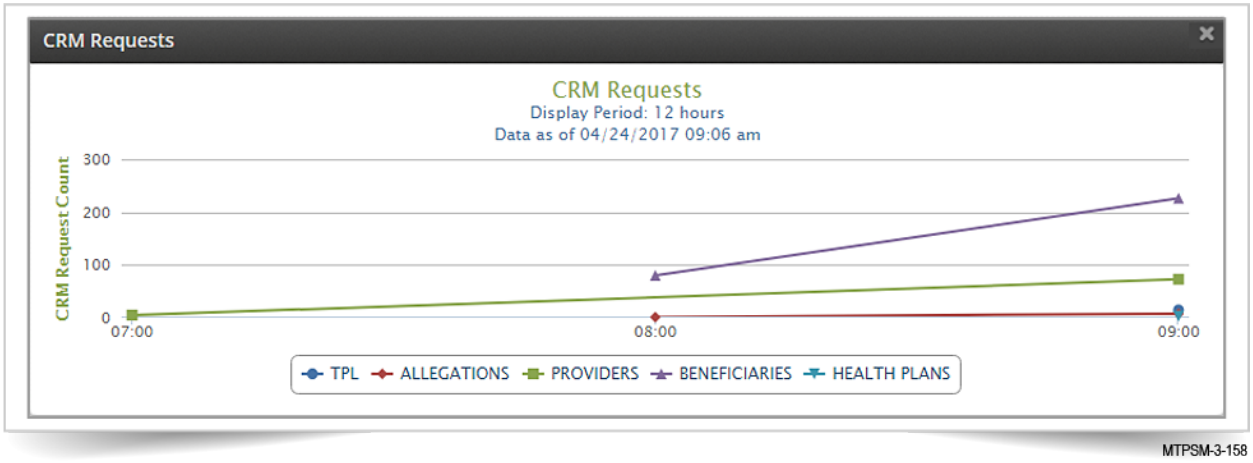


Figure 3.10.4-18. Hourly CRM Request Count. A HealthBeat screen shows the CRM request count, which helps for future planning of the system.

Figure 3.10.4-19 depicts a HealthBeat screen showing the web transaction metrics in the system. This is part of business capacity planning, which portrays the current system load, allowing us to refine capacity sizing.

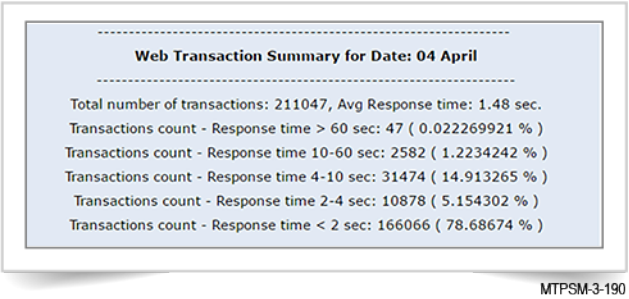


Figure 3.10.4-19. Web Transaction Summary. A screen from HealthBeat reports the transaction summary, which helps to analyze the performance of the system.

Disaster Recovery and Business Continuity

Given the criticality of Medicaid business operations, business continuity is an inherent component of our evoBrix PMIS solution. As a partner, Team CNSI's Disaster Recovery/Business Continuity (DR/BC) Plan will ensure that Team CNSI's evoBrix PMIS solution continues with little disruption, as well as meeting and exceeding their business continuity requirements. Team CNSI's DR/BC Plan template has been refined from our experience in similar large-scale projects, including MMIS projects in the states of Michigan and Washington.

The following examples can lead to the declaration of a disaster:

- Extended power outage expected to exceed backup power capacity facility-wide

- Loss of a building or buildings due to fire, flood, earthquake, or a hazardous material (HAZMAT) incident
- Water or structural damage
- Regional or local damage or conditions from severe weather
- Incidents that causes the primary data center or telecommunication lines to be non-functional

Approach to Providing a DR/BC Plan

Team CNSI determines the critical and non-critical business functions for the disaster recovery purpose and documents the same in the DR/BC Plan. Our plan defines procedures and processes to recover the system from a disaster at the primary data center site. "Disaster," for purposes of this document, is defined as an event or occurrence that directly or indirectly impacts the processing capabilities of the system, causing a loss of critical service, exceeding defined limits, such that a decision is made to restore operations at a pre-determined alternate facility. This process is documented thoroughly and separately. The DR/BC Management Plan includes the following plans:

- Business Impact Analysis (BIA) Plan
- Documentation Template
- BC Plan Management Schedule
- DR Test Plan
- DR Process

Business Impact Analysis Plan

The BIA Plan helps to determine and evaluate the potential effects of an interruption to critical business operations because of a disaster. The BIA Plan seeks to categorize and prioritize business activities for recovery, identify all internal and external dependencies associated with critical activities, determine the amount of time required to resume critical activities, and estimate the resources that each critical activity will require for resumption of business.

Figure 3.10.4-20 shows the template of the BIA Plan along with the type of information that is requested.

Business Impact Analysis (BIA) Plan	
Business unit name	*Enter the business unit name*
Head count	*Enter the number of full-time staff in the business unit, optionally, part-time and contractors, if applicable*
Parent process	*Describe the principal activities the system performs*
Priority ranking	*Enter a number here for subjective ranking of process importance*
Recovery time objective (RTO)	*Enter a time frame, e.g., 24 hours; it describes the time the system must return to "business almost as usual" following a disruption*
Recovery point objective (RPO)	*Enter a time frame, e.g., one hour; this is a point in time to which parent process work should be restored following a disruption*
Parent process depends on	*Enter names of organizations and/or processes the parent process depends on for normal operations*
Parent process required by	*Enter names of organizations and/or processes that depend on the parent process for normal operations*
Quantitative impact	*Enter a financial amount associated with the parent process, e.g., annual revenue generated by the process*
Qualitative impact	*Enter a non-financial impact to the company, e.g., loss of reputation, loss of customers associated with parent process*
Time needed to recover staff	*Enter the number of staff that need to be back to "business almost as usual" within specific time frames*
Recovery strategy	*Enter specific actions the business unit can take to recover to a "business almost as usual" state, e.g., work from home, relocate etc*
Technology/Services recovery time	*Enter the system and services in each time space that must be recovered within the specific time frame*

MTPSM-3-219

Figure 3.10.4-20. BIA Plan Template. A template that captures the information required for the BIA Plan. This template helps to determine the impact of a disaster on critical business functions.

Documentation Template

Documentation Templates provide a description of the Minimum Focus Areas (MFA)/Mission Essential Functions (MEF). MEFs and MFAs represent a limited set of DPHHS functions that must be resumed rapidly after a disaster occurs. Figure 3.10.4-21 describes representative information from Team CNSI's MFA/MEF.

Business Area	Brief Overview/Description
Provider Support	Provide centralized support and services to Medicaid providers that affect their billing and reimbursement. Research and resolve billing and reimbursement issues that providers present via hotline, email, fax, mail, or at training sessions. Enroll and maintain Medicaid providers. Distribute educational resources for providers.

Figure 3.10.4-21. Documentation Template for MFAs and MEFs. Team CNSI conducts detailed business continuity planning and supports collaboration with DPHHS to ensure minimum essential functions are addressed.

DR/BC Plan Management Schedule

Team CNSI reviews the DR/BC plan periodically and focuses on the following elements and scenarios:

- Changes in functionality
- Changes in mission-support requirements

- Changes in operational support environment
- Changes to the organization and management of users
- Changes in the BIA that affect Return to Operations priorities
- Changes in regulatory or security requirements

Disaster Recovery Test Plan

Team CNSI's DR/BC Plan will undergo additional discussions with DPHHS and the SI to refine and maintain the plan. A DR Test Plan is the examination of each step in a DR/BC Plan. It also includes dependencies, key staff from DPHHS and Team CNSI, and important information that covers third-party hardware and COTS vendors, including contact information and support contract information. This test ensures that Team CNSI's DR/BC solution recovers data, restores business-critical applications, and continues operations after an interruption of services. This DR Test is conducted once per year.

During the DR Test, Team CNSI does sanity checks and analyzes audit logs and other data to determine what worked as expected, what didn't work as expected, what changes need to be made to the DR/BC plan's design, and what tasks need to be scheduled for re-testing. These results and other artifacts generated out of the DR Test are then delivered to DPHHS.

Disaster Recovery Process

For a successful recovery from a disaster, snapshots of the production systems are taken every four hours at the Production Data Center and replicated to a dedicated DR site housed in a geographically diverse DR datacenter. Databases are replicated in real time between the Production and DR Data Centers using the Oracle Data Guard Solution. The distance between the two sites is great enough to mitigate all natural and man-made disasters. To ensure uptime recovery of eight hours or less in the disaster recovery site, replicated system copies are immediately merged into the active storage system in the disaster recovery site. An automated disaster recovery orchestration tool automatically tracks changes on the primary site production network and configuration and automatically makes all necessary configuration changes in the DR site environment. All static network settings applicable to the environment configuration are pre-configured by a team of expert system and network engineers to ensure that any DR event or DR test is seamless.

If a disaster is declared at the production site by the State and Team CNSI, a preplanned recovery process is set in motion. All users of the evoBrix solution will be redirected to the disaster recovery site. The plan also has required steps and dependencies, a list of key staff from the State and Team CNSI, and important information that covers third-party hardware and COTS vendors, including contact information and support contract information.

The DR/BC Plan is tailored to meet the maximum allowable recovery time objective (RTO) of 24 hours and a recovery point objective (RPO) of eight hours. The DR site is designed to be equivalent to a Production site. In the event of a disaster that results in the production site being down for more than seven business days, then at the sole discretion of DPHHS, Team CNSI will repurpose the DR site to be a primary site and work on building a new backup/DR site data center within 30 calendar says.

Disaster Recovery Tools and Methods

Oracle Database Replication

The Oracle databases for the evoBrix PMIS solution are synchronized between the Production site and DR site using Oracle Data Guard. Team CNSI's Oracle database teams are experts in this technology and have proven that this approach works in all MMIS systems that we host. Because the Data Guard

technology is built by Oracle, it provides native integration and is managed under the same pane as the Oracle databases, providing a real-time view of the synchronization in progress. The tool seamlessly integrates with the database instances and requires no additional training for our Oracle database administrators to manage. It maintains the versioning, transaction logs, and all other pieces needed to keep the data synchronized between the primary data center and the DR data center.

Operating Systems and Applications

The synchronization of the various operating systems and COTS products (other than databases) between the primary and DR data centers is managed automatically by a replication software Actifio Resiliency Director (ARD). This includes operating system (OS)-level patches, OS files, and hardware and network configurations. Each DR system replicates the Production system in terms of specifications and configurations. ARD and the underlying Actifio replication technology helps to orchestrate one-click DR.

Service Operations

Team CNSI will ensure readiness of all the components required for a successful evoBrix PMIS solution implementation, a seamless transition into operations, and finally certification. The System Operations Manager will be responsible for creating the Operations and Maintenance (O&M) Plan, and ensuring transparency by including inputs from Team CNSI, the SI vendor, and DPHHS to compile and then review for quality and completeness. The O&M Plan will use industry best practices and be presented in a comprehensive Operations Manual that is in alignment with our proven service operations framework running in four states – including cloud operations for the states of Michigan and Illinois – and as described by ITIL v3, CMS eXpedited Life Cycle (XLC) Operations & Maintenance Manual and architectural design. Figure 3.10.4-22 shows ITIL v3 Services areas covered under Service Operations.

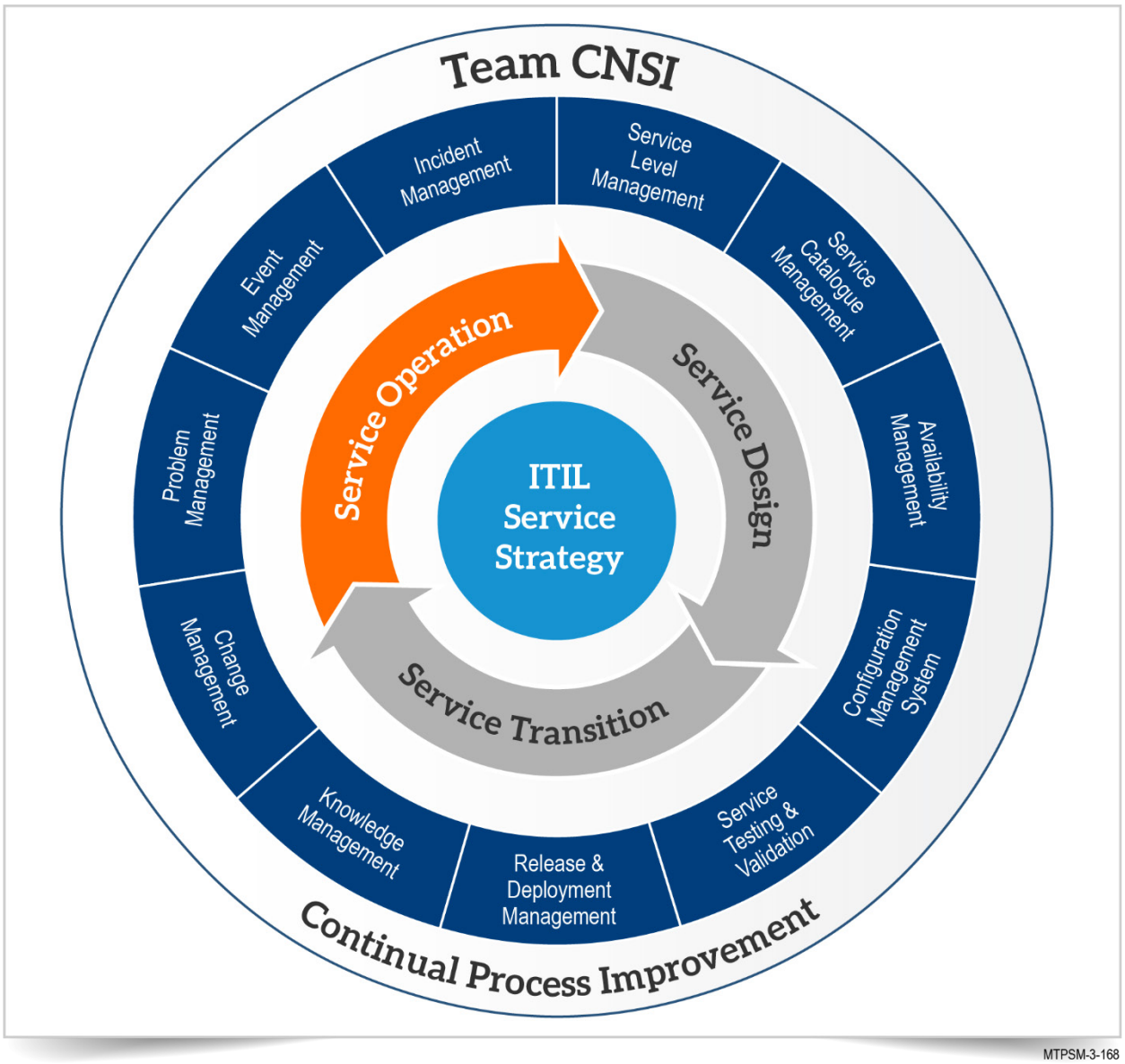


Figure 3.10.4-22. Team CNSI's ITIL-based Service Operations. Team CNSI's systems operations services ensures readiness of all the components required for a successful evoBrix PMIS solution.

Team CNSI leverage our existing Operations Manual standards and tailoring as necessary for the evoBrix PMIS solution. The Operations Manual will describe our ongoing support and operations procedures and will be formatted in the following structure:

- System Overview
  - Functional System Overview

    Application/System Dependencies
  - Physical System Overview

    Physical Architecture

System Software to Hardware Specifications
Special Server Conditions
System Firewall Specifications

- System User Overview

  Estimated Users
  Peak Processing Times
  Hours of Operations
  User Impacts for System Failures

- Processing Overview

  Data Flow Diagram
  Data Sources
  Data Refresh/System Updates
  Reporting Requirements
  Service Level Agreements

- Security and Privacy Overview

- Roles and Responsibilities
- Operations Procedures
- Data and Database Administration Procedures
- Configuration Management Procedures

The O&M Manual will also provide Team CNSI and DPHHS with a regularly updated list of personnel who will be performing evoBrix PMIS solution production support, along with their contact information and areas of expertise. It will provide the framework of our production and support processes, define day-to-day support, and include detailed procedures for items including:

- Identifying the root cause of corrupted data, identifying the fix, and repairing any corrupted data that is associated with a problem
- Providing the State with a copy of the routine planned maintenance schedule no less than 30 calendar days in advance of the scheduled maintenance date for approval (including the process for presentation to the State and receiving concurrence from the State) and the scheduling of the maintenance so as not to disrupt the negotiated operational hours
- Developing an automated process for purging production Software as a Service (SaaS) platform files as determined by data governance decisions
- Include administration procedures and describe the scheduled operations of the production system, including specific instructions on things an operator needs to do to manage the system daily
- Descriptions of administrative tasks
- Instructions on how to run interface and database (DB) jobs
- What to do in abnormal situations; for example, an interface job failure or a system restart due to hung treads
- System documentation will also detail the following:

  - Operations procedures, including batch or background process schedules, dependencies, sequencing, and timing
  - Administrative tasks, including user administration, system security administration, reference data maintenance, creation of report templates, and maintenance of service provider data and contracts

  - Other reference materials and presentations required to supplement the training and support activities

- A High Availability and Disaster Recovery Plan for the entire evoBrix solution driven by the State's Recovery Time Objectives
- Help Desk Support for use by the responsible entity service desk, addressing items including:

  - Overview of the support strategy
  - Help and service desk design
  - Help and service desk operations (processes and procedures)
  - Incident management procedures and processes, including escalation
  - Problem management procedures and processes
  - Application support
  - Reporting
  - Help and service desk scripts and decision trees for tier 1 help desk and tier 2+ service desk support

- Additionally, as part of ongoing production support, the manual will provide:

  - Frequently Asked Questions
  - Application validation procedures
  - Server startup and shutdown procedures
  - Build documentation

Request Fulfillment

Request Fulfilment Support

Team CNSI provides and maintains the tools, processes, skills, and rules for an effective and efficient handling of service requests, and provisions the infrastructure and services for help desk application (OTRS) that users can use to submit the requests.

Help Desk

Team CNSI's Help Desk is expected to receive varying types of service requests which will come from multiple sources. The Help Desk delivers top-quality customer service with knowledgeable, well-trained support staff and powerful tools to produce a high first-contact resolution rate. Help Desk staff are trained to handle any service request that may come. Our Help Desk request model is built for each type of request received and addresses each step or phase of request fulfillment. The Help Desk services provide a centralized support system, including staff with specialized knowledge to respond to the variety of inquiries and requests made by end users, internal staff, and other third-party support organizations. The Help Desk is accessible to users via telephone, email, and the web via the OTRS ticketing system.

Direct Requests via Open Source Ticket Request System

Team CNSI uses OTRS for logging and tracking evoBrix end-user system or application related requests. Approved Team CNSI business teams, DPHHS, and third-party users can log requests directly into OTRS via the web interface. Requests coming through the Help Desk are also logged by Help Desk personnel directly into OTRS.

OTRS assigns tickets to incoming queries and tracks further communications about them. Team CNSI uses OTRS for incoming support requests, inquiries, complaints, defect reports, and other

communications. Every ticket generated by the system has persistence or "history" showing what happened to the ticket within its life cycle. OTRS has the ability to merge multiple tickets for the same issue or request to eliminate duplicate tickets. OTRS is a multi-user system, which means that multiple users may work simultaneously on tickets, reading incoming messages, and updating them. OTRS is highly scalable, capable of handling thousands of tickets per day, and can handle a large number of users working simultaneously. Once a request is entered, it is triaged and assigned to the right team to handle, based on the severity and complexity of the request.

Request Logging and Categorization

Team CNSI's Help Desk completes an initial evaluation and triage of each ticket as they are logged, 24x7x365, and routes them to the correct queue for further analysis and evaluation. When a queue is assigned, Team CNSI operations staff reviews the newly logged ticket and responds accordingly. As a part of our technical processes, Team CNSI establishes two Change Control Boards (CCBs) to manage review and approval of changes as follows:

- **Tier 1 CCB** – consisting of Team CNSI technical and business operations staff with a focus on reviewing and approving changes
- **Tier 2 CCB** – consisting of Team CNSI and DPHHS staff to review status of tickets and approve changes prior to production implementation

Figure 3.10.4-23 explains the priority levels of an OTRS ticket, necessary actions, and management responsibilities with their required communication plans.

OTRS Priority/ Definition	Required Action	Corrective Action Timing	Management Responsibility	Communications Plan
Urgent Severity 1	■ Direct user contact required ■ Management Communications will occur once triage is complete ■ Follows Tier 2 CCB escalation process	■ Corrective action will be taken on a priority basis ■ All attempts will be made to correct the issue through operational means ■ Alternative measures include RFC or emergency code release if necessary and approved by Tier 2 CCB	■ Tier 1 CCB ■ Tier 2 CCB	■ Send notification when triage is complete ■ Notification will include plan of action and estimated time to restoration if known
High Severity 2	■ Follows the Tier 1 CCB process	■ Follows Release Planning process	■ Tier 1 CCB	■ Follows Tier 1 CCB review process
Medium Severity 3	■ Follows the Tier 1 CCB process	■ Follows Release Planning process	■ Tier 1 CCB	■ Follows Tier 1 CCB review process
Low Severity 4	■ Follows the Tier 1 CCB process	■ Follows Release Planning process	■ Tier 1 CCB	■ Follows Tier 1 CCB review process

Figure 3.10.4-23. OTRS Priorities. The OTRS priority strategy helps to distinguish tickets based on the business impact and track them to resolution.

Request Execution

Figure 3.10.4-24 shows the response time for tickets triaged by each team.

Support Level	Support Level Description	Support Teams	Responsibilities	Availability	Response Time
0	Self-Service	OTRS	■ Web-based ticketing system ■ Instant visibility of tickets to all support tiers	■ 24x7x365	■ Real-Time
1	Basic	NOC/Help Desk	■ Log tickets and perform triage and ticket routing ■ Monitor system performance and operations processes ■ Support requests, application processing operations, access requests, and technical inquiries ■ Escalate tickets to Tier 2 or Tier 3 based on defined procedures	■ 24x7x365	■ 30 minutes
2	Moderate	Operations Support	■ Manage and support all operational activities ■ Monitor and maintain SLA compliance ■ Track, facilitate, and coordinate tickets and operations processes ■ Oversee operations processes including access requests, Incident Management, Event Management, Release Management, Change Requests, and SLAs ■ Escalate tickets to Tier 3 based on defined procedures	■ On Call (24x7x365)	■ 1 hour
3	Technical/Integration	Application Services	■ Triage, prioritize, and support tickets, incidents, and requests ■ Follows the DevOps model and collaborates closely with their business counterparts and CCB teams	■ On Call (24x7x365)	■ 1 hour
3	Technical/Integration	Infrastructure/ Data Services	■ Monitor, maintain, and provide incident response for infrastructure and data services	■ On Call (24x7x365)	■ 1 hour

Figure 3.10.4-24. Team CNSI's System Support Model. Team CNSI establishes systematic processes to provide event/incident management support based on ITILv3.

Request Monitoring and Escalation

OTRS requests are monitored closely and triaged by our support teams for efficient resolution. Evaluated OTRS tickets result in one of the following:

- Defects/Enhancements – Jira tracking Ticket
- Operational Requests – Request for Change (RFC)
- Single Sign-On (SSO) Issues – SI Ticketing System
- No change required – Escalate to Tier 2 CCB for closure

Figure 3.10.4-25 shows the OTRS ticket passing through various stages of reviews from different teams for resolution.

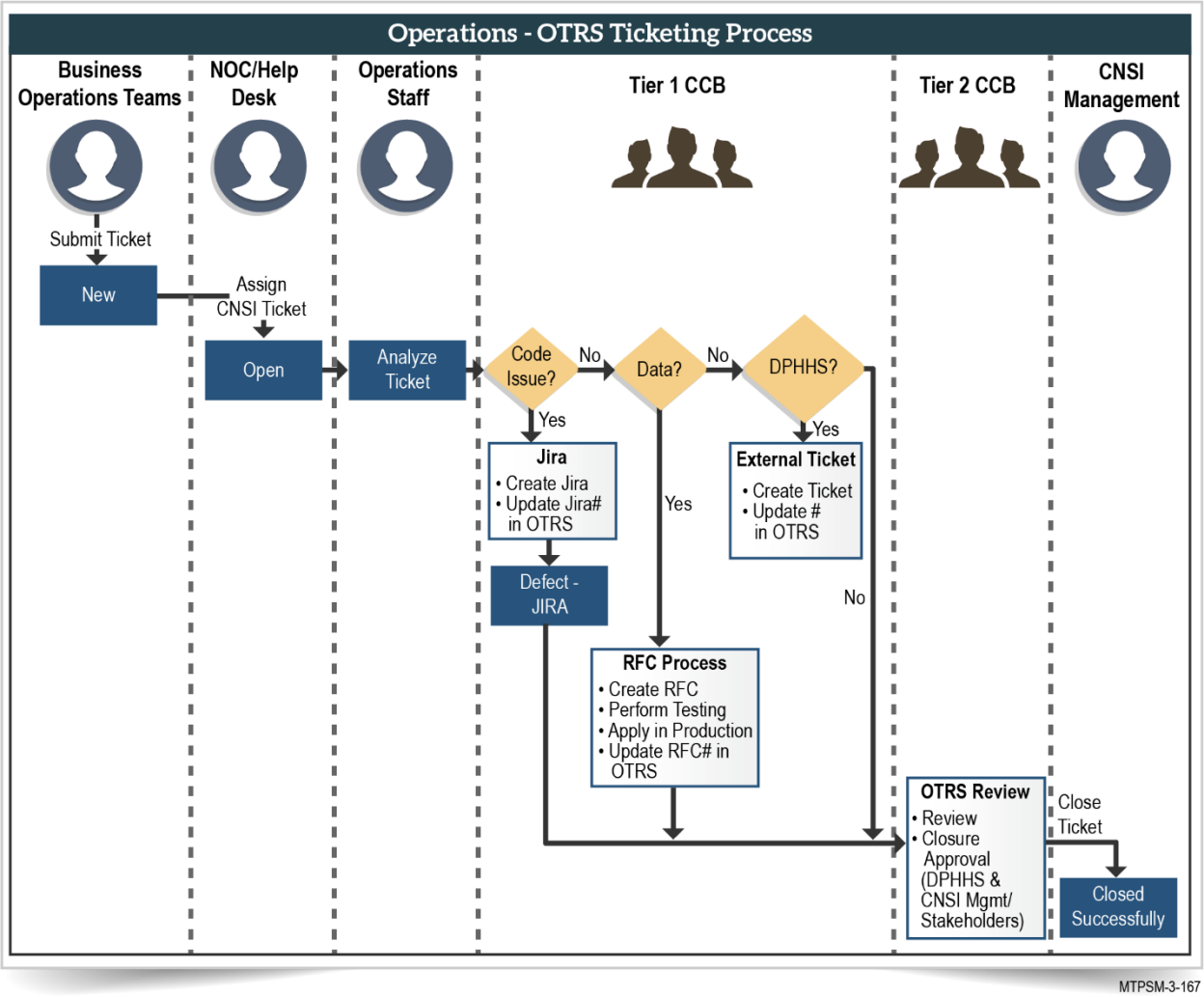


Figure 3.10.4-25. OTRS Request Flow. OTRS enabled by specific standard rules helps to involve all the required or impacted teams and get the approvals before the actual implementation.

Opened tickets are reviewed at the Tier 1 CCB meetings. The meetings are held weekly with representation from Team CNSI Teams, DPHHS, and additional stakeholders. The status of each opened ticket is summarized in the meeting, and tickets requiring more information are discussed. If agreement on a common solution or resolution cannot be reached, the ticket is escalated to a Tier 2 CCB management meeting for review.

Request Closure and Evaluation

The Tier 2 CCB authorizes closure of each OTRS and associated Jira ticket. Ticket closure falls into the following categories:

- OTRS resolved through Operational RFCs
- OTRS due to no change required
- Rejected Jira Tickets
- Production Released (UAT Passed) Jira Tickets

The Tier 2 CCB also discusses requests and issues escalated from the Tier 1 CCB. The Tier 2 CCB can escalate unresolved issues to senior management and stakeholders.

Events and Incident Management

Similar to the Request Fulfillment process, the Team CNSI business areas and technical operational teams use OTRS to log both Event and Incident Management items so they can be tracked and triaged to resolution and finally closure. Events and incidents often become confused. Differentiation and understanding of the two terms as well as their respective processes is determined as follows:

- Event monitoring is not just to detect "something wrong." It is also to get assurances of things "going right" and things that "might" need some action.
- When an event indicates "something really wrong," then it is an incident and calls for the Incident Management process.

If an operations team member determines an event or incident should be logged and tracked, then they will enter a ticket into Team CNSI's ticket tracking tool, OTRS, where the ticket will be triaged by our 24x7 NOC Help Desk, located in our COE, and then addressed appropriately; for example, a report of a planned outage would trigger our Event Management process to track the planned downtime, while a report of an unplanned outage would trigger our Incident Management process to ensure quick restoration of services. Both event and incident tickets ultimately follow the OTRS ticket resolution and tier processes to resolution and closure.

Team CNSI processes allow users to track and log events and incidents via OTRS. Like requests, events and incidents are monitored closely and triaged by the Team CNSI support teams for efficient resolution. For example, an event where the operations team needs to be notified of server maintenance, scheduling changes, or downtime request, is converted to a Jira Request for Change (RFC) ticket, then goes through a review and approval process prior to the execution of a request. After execution, the RFC is moved to the Tier 2 CCB for review. After the review is complete, the Tier 2 CCB approves the RFC for closure.

When an incident – such as an unplanned outage or a reported defect in an application or screen – occurs, a ticket is logged, the NOC Help Desk then reviews the incident ticket to ensure that it is routed to the correct queue for triaging.

An OTRS ticket describes the incident and the system, subsystem, or operational area affected by the issue. The NOC validates the Priority Level (i.e., Urgent, High, Normal, or Low), and enters pertinent information. Figure 3.10.4-23 in subsection, Request Fulfillment, defines the different Priority Levels, actions to be taken, and the communication plan. The Help Desk notifies the appropriate response team via auto-generated email or by phone (depending on the level of severity) so the triage process can move forward. Each evaluated OTRS ticket results in one of the following actions:

- Defect/Enhancement – Jira Ticket
- Operational Request – RFC ticket (data change, queue change, schedule request, or infrastructure)
- Single Sign On (SSO) Issue – DPHHS System Integration Services (SIS) Ticket
- No Change Required – Escalate to Tier 2 CCB for closure

Our support service provides transparency in reporting, fulfilling user requests, resolving service failures, fixing problems, and carrying out routine operational tasks.

Problem Management

Team CNSI defines a problem as any anomaly in the operational or technical environment that affects delivery of services. When a problem occurs:

- Team CNSI's operations management is notified.
- Team CNSI Help Desk is notified of the issue and impact to services. The Help Desk opens an incident ticket using OTRS.
    - The ticket describes the event and the module or operational area affected by the issue
    - The Help Desk assigns the Priority Level (i.e., Urgent, High, Normal, or Low) and enters pertinent information
    - Help Desk notifies the appropriate response team
    - Help Desk notifies account management of the issue and the assigned response team
- Team CNSI assembles the appropriate personnel to conduct an analysis of the issue and define an action plan to resolve the issue depending upon the severity level of the issue.
- Once the appropriate course of action is determined, Team CNSI opens a Jira ticket for internal tracking purposes.
- Team CNSI assigns the appropriate personnel to conduct its own detailed internal review and obtain the appropriate approvals to commence the resolution. In this meeting, a discussion of the issue, solution, and a review of the scripts, if any, is conducted. Scripts should meet the same standards set by CNSI internally to ensure continuity and reduce the chance of negative effects to the system.
- Once approved, the resolution will be implemented.
- Team CNSI Operations Management receives periodic updates throughout the incident until the resolution is completed.
- Team CNSI management notifies the appropriate DPHHS personnel.

After the incident or problem has been resolved, Team CNSI creates an Incident Report, an example of which is shown in Figure 3.10.4-26. An Incident Report compiles the following information:

- What triggered the incident
- What services are affected by the incident
- A complete timeline of events
- All actions taken to resolve the issue
- Lessons that were learned and ideas for prevention in the future
- List of each person involved at any time throughout the incident
- Summary of each communication
- Attachments, including actual emails and records of phone calls and meetings, with a summary of what was discussed

CNSI
WWW.CNS-INC.COM

Production Incident Report

Incident Headline:	
Incident Date/Time:	
Report Author:	
Team(s)/Individual(s) Involved:	
Date Report Prepared:	
Ticket Number(s):	

Incident Details

Description:

Detailed description of the incident.

Scope and Impact of the Incident:

Who or what was impacted by the incident. List both short term and long term Impacts.

Incident Resolution Timeline

Communications:

List all communications relating to the incident (emails, phone calls etc.). Include individuals involved & timelines.

Solution: Steps Taken to Resolution and Next Steps:

Detailed descriptions of steps taken to resolve the incident including timelines.

Root Cause:

Detailed description on what caused the incident to occur.

Incident Prevention Plan

Lessons Learned and Recommendations:

Describe lessons learned as a result the incident and provide detailed recommendations on how to prevent this incident from reoccurring in the future.

Action Plan:

Describe the Action Plan to implement the Recommendations including Owners and expected completion dates for the Actions.

Step	*Task*	*Owner*	*Planned Date*
1	*Example: Install new certificate when there is a change or time to renew the LN SSL certificate.*	*PCS and MI Deployment team*	NA

Incident Report Template.docx CNSI Page | 1

MTPSM-3-159

Figure 3.10.4-26. Sample Production Incident Report. Team CNSI focuses on root cause analysis to address incidences during production.

The completed Incident Report is then distributed to Team CNSI management. After review, Team CNSI management distributes the Incident Report to the appropriate DPHHS personnel. If more than one problem occurs in the same area, Team CNSI conducts a root-cause analysis to develop a thorough understanding of the issue and its causes. The Incident Reports for those problems are used as part of the tracking and understanding of the problems. A plan is derived from the analysis for either corrective or preventative actions that will reduce the risk of another occurrence to an acceptable level. The corrective or preventative actions will be documented, implemented, and shared with DPHHS. Follow up reviews of the actions are conducted to make sure they are properly alleviating the issue and determine whether there is a more efficient way of correcting or preventing the problem.

3.10.4.1 Maintenance and System Enhancements

Throughout the life of the contract there are two distinct classifications of work that all MPATH Module Contractors will perform maintenance and system enhancements.

Maintenance

DPHHS defines maintenance for each MPATH module as follows: -

1. *Making configuration updates as requested by DPHHS. Configuration includes changes to table values, parameters, codes, and business logic, including hardcoded business logic.*
2. *Correcting deficiencies (defects) found in the solution(s) based on detailed requirements described in the scope of work and published design specifications.*
3. *Correcting deficiencies (defects) found in the solution(s) based on a failure to meet the detailed requirements in completed enhancement, configuration or maintenance requests.*
4. *Conducting research requested by DPHHS or required to support the Department. For example:*
   a. *System behavior and results*
   b. *New healthcare initiatives*
   c. *Best practices research across states and industry*
   d. *Impacts of new State and federal legislation*
5. *Performing mass adjustments or mass changes as requested by DPHHS or required to support Montana Healthcare Programs (for example, errors in pricing, eligibility, cost share, and financial code assignments, TPL discovery, and provider reimbursement changes).*
6. *Performing regular maintenance as needed by DPHHS required to support Montana Healthcare Programs. Examples of maintenance include but are not limited to:*
   a. *Performance optimization.*
   b. *Database management.*
   c. *Software, hardware, and tools (e.g., patches, upgrades, and replacement).*
   d. *Interface, report, and correspondence changes.*
   e. *Making corrections or changes to maintain the integrity of the system or the data within it (e.g., backing out changes, correcting duplicate records, cleansing corrupt data, adding security measures, adding redundancy).*
7. *Using appropriate testing, configuration, and change control procedures.*
8. *Updating system, user, and training documentation and online help to reflect changes that have been made to the solution.*
9. *Performing the activities above to maintain customizations implemented as part of an approved enhancement.*
10. *Perform incremental integration services via configuration. Incremental integration services should be included in the DDI costs.*

If incremental integration can be handled using configuration, the integration will fall under the definition of maintenance, if the incremental integration requires system development and testing efforts the integration will fall under the definition of enhancement.

All maintenance activities will be performed at no additional cost to the State in the Contractor's response. The Contractor will be required, at no additional cost, to add resources necessary to complete all activities by the required due date. Maintenance activities and any associated hours will not be applied to the system enhancement hourly pool.

System Enhancements

DPHHS defines systems enhancements as follows:

1. *System enhancements exclude any activities defined in "Maintenance" above.*
2. *New features or functionality that fall outside the scope of all RFP requirements, Offeror's RFP response, the contract, or agreements of any supplemental negotiations.*

The State must approve both the design and level of effort prior to the start of development or configuration for system enhancements. DPHHS must approve any changes to the design or level of effort that occur after the original approval. The level of effort billed cannot exceed the level of effort approved by DPHHS. The level of effort incurred to complete an enhancement will be applied to the System Enhancement Pool once the enhancement is implemented and approved by the Department. If the level of effort exceeds the System Enhancement Pool hours remaining, the Department may choose to utilize hours from the next Contract operations year or have the Contractor invoice the Department for the balance at the rates defined in Attachment G, Provider Pricing Schedules, Schedule E – Resource Hourly Rates.

The Contractor must provide an estimate of any impact to annual operations cost, for the enhancement during the operations phase of the Contract if applicable. Reimbursements for any additional operations costs must be addressed in a contract amendment.

System Enhancement Pool
DPHHS recognizes that enhancements to the solution may be required periodically throughout the life of the contract to meet mandated Federal or State rules or regulations or to provide increased efficiency in operations or promote cost savings. The Contractor will add resources as necessary to complete enhancements by the required due date.

System Enhancement Pool for DDI Base Scope of Work
The Contractor will provide 1,500 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 1,500 system enhancement pool hours are included in the offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.

The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one-month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

System Enhancement Pool for DDI Option A Scope of Work
The Contractor will provide 500 system enhancement pool hours for the duration of the DDI phase of the contract for the Option A Scope of Work. The cost of these 500 system enhancement pool hours are included in the offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.

The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will

require one-month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

System Enhancement Pool for DDI Option B Scope of Work
The Contractor will provide 250 system enhancement pool hours for the duration of the DDI phase of the contract for the Option B Scope of Work. The cost of these 250 system enhancement pool hours are included in the offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.

The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one-month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

System Enhancement Pool for Operations Base Scope of Work
The Contractor will provide 500 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 500 system enhancement pool hours are included in the Offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D – Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G, Provider Pricing, Schedule D – Enhancement Pool Hours.

System Enhancement Pool for Operations Option A Scope of Work
The Contractor will provide 100 system enhancement pool hours during the Operations phase per operations year for the Option A Scope of Work. The cost of these annual 100 system enhancement pool hours are included in the Offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D – Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G, Provider Pricing, Schedule D – Enhancement Pool Hours.

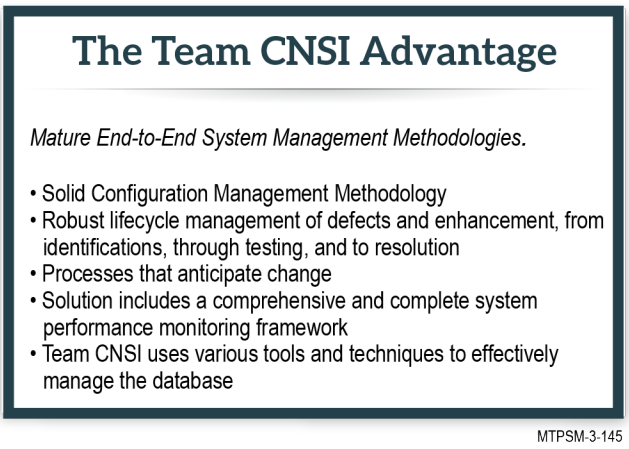
System Enhancement Pool for Operations Option B Scope of Work
The Contractor will provide 100 system enhancement pool hours during the Operations phase per operations year for the Option B Scope of Work. The cost of these annual 500 system enhancement pool hours are included in the Offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

©2017 CNSI

Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D – Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G, Provider Pricing, Schedule D – Enhancement Pool Hours.

The Offeror must describe their approach to meet each of the detailed Operations, Maintenance, and Configuration requirements defined in Attachment F, Requirements Matrix.

Team CNSI's operations maintenance and system enhancement approach is based on ITIL standards. We carefully manage maintenance and enhancement activities to ensure maximum efficiency, stability, and performance. Proactive maintenance, patching, and an efficient enhancement process for the evoBrix solution will be a combined effort, which will involve our Center of Excellence (COE). The COE, located in Lansing, MI and Rockville, MD, utilizes a shared services model and is comprised of Operation support, Application Services, Development, Infrastructure Management, and testing teams.



Team CNSI is able to leverage years of MMIS operations maintenance and system enhancement experience to accurately assess whether staffing levels and expertise required are appropriate to the needs of the stabilization and certification periods, as well as ongoing operations and on through to turnover should that phase be activated by the state. Team CNSI prides itself on having knowledgeable and response staff to manage and execute operations activities. Utilizing shared services and matrixed approaches, we are assured of experienced staff being available to perform both routine and complex tasks required during operations.

Another key factor of our operations success is that Team CNSI creates and maintains robust operations documentation covering aspects from infrastructure to applications and the related processes. The application documentation is updated in alignment with system change requests, to ensure that our teams are always working from documentation that represents the most current state of the system. Similarly, for the infrastructure, the documentation is updated with every update (e.g., change in software version or upgraded firmware) and is reviewed quarterly by the shared services support teams.

Team CNSI will comply with the base software maintenance period and will follow an approved release process and calendar to ensure defects, enhancements to ensure system stability over the maintenance period. Team CNSI recognizes that the maintenance periods include "adaptive" maintenance/ modification of the system performed after completion of deployment to keep the system usable in a changed or changing environment, and "perfective" maintenance which is modification of the system after completion of deployment to improve performance or maintainability. During this period, Team CNSI will be in charge of maintenance, and hosting and operating the system and providing disaster recovery services.

Incident and maintenance request reporting will be embedded in our operations processes. We will produce all required operations reports and, specifically for incident and maintenance requests, we will report on trends that provide meaningful metrics, such as ticket categories and rate of open/closure, etc. For additional detail on our incident and maintenance request reporting, please see section 3.10.4 Operations, Maintenance, and Configuration.

Categories of System Maintenance and Enhancements

Changes are a natural part of projects and operational environments. Team CNSI utilizes processes that not only anticipate changes but also address them on a timely and proactive basis. Team CNSI delivers high quality software to its customers through the execution of our CMMI level 3 & ITILv3 processes. Maintenance and Enhancements fall into the following categories:

- Maintenance – Regular patching, upgrades, tuning, and other maintenance to system components to maintain performance, functionality, and security during operations
- Support – Providing operations support to DPHHS resources within Team CNSI's scope of operations
- Defects - System faults identified as part of the scope of the original development effort during the Software Maintenance period
- Enhancements – System changes that are not part of the original scope

Change Management

Defects and Enhancements identified during operations are tracked through Team CNSI's Change Management process. The process and associated supporting artifacts, such as forms, templates, or reports will be included in the Change Control Plan. All identified changes are tracked as a Change Request (CR) in the JIRA ticketing system.

The high-level steps conducted in tracking Change Requests (CRs) are as follows:

- Create and submit the CR
- Record and review the CR information
- Assess and evaluate the CR
- Authorize the change through the change control board (CCB)
- Update plans and other documents based on the impact analysis
- Implement the CR and coordinate with impact organizations
- Review and close the CR

The following section provides details of the change control management process.

Create/Record CR

A CR may be used to propose a change to the scope, schedule, cost, or configurable items such as hardware, software, or security permissions. A CR can originate from the State, fiscal intermediary staff, other project team members, external stakeholders, and end users that need service. CRs may also originate from the risk or issue management processes.

Review CR, Assess and Evaluate Change

After the CR is submitted, it will be reviewed and analyzed by Team CNSI. The submitted CRs may be as a result of:

- A new CR submission
- Update of an existing CR
- Consideration of a postponed CR for a new release cycle

The CR is placed in the CCB review queue. No owner assignment takes place as a result of this action. An initial review of the contents of the CR is conducted in a CCB review meeting to determine if it is a valid request. If a CR is believed to be a duplicate of another CR that has already been submitted, it will be assigned to team member to resolve it based on the status of the original CR.

The CR may be determined, in the CCB review or by the assigned team member, to be an invalid request or that more information is needed from the submitter. The CR may be scheduled for re-review by the CCB at a later date. The originator may also be consulted for further information or justification.

A project member or small team may be assigned to the CR to conduct a more thorough analysis on a specific issue or aspect. This analysis will include a review of the contract, requirements, plans, and other documentation.

Authorize CR

State staff and Team CNSI project management staff will authorize the implementation of the CR and place it into the change control management work queue (team or area that will own the resolution of the CR). These queues may include work areas such as business process area, system development, and system administration.

Update Plan

Once the CR has been placed into an "assigned" status, the owning team member updates the detailed project schedule as necessary The Detailed Project Work Plan is evaluated, and after the schedule is evaluated and impacted changes made, the CR is placed in a "scheduled" status.

Coordinate the Change Implementation

Depending on the type of change, this sub-process has a number of possible procedures. Once a resource starts working on the CR, it is placed into an "Assigned" status to reflect that it is being worked. The assigned team will coordinate with the implementation of the change.

Review and Close the Change Request

Once the CR is completed by the assigned staff, it will be reviewed by quality assurance (QA) to verify the implementation. The Team CNSI and DPHHS management will validate that the processes have been executed.

OMC01

The Contractor shall cooperate and assist the Department in responding to all law enforcement, federal and State audit and review requests. The Contractor shall provide audit support including, random sample generation, data extracts, hard-copy documents, and provide any requested data or information.

Team CNSI will cooperate and assist DPHHS in responding to all law enforcement, federal, and State audit and review requests. Team CNSI will provide audit support including random sample generation, data extracts, and hard-copy documents, and provide any requested data or information. The Team CNSI

Operations Project Manager will respond to specific requests, including email archive requests, and needs of the OAG, within individually specified timelines, outlined in each request submitted to Team CNSI.

OMC02

The Contractor shall support the disaster recovery activities that will provide timely failover and create relevant documented policies and procedures to implement a recovery.

Given the criticality of Medicaid business operations, business continuity is an inherent component of our evoBrix PMIS solution. As a partner, Team CNSI's Disaster Recovery/Business Continuity (DR/BC) Plan will ensure that Team CNSI's evoBrix PMIS solution continues with little disruption, as well as meeting and exceeding their business continuity requirements. Team CNSI's DR/BC Plan template has been refined from our experience in similar large-scale projects, including MMIS projects in the states of Michigan and Washington.

The following examples can lead to the declaration of a disaster:

- Extended power outage expected to exceed backup power capacity facility-wide
- Loss of a building or buildings due to fire, flood, earthquake, or a hazardous material (HAZMAT) incident
- Water or structural damage
- Regional or local damage or conditions from severe weather
- Incidents that causes the primary data center or telecommunication lines to be non-functional

Approach to Providing a DR/BC Plan

Team CNSI determines the critical and non-critical business functions for the disaster recovery purpose and documents the same in the DR/BC Plan. Our plan defines procedures and processes to recover the system from a disaster at the primary data center site. "Disaster," for purposes of this document, is defined as an event or occurrence that directly or indirectly impacts the processing capabilities of the system, causing a loss of critical service, exceeding defined limits, such that a decision is made to restore operations at a pre-determined alternate facility. This process is documented thoroughly and separately. The DR/BC Management Plan includes the following plans:

- Business Impact Analysis (BIA) Plan
- Documentation Template
- BC Plan Management Schedule
- DR Test Plan
- DR Process

Please refer to section 3.10.1.3 Hosting and Environments and Section 3.10.4 Operations, Maintenance, and Configuration for a complete overview of Disaster Recovery, Business Continuity and approach.

Executing DR Activities

In the unlikely event that a disaster is declared, Team CNSI will immediately form a Disaster Response team to manage the process of Disaster Recovery. The team will be led by Team CNSI's System Operations Manager and will include a multi-disciplinary team of experts from infrastructure, application, and operations support teams.

The Disaster Response team's priority will be to restore system function as soon as possible and within the defined Recovery Time Objective and with minimum data loss as specified by the Recovery Point Objective. Team CNSI's DR architecture is designed to accomplish both RTO and RPO objectives in the event of a DR. It is the Disaster Response team's responsibility to ensure that activities are conducted in accordance with the DR architecture and DR plan. Past executions of DR tests serve as valuable tools in ensuring successful execution of activities in the event if an actual DR scenario.

While infrastructure and application teams focus on the technical tasks to complete the DR activities, the operations support team focuses on communication of status to key stakeholders and notifications to system users. They also track overall progress of DR activities and document any issues encountered during the execution of DR activities.

Once all DR activities are complete and all system functions are restored, the System Operations Manager will inform all key stakeholders. The operations support team will notify system users that they may resume normal system use. Once the issue that activated the Disaster Recovery situation is resolved, the System Operations Manager will consult with key stakeholders to determine the feasibility and timing of returning operations to the Primary Hosting environment. Once a decision is made to return operations to the Primary Hosting environment, the Disaster Response team will execute the documented plan to transfer operations back to the original state.

Finally, once operations are returned to their normal state in the Primary Hosting environment, a final report will be issued by Team CNSI documenting the DR activities executed. The report will outline the conditions that caused the DR incident, the steps executed as part of the DR Response, and any recommendations for future improvement in DR processes.

OMC03

The Contractor shall conduct an annual test of the Disaster Recovery and Business Continuity Plan and submit the Disaster Recover/Business Continuity Test Report that includes the outcome, corrective action plan, and revisions, if any, to the Department.

Team CNSI conducts an annual test of the Disaster Recovery and Business Continuity Plan and submits the Disaster Recover/Business Continuity Test Report that includes the outcome, corrective action plan, and revisions, if any, to the DPHHS for review and approval. Please refer to Section 3.10.1.3 Hosting and Environments and Section 3.10.4 Operations, Maintenance, and Configuration for a complete overview of Disaster Recovery, Business Continuity and approach.

OMC04

The Contractor shall provide Operations support, Maintenance, and ongoing Configuration of the provided Solution(s) throughout the life of the Contract. This includes providing Operations support as described in the scope of work as well as providing Maintenance and Enhancements to the provided Solution(s). The Contractor will follow project management and system development processes throughout the life of the Contract.

The Agency defines maintenance for each module as follows:

1. Making configuration updates as requested by the State. Configuration includes changes to table values, parameters, codes, and business logic, including hardcoded business logic.

2. Correcting deficiencies (defects) found in the solution(s) based on detailed requirements described in

the scope of work and published design specifications.

3. Correcting deficiencies (defects) found in the solution(s) based on a failure to meet the detailed requirements in completed enhancement, configuration or maintenance requests.

4. Conducting research requested by the State or required to support the Department. For example:

a. System behavior and results

b. New healthcare initiatives

c. Best practices research across states and industry

d. Impacts of new State and federal legislation

5. Performing mass adjustments or mass changes as requested by the State or required to support the State's healthcare programs (for example, errors in pricing, eligibility, cost share, and financial code assignments, TPL discovery, and provider reimbursement changes).

6. Performing regular maintenance as needed by the State required to support the State's healthcare programs. Examples of maintenance include but are not limited to:

a. Performance optimization.

b. Database management.

c. Software, hardware, and tools (e.g., patches, upgrades, and replacement).

d. Interface, report, and correspondence changes.

e. Making corrections or changes to maintain the integrity of the system or the data within it (e.g., backing out changes, correcting duplicate records, cleansing corrupt data, adding security measures, adding redundancy).

7. Using appropriate testing, configuration, and change control procedures.

8. Updating system, user, and training documentation and online help to reflect changes that have been made to the solution.

9. Performing the activities above to maintain customizations implemented as part of an approved enhancement.

10. Perform incremental integration services to retrofit previously implemented modules to accommodate integration with modules in the design, configuration and build phase. Incremental integration services should be included in the DDI costs.

Team CNSI will implement its proven change management maintenance processes upon project initiation, which governs changes throughout Operations phases of the project. Our process efficiently and effectively manages technical, programmatic, and operational changes across the overall program. Prior to the Operations Phase, we will review and refine the Change Management Plan as needed for operations. Ongoing maintenance and operations will use the ITIL service management and Configuration Management plan model to perform maintenance, operations, and enhancements. Using a foundation with which the team is already familiar will provide a smoother transition to operational changes.

Also as part of our quality assurance program, Team CNSI reviews all operational areas and work processes on a regular basis, which helps ensure the quality of work meets or exceeds the acceptable level and that the defined operational procedures are being followed. At least one formal review must be conducted before any new process or function is implemented, and a review must be conducted when a process changes significantly. After that, business processes are subject to informal and formal reviews. We will continue this process, along with other established quality assurance practices, throughout MT PSM operations.

Team CNSI will also work with the State to assess the impact of business process and technical changes from the system perspective using the change management and configuration process. When a business process change is introduced through the change management process, Team CNSI will assess each aspect of the change's impact to the environment including the impact upon communication, training, and publications related to system functionality. The change management process and the training plan will be used to coordinate timing and approvals that ensure changes required to revised artifacts have at least 90 days to be updated when a business process change has been requested.

Figure 3.10.4-27 shows how different requirements are handled through the Change and Release Management process as opposed to scheduled maintenance activities during the Operations.

Change and Maintenance Activities	Process
■ Correcting deficiencies (defects) found in the solution(s) based on detailed requirements described in the scope of work and published design specifications. ■ Correcting deficiencies (defects) found in the solution(s) based on a failure to meet the detailed requirements in completed enhancement, configuration or maintenance requests. ■ Making configuration updates as requested by the State. Configuration includes changes to table values, parameters, codes, and business logic, including hardcoded business logic. ■ Performing mass adjustments or mass changes as requested by the State or required to support the State's healthcare programs (for example, errors in pricing, eligibility, cost share, and financial code assignments, TPL discovery, and provider reimbursement changes). ■ Using appropriate testing, configuration, and change control procedures. ■ Updating system, user, and training documentation and online help to reflect changes that have been made to the solution. ■ Performing the activities above to maintain customizations implemented as part of an approved enhancement. ■ Perform incremental integration services to retrofit previously implemented modules to accommodate integration with modules in the design, configuration and build phase. Incremental integration services should be included in the DDI costs. ■ Interface, report, and correspondence changes. ■ Software changes.	Change and Release Management (See Section 3.10.7 Project Deliverables and Documentation)
■ Performing regular maintenance as needed by the State required to support the State's healthcare programs. Examples of maintenance include but are not limited to: • Performance optimization. • Database management. • Hardware, and tools (e.g., patches, upgrades, and replacement). • Making corrections or changes to maintain the integrity of the system or the data within it (e.g., backing out changes, correcting duplicate records, cleansing corrupt data, adding security measures, adding redundancy). Tracking, facilitating, and coordinating tickets and operations processes.	Maintenance Plan (Activities and Scheduled Maintenance) (See Section 3.10.7 Project Deliverables and Documentation)

Figure 3.10.4-27. Change and Release Management. Shows how Change and Release Management and regular maintenance activities are handled.

Tracking System Changes

Team CNSI uses a defined Tier meeting structure and processes within our operations to discuss MT PSM changes and to ensure technology impacts are identified and changes are implemented within the required timeframes. Team CNSI will work with the state to utilize the Tier meeting structure for MT PSM System Operations. The Tier meeting structure consists of a Tier 1 CCB and a Tier 2 CCB. The Tier 1 CCB consists of DPHHS and Team CNSI evoBrix subsystem business and technical stake holders. The Tier 1 CCB meets weekly to discuss incidents and change management requests. Figure 3.10.4-28 shows the Tier Structure and responsibilities.

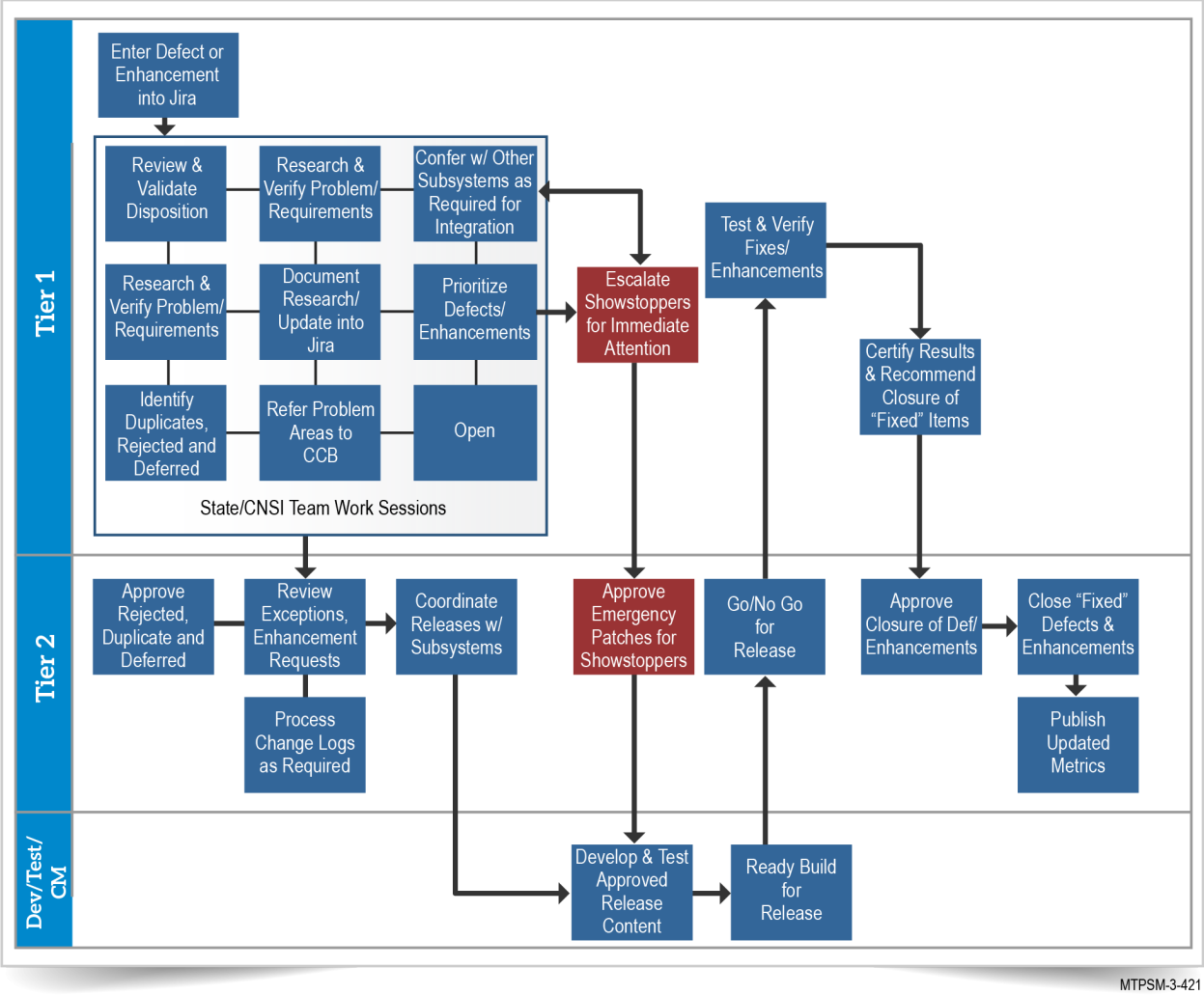


Figure 3.10.4-28. Team CNSI Weekly Tier Meeting Structure. Weekly meetings help facilitate system changes.

Tier 1 change management decisions, as well any situations that cannot be resolved by the Tier 1 CCB, are escalated to the Tier 2 CCB for final decisions and approval. The Tier 2 CCB consists of the State, Team CNSI, and MT PSM business owners as well as representatives from the PMO. The change process begins with a ticket is submitted by DPHHS through the Open Source Ticket Request System. Each request is evaluated by the Tier 1 CCB. As a result of the evaluation, the change request is placed in one of the categories defined below:

- **Enhancement**: The request represents a change to the approved design. Enhancements are typically triggered by a policy change, newly identified system capabilities, or business process changes.
- **Defect**: The system is not performing as designed. A code change is required to correct the issues.
- **Data Change Request (DCR)**: There is a request to change system data, such as a list of reference codes, interface run parameters, or claim batch processes. No code change is required. DCRs can typically be processed when appropriate without the need for a software release.

Enhancements and defects are assigned a unique identification number for tracking through the change process, and a change request is created for enhancements. This request contains a clear definition of the requested change, Team CNSI's response to the change, and an inventory of all impacted system modules

and design artifacts. All enhancements and defects are reviewed and approved by the Tier 2 CCB as defined in the Release Management section below. For all enhancements approved to be included in a release, the Tier 1 CCB team participates in one or more CAD sessions to create or revise the design artifacts that are required to support the change. These design artifacts include all use cases, screens, reports, letters, and interfaces that are impacted by the change. Upon completion of the CAD sessions, Team CNSI finalizes the change request package and submits it to DPHHS for approval.

The next step is for Team CNSI to develop the software changes needed for each enhancement or defect. Once the software is completed and unit tested, the enhancement or defect is turned over to Team CNSI's test team for System Testing. Once the ticket passes System Testing, Team CNSI turns the enhancement or defect over to DPHHS's independent User Acceptance Test (UAT) team for testing. Once the enhancement or defect passes UAT, it is approved by the Tier 2 CCB for deployment to production.

Scheduled Maintenance

Team CNSI also has a well-defined maintenance schedule to perform regular maintenance as needed by DPHHS to support state patching, maintenance and optimization. During the maintenance window, Team CNSI completes such activities as:

- Performance optimization
- Database management
- Software, hardware, and tools (e.g., patches, upgrades, and replacement)

There are three types of maintenance windows:

- **Scheduled Maintenance (no downtime).** This type of maintenance covers all regular maintenance activities such as system modifications and changes. This type of maintenance does not require a downtime because high availability is achieved through multiple redundant services, thus resulting in no interruption to operations. Figure 3.10.4-29 contains a list of components that provide redundancy and scalability needed to support 99.5% availability and the goal of minimal disruption to providers, members, and other users of the solution.

System Components	Built-in Redundancy
Telecommunications	The telecommunication circuits have redundancy with diverse paths.
Network	Firewalls, switches, and other network equipment are configured in redundant load balanced pairs to eliminate any single point of failure.
Application Servers	Pairs of load balancers interface with application servers that serve end users.
Database Servers	Oracle Real Application Cluster along with Database Backups and Data Guard Replication ensures high availability for databases

Figure 3.10.4-29. System Components. An overview of various system components along with their built-in-redundancy strategy enables the system to be highly redundant.

- **Scheduled Maintenance (with downtime).** This type of maintenance covers all regular maintenance activities that require a downtime. There are some configuration parameters that cannot be altered online and hence require a downtime window. In such cases, Team CNSI will develop a maintenance schedule (monthly or quarterly) for the MT PSM solution in collaboration with DPHHS, and will seek formal approval before implementing it or making any changes. Every maintenance plan is accompanied by an impact analysis plan as well as a timeline required for the downtime.

- **Unscheduled Maintenance.** This type of maintenance covers high priority changes that cannot wait until the next scheduled maintenance window or release. In such cases, Team CNSI will plan an ad hoc maintenance schedule in collaboration with DPHHS and will seek formal approval before executing the same. This ad hoc maintenance plan will also be accompanied by an impact analysis plan along with the timelines and contingency plans.

Configuration Management

Team CNSI's software Configuration Management (CM) policies and procedures are based on our iVision360 SDLC methodology, tailored to configure Team CNSI's evoBrix platform and components to meet the evoBrix PMIS solution implementation and operational needs.

This approach will allow the following for DPHHS:

- Consolidated snapshot of Configuration Items (CIs) for the project
- Snapshot of baseline contents
- Configuration Control for CM systems
- Specifications on building work products out of CM systems
- Maintain the integrity of the baseline

Team CNSI's knowledge and understanding of building, testing, and successful integration of various modules to provide the requisite services provided by an MMIS is based on multiple implementations certified by CMS, coupled with adherence to the industry best practices by following the ITIL-aligned CM policies, processes, and procedures. This provides a framework to avoid any unauthorized changes, manage the baselines to support multiple environments, and provide traceability and auditing for all CIs throughout the lifecycle of the evoBrix PMIS solution.

The ITIL framework defines several processes and functional groups and their relationship with a CM system. New Systems Team members are encouraged to obtain ITIL certifications while existing members already have or are on track towards obtaining ITIL foundation level certifications at a minimum to maintain alignment with the latest standards. Figure 3.10.4-30 illustrates how the different functional groups feed and obtain data from the CM-maintained system.

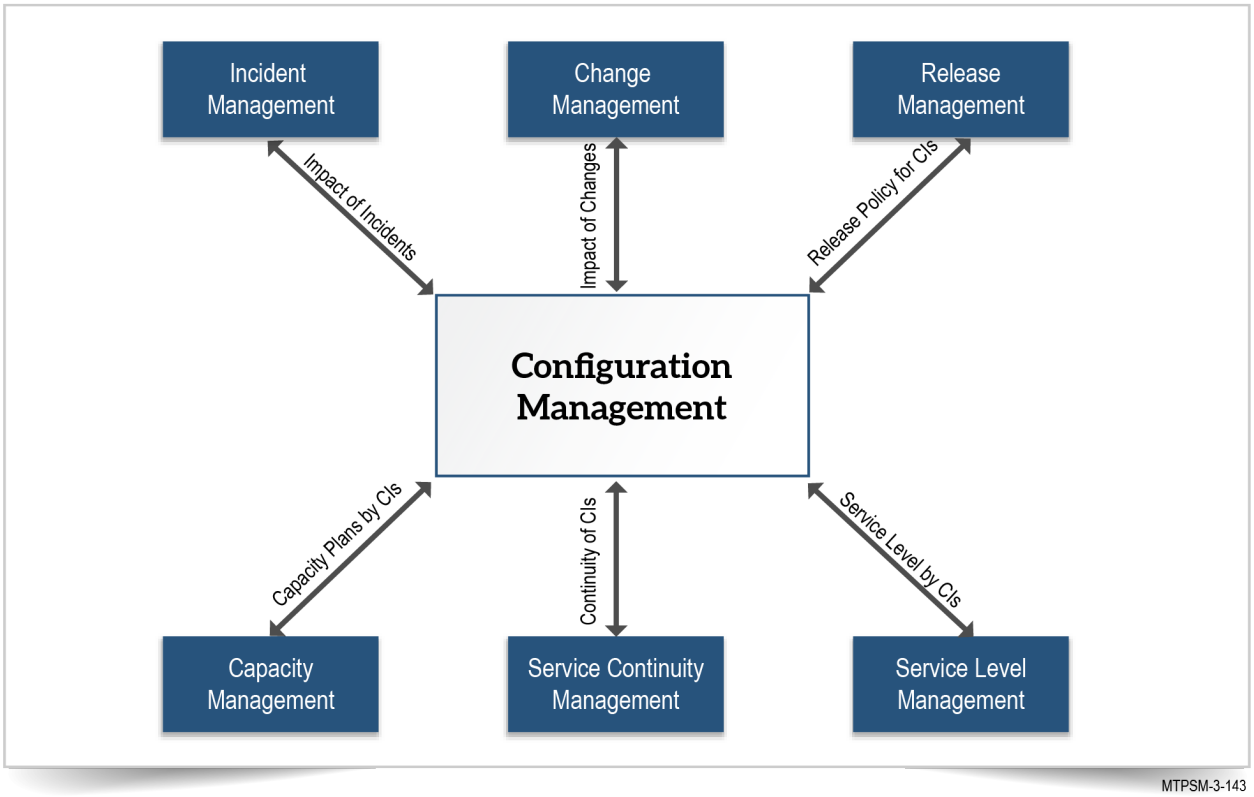


Figure 3.10.4-30. Configuration Management as Part of ITIL Framework. Team CNSI's approach to Configuration Management provides a holistic view across all ITIL service areas.

A brief description of all the various ITIL Process areas interacting with the Configuration Management process area is listed in Figure 3.10.4-31.

ITIL Process Area	Brief Description
Incident Management	Incident Identification, incident logging, categorization and prioritization, resolution, closure and communication to all the stakeholders at a high-level.
Change Management	Planning and tracking a change to a Configuration Item to meet the defined business requirements at a high level.
Release Management	Planning, preparing, scheduling, and deployment or distribution of release content to meet the business requirements. Controls and checks defined as part of Configuration and Change Management guide.
Capacity Management	Ensuring that the IT infrastructure can provide IT services at the SLAs in the most efficient and optimum manner feasible.
Service Continuity Management	Managing risks that might adversely affect the performance of IT Services or disrupt business continuity.
Service Level Management	Designing, monitoring, and reporting on service levels to make sure that agreed to SLAs are being met
Configuration Management	Tracking the individual configuration items that would contribute towards building and maintaining an IT solution to meet the defined business requirements

Figure 3.10.4-31. ITIL Process Areas. A brief description of each process area that interacts with CM.

Team CNSI's CM methodology is based upon the following terms:

- Configuration Item (CI): Defined as any artifact that needs to be managed to deliver an IT service; it can be a hardware artifact, source code artifact, software artifact, document, or an IT service.
- Baseline: Defined as a snapshot of the CI or set of CIs frozen and recorded at a point of time; it can be used to restore an IT service to a given state should something go wrong or as a reference point for any change that might be required.

Figure 3.10.4-32 summarizes the tools that will be used for each of the ITIL Process areas.

ITIL	Tools
Incident Management	Open Ticket Request System (OTRS)
Change Management/Configuration Management	SharePoint/Jira/ iTOP
Release Management	Subversion/Jira/SharePoint/MW Ops Portal
Capacity Management	HealthBeat
Service Continuity Management	HealthBeat/SLA Monitoring
Service Level Management	HealthBeat/SLA Monitoring

Figure 3.10.4-32. Implementation Tools by ITIL Process Areas. Lists various tools used for the ITIL Process areas.

Configuration Management Methodology

CM is the discipline that applies technical and administrative directions to:

- Managing product baselines
- Identifying CIs
- Controlling changes to CIs
- Recording and reporting information as needed to manage CIs
- Auditing CIs to verify conformance

Figure 3.10.4-33 lists Team CNSI's CM methodology. The remaining sections of this response section present various aspects of our CM methodology.

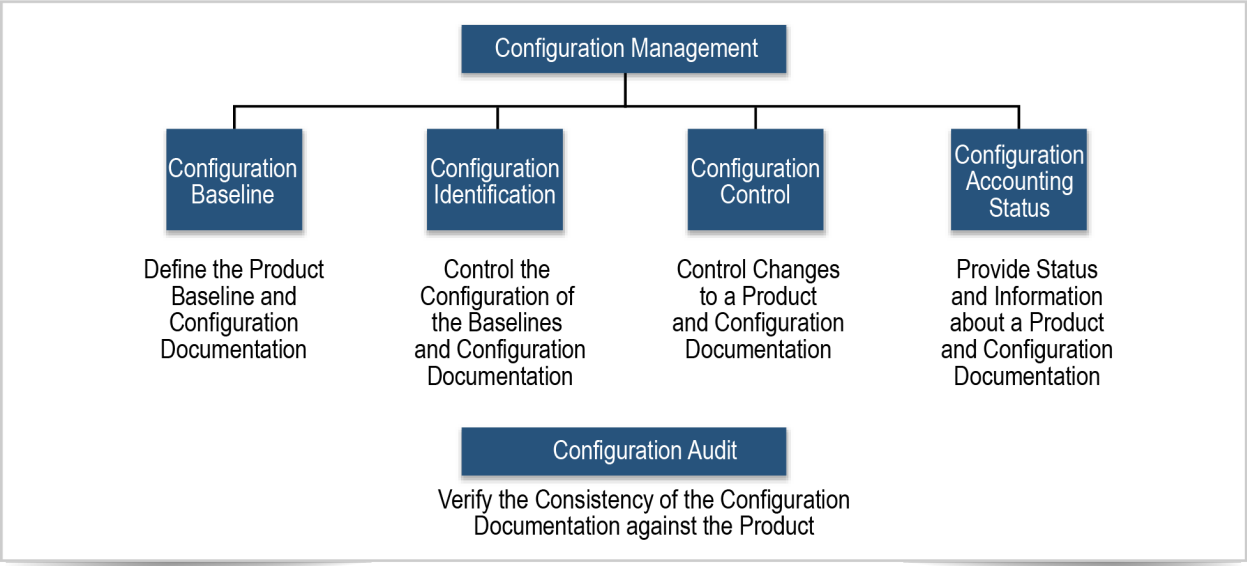


Figure 3.10.4-33. Components of Team CNSI's SCM Methodology. This methodology provides complete traceability and transparency throughout the SDLC phases.

Configuration Baseline

The objective of establishing a baseline is to define a basis for further activities performed as part of iVision360 framework in implementing and integrating the modules for evoBrix PMIS solution, and allow reference to, control of, and traceability among various CIs.

- A baseline is established for both software (source code) and document CIs
- Change control procedures are performed to develop a derivative baseline from an established one

Configuration Identification

Configuration identification consists of setting and maintaining baselines that define the module at any given point in time. Each baseline is assigned a unique label using the configuration naming convention.

The criteria for configuration identification include the following:

- The item will be used by one or more groups
- The item is expected to change over time due to defects logged or enhancements
- The item is either dependent on another item or triggers a change in other items because of a change in this one
- The item is critical to the project

Figure 3.10.4-34 lists the various types of CIs that exist on the project.

Type of CI	Description
Source Code	Project source code
Status Records	Records in Jira or SharePoint providing a snapshot of the CI status

Type of CI	Description
Document	Documents created as part of project activities
Hardware	Servers and routers that help implement the project activities

Figure 3.10.4-34. Types of CIs. Various types of CIs will be tracked for the entirety of evoBrix PMIS solution.

Figure 3.10.4-35 lists the applicable CMDB for each of the CIs in the system.

Name	Type of CI	Repository	Configuration Control Trigger
Java, JSP, XML, JS, PL/SQL, SQL, CSS, HTML, Images	Source code	Subversion	Initiation of the project
Source Code Defects/Enhancement Requests	Status Records	Jira	Submission to State
Formal Document Deliverables, as defined in the CDML	Document	SharePoint	Submission to the State
Servers, Routers, Switches	Document	iTOP/Wiki	Initiation of the Project
Non-Contract Deliverables, as defined in the Project Work Plan	Document	SharePoint	Approval by Delivery Manager/Director

Figure 3.10.4-35. Items Under Configuration Management. Lists each type of CI, repository where it will be stored and the phase that the CI will be placed under configuration control.

Figure 3.10.4-36 lists all the tools that form the CMDB system for the evoBrix PMIS solution implementation. The SCM Team automates the building and deployment of software to enhance integrity, reliability, repeatability, and traceability of the product. Much of the automation revolves around build and deployment scripting, which is in turn versioned along with the source code in Subversion (SVN).

Figure 3.10.4-36 provides a summary of Team CNSI's Configuration Management toolset.

Tool	Task	Description
SharePoint	Tracking Project Documentation	Collection and tracking of project documentation, including manuals, plans, status reports, meeting minutes, and project-related artifacts including Solution/Configuration Mapping Documents.
SVN	Managing Code Development and CIs	Management of code development and tracking of versions of CIs. A separate SVN Software Development Library server is used to maintain the repository.
Jira	Managing CRs	Management of CRs to the source code baseline. The Jira database is maintained on a separate server.
OTRS	Managing Requests Post Deployment Phase	Management of incidents once the project is live. Triaging of these incidents will result in defects and enhancements being logged into Jira or SharePoint.
HealthBeat	Displaying Capacity Planning/SLA Management	Enables system performance metrics and capacity planning for future and current needs.
iTOP	Hardware Asset Management	Management of all hardware CIs to manage multiple environments.
Hudson/Jenkins	Build/Continuous Integration	Build tool to facilitate continuous integration.
Operations Management Portal (OMP)	Manage User Access Requests	In-house tool to track all access requests.

Figure 3.10.4-36. CM Tools. Lists the CM Tool for each responsibility executed as part of providing day to day support for evoBrix PMIS solution.

Configuration Status Accounting

The purpose of status accounting is to ensure that the integrity of individual configuration items and the associated baselines are established and maintained. This requires the following:

- Configuration records describing CIs and baselines
- Audits to maintain the integrity of the baselines
- Every activity related to source code, defects or enhancements, and document changes in SVN, Jira, and SharePoint is recorded in sufficient detail so that the content and status of each work product is known and previous versions can be recovered.

Jira and SharePoint provide an ad hoc reporting capability to allow the stakeholders to produce a daily, weekly, or monthly status report as needed that can summarize:

- CRs in process
- Total open vs. closed CRs
- CR aging reports

Configuration Audits

The CM Team will conduct several types of audits throughout the applicable iVision360 phases:

- Periodic Physical Compliance Audits (PCAs) for CIs in SVN and Jira
- Status Accounting for CIs in SVN and Jira

Project Managers conduct Periodic Physical Configuration and Status Accounting audits throughout the project life cycle for project documentation in SharePoint.

Quality Assurance (QA) Teams will audit CM activities and review the PCA reports as part of the Process and Product Quality Assurance (PPQA) process.

The audit reports will at a minimum contain the content shown in Figure 3.10.4-37.

Section	Description
Audit Description	This section also identifies the methodology used in conducting the audit. Team members are identified along with their functional specialties. Any specific assumptions/known-issues are called out. Action Items are listed and tracked for completion.
Summary of Audit Findings	Summarizes the findings of the audit. Identifies those areas having an impact on production, if applicable. Includes a general discussion of the overall evaluation of the efforts.
Recommendations	Suggests specific methods to correct identified deficiencies. If applicable, recommendations are made concerning the necessity for any audit follow-ups and tracked to completion by the CM Manager.

Figure 3.10.4-37. Sample Audit Report. Lists sections that are a part of a typical audit report.

Governance Authority for Each Configuration Item within CMDB

Change Control as described in the Change Management Plan is the guiding document for providing the governance framework for each configuration item in the Team CNSI CMDB ecosystem. It includes the systematic evaluation, coordination, development, approval or disapproval, and implementation of changes after the establishment of a baseline. CRs are tracked from inception to final resolution, ensuring that a standard repeatable process is maintained for handling proposed changes and that unauthorized changes are not introduced into the controlled baseline.

Figure 3.10.4-38 is a mapping of a role-name that is responsible for each type of CI throughout the duration of the project.

Role Name	Type of CI	Repository
Module Team Lead/Development Manager/Configuration (Functional) Manager/Quality Manager	Source code	Subversion
Configuration (Functional) Manager/Test Manager/Development Manager	Status Records	Jira
Configuration (Functional) Manager/Test Manager/Development Manager	Document	SharePoint
Systems Team Managers/Leads	Hardware	iTOP/Wiki

Figure 3.10.4-38. Role Authority Mapping. Shows role authority mapping for each CMDB.

Hardware Change Management

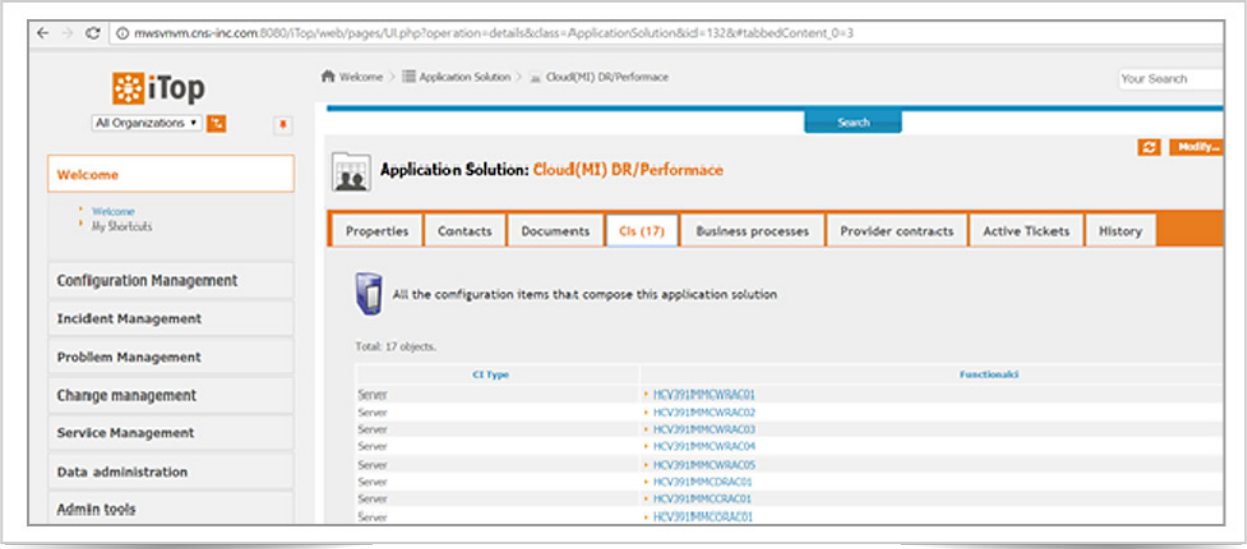
This section describes the functions of the CCB as it relates to the management of hardware changes for the evoBrix PMIS solution. Direction is determined by consensus of all organizations represented at the board including, at a minimum, personnel from Team CNSI, the SI vendor, and the DPHHS PMO.

The CCB represents the interests of project management by ensuring that a structured process is used to consider purchases or upgrades for hardware and supporting the installation of the hardware to support evoBrix PMIS solution.

The Change Control Board:

- Requests that impact analysis of proposed hardware changes be performed
- Reviews the hardware changes
- Makes decisions regarding hardware
- Monitors progress of the hardware installation
- Communicates decisions made to affected groups and individuals

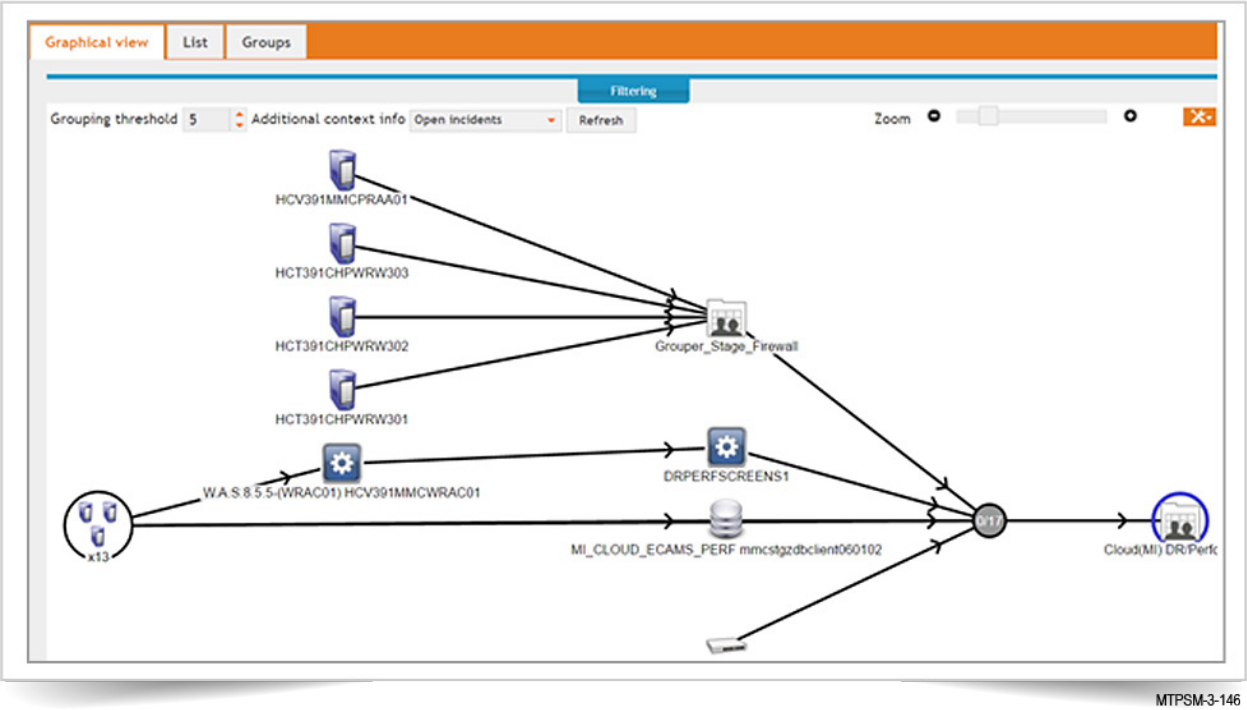
Team CNSI maintains the hardware for the evoBrix solution and it is listed in iTOP CMDB maintained by Team CNSI personnel. Figure 3.10.4-39 shows a snapshot of a list of hardware CIs available in the CMDB.



MTPSM-3-149

Figure 3.10.4-39. iTOP CMDB. Team CNSI's tool for tracking Hardware CIs.

Once all the CIs are entered, the CMDB tool allows team members to establish relationships among them showing a layout of all the hardware CIs that constitute a logical environment, as shown in Figure 3.10.4-40. The tool records the time and action to provide an audit trail of changes made to a CI.



MTPSM-3-146

Figure 3.10.4-40. Graphical Representation of Hardware CIs Constituting a Logical Environment. Helps plan for maintenance, availability, and system health of a given logical environment

Separate audits are performed by Team CNSI against the bill of materials (BOM) whenever new hardware for the evoBrix PMIS solution is received in one of the designated datacenters.

COTS Components

Each of the COTS products (e.g., Oracle Database, Oracle WebLogic, and Siebel) is treated as a configuration item, and the current version is recorded as part of the product baseline. Configuration changes and patches necessary to maintain optimum performance levels per the project requirements are discussed between all the concerned stakeholders in CCB, scheduled and implemented as part of the agreed Release and Maintenance cycle, and results are captured at each stage.

A major release for a COTS product would typically include major changes to the feature set of the tools, adherence to new J2EE framework, or becoming cloud-enabled. Minor changes to COTS products typically involve patches to fix identified issues reported by the user-community in general or fixing any security vulnerabilities that are discovered.

Documentation Change Management

This section describes the functions of the CCB as it relates to the management of documentation changes for the evoBrix PMIS solution. Direction will be determined by consensus of all organizations represented at the board which would at a minimum include personnel from Team CNSI, the SI vendor, and the DPHHS PMO.

The Change Control Board:

- Requests that impact analysis of proposed documentation changes be performed
- Reviews CRs that impact project documents
- Makes decisions regarding CRs
- Monitors progress of documentation delivery and change implementation
- Communicates decisions made to affected groups and individuals

The CCB operates as follows:

- CCB meetings are held periodically as determined by the CCB representatives in attendance
- The CCB Chair or Moderator, as defined in the Project Management Plan (PMP), facilitates the meetings and ensures that meeting notes are distributed

The CCB performs the following functions:

- Oversees the release calendar
- Evaluates and approves release content
- Confirms implementation of releases and documentation updates

The CCB provides oversight to the change management process areas including:

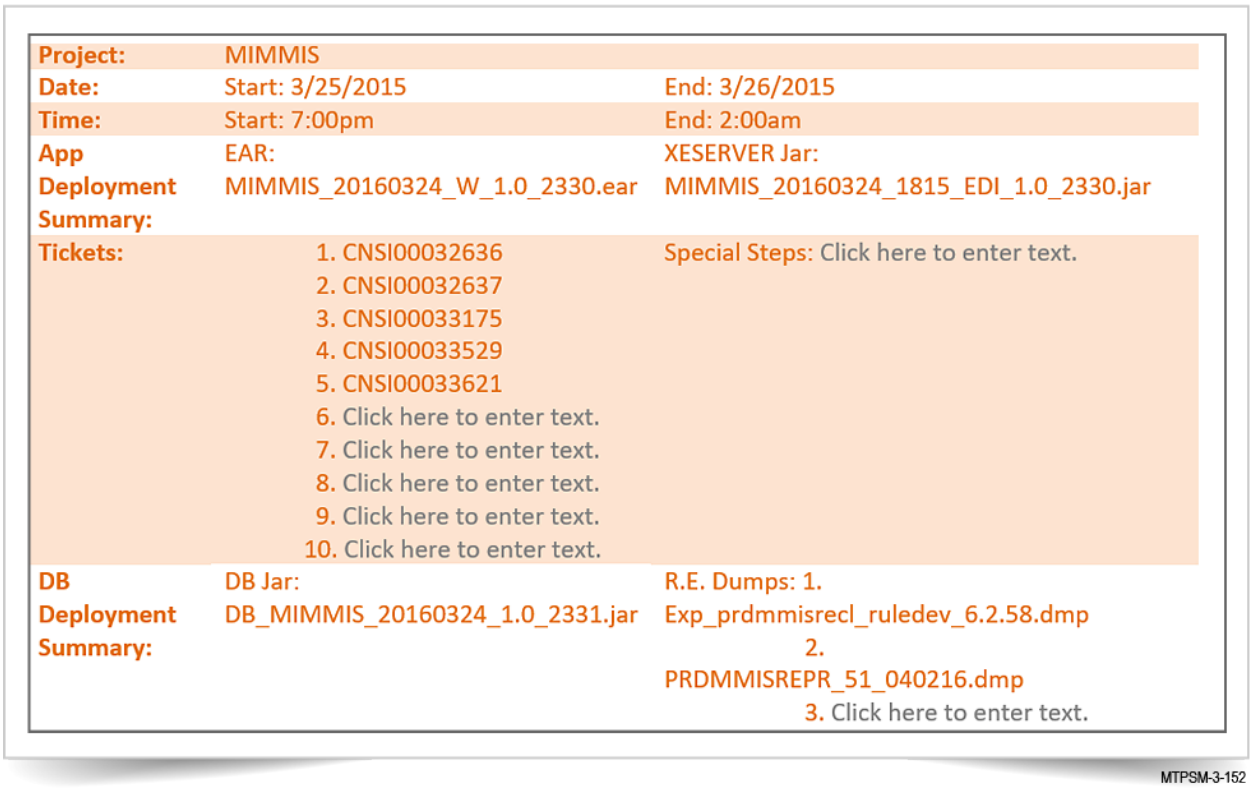
- Managing CRs
- Solution, configuration, and testing
- Deploying

All project documentation work products as defined in the Project Schedule (contract deliverables, non-contractual work products and internal documentation) are maintained in SharePoint to allow for sharing among the project team. Each project has its own work product portal within SharePoint.

Examples of documentation work products include the following:

- Project Management Plan (contract deliverable)
- Configuration Management Plan (CMP) (internal)

Most of the configuration changes will be part of the source code binary bundle that is built out of the source code version control system, and the remainder is part of data-scripts that is all packaged together when time comes for code promotion from one environment to another, all the way up to Production. Figure 3.10.4-41 shows a checklist form that is used for verification and validation of all the changed CIs during every Production release.



Project:	MIMMIS	
Date:	Start: 3/25/2015	End: 3/26/2015
Time:	Start: 7:00pm	End: 2:00am
App Deployment Summary:	EAR: MIMMIS_20160324_W_1.0_2330.ear	XESERVER Jar: MIMMIS_20160324_1815_EDI_1.0_2330.jar
Tickets:	1. CNSI00032636 2. CNSI00032637 3. CNSI00033175 4. CNSI00033529 5. CNSI00033621 6. Click here to enter text. 7. Click here to enter text. 8. Click here to enter text. 9. Click here to enter text. 10. Click here to enter text.	Special Steps: Click here to enter text.
DB Deployment Summary:	DB Jar: DB_MIMMIS_20160324_1.0_2331.jar	R.E. Dumps: 1. Exp_prdmmisrecl_ruledev_6.2.58.dmp 2. PRDMMISREPR_51_040216.dmp 3. Click here to enter text.

MTPSM-3-152

Figure 3.10.4-41. Snapshot Checklist of Various Types of CIs. Representation of various types of CIs such as Application, Database, and Infrastructure changes that are packaged and verified among various teams before and after Production release.

A graphical representation of the steps followed along with the various teams that participate through the lifecycle of the change request is shown in Figure 3.10.4-42.

There is a comprehensive check performed by the Configuration (Functional) or Development Team in coordination with the Release Team at each stage of code promotion from one Test environment to another to make sure that all the configuration changes promised for a given release are available in the bundle.

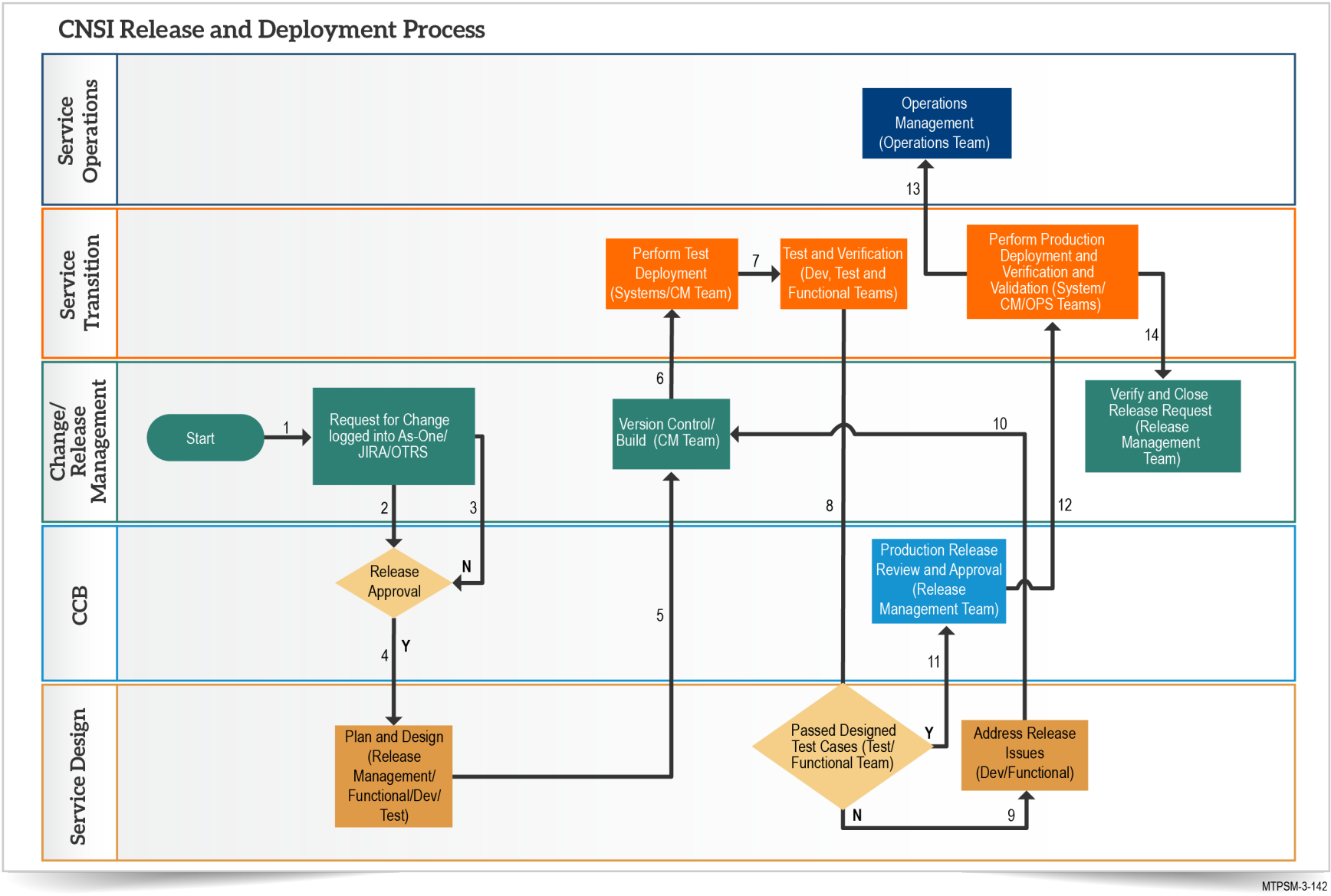


Figure 3.10.4-42. Change Request Lifecycle. Describes the lifecycle of the change request.

When the time comes for code-promotion to Production, a comprehensive check is performed, independently of each other, by the SCM Team and Configuration (Functional) and Development Team in coordination with the Release Management Team, and the lists are reconciled.

Once the code-promotion activity is complete in Production, another thorough round of checks is performed to validate the configuration changes across each of the modules or COTS product that was changed during the release process by authorized personnel across Configuration (Functional) and Development (Operations) Teams. The typical areas of checks cover application screens, Database, Interfaces, web service, Reports, and any infrastructure changes, at a minimum.

Once the systems are brought up, there is a comprehensive non-intrusive sanity check performed by the Operations and Configuration (Functional) teams to make sure all configuration changes planned for the release are applied and working as desired. The Release activity is marked as complete with necessary notifications to the concerned stakeholders after this last step of non-intrusive checks. A similar process is followed during every major release in lower environments as well.

The evoBrix PMIS solution is configured to comply with state and federal policies, laws, statutes, and guidelines. The solution will enforce these as business rules. Team CNSI will work with DPHHS to cross-reference the regulations and policies to the Detailed System Design Document (DSDD) that outlines these business rules. The business rules are then implemented by making an authorized change to the applicable configuration item stored in its respective CMDB repository. The requested change could result in an upgrade to evoBrix PMIS solution or a COTS supporting the solution. For example, if a business rule implementation involves change to a hardware or software (COTS) CI, it would be recorded in iTOP CMDB. Similarly, if it involves change to source code CI, it would be recorded in a combination of SVN and Jira, SharePoint, or OTRS. These configuration changes are then tracked, controlled, and promoted per the agreed release cycle between Team CNSI and DPHHS. This process enables traceability and mapping for a given change request all the way from initial request to final implementation and closure in terms of functionality and documentation. The process has been refined through several iterations as needed after incorporating lessons learned from Team CNSI's successful rollouts of 4010, 5010, ICD-10, Affordable Care Act mandates on our CHAMPS and ProviderOne programs, thereby providing a proven process model for the evoBrix PMIS solution.

Change (Enhancements) & Incidents (Defects)

Team CNSI follows its proven change management practices throughout the project life cycle. Change management during implementation is applicable to any change that affects the baseline project scope, approved deliverable, or scheduled completion dates. During operations, change management is applicable to enhancements to the system in production, changes to production data, interface scheduling, and other configuration changes. Team CNSI's change management process addresses the following:

- Activities that occur when a change is proposed
- Personnel roles and responsibilities in the initiation, impact analysis, review, and approval of changes
- Team CNSI's project manager oversees changes for the DPHHS MT PSM project and uses the following process:
    - Receive change request
    - Assign for review and analysis
    - Analyze alternative and identify recommendation
    - Prepare costs, schedule, and scope impact analysis
    - Present proposed changes to DPHHS and relevant stakeholders
    - Update affected baselines if approval is received

Additional details on change management are provided in 3.10.2.1 Project Management.

Conducting research requested by the State or required to support the Department

Continuous Improvement is one of the core focus areas for all of practice areas of Team CNSI. As part of it, we constantly leverage ITIL v3 processes recently assessed at CMMI L3. The toolset used by Team CNSI provides for an automatic capturing of relationships between various CIs such as source code, documentation, hardware, and software, and also captures any actions to change them as part of audit history. It helps provide for automated builds and deployments and full traceability and transparency across iVision360 SDLC phases. All of these steps contribute toward getting a successful and certified CMS system. Complying with PCI standards for all of Team CNSI's Software installations on State of Michigan Hardware is one such example.

Performing mass adjustments or mass changes as requested by the State or required to support the State's healthcare programs

Mass adjustments or mass changes requested by the State are handled by Team CNSI, via the Operations Request for Change (RFC) Process. This process is used when there is no evoBrix screen functionality availability to complete the task. Requests originate via the Open Source Ticket Request System (OTRS) and then get converted by Team CNSI into a Jira operational RFC ticket. Jira is a tool used to plan, track, and release system changes.

The primary reasons for Operational Data Scripts and Configuration changes are:

- Schedule changes for Interfaces, Database to Database (DB2DB) jobs, and Data Warehouse jobs due to business needs or changes from external entities
- Queue changes due to fluctuations in transaction volumes or to handle specific problems on a temporary basis
- Data scripts that are needed due to application issues
- Data scripts that are requested by the State for some business purpose – often one-time requests with short notice and thus not candidates to be part of the regular release process

The RFC process proceeds as follows:

- State and Team CNSI identifies the need for a change, an OTRS ticket is created by the state.
- The developer creates a Team CNSI Jira Ticket to perform the necessary change and tie the RFC ticket number to OTRS ticket.
- The requestor must provide the following information:
    - Change Type – Regular, Emergency, or Ongoing
    - Request Type – RFC-Queue, RFC-Interface, RFC-DB2DB, RFC-DW Extract, RFC-Cognos, or RFC-Data Script
    - Regression Required (Yes/No)
    - For non-Data Script requests:
- All Data Requests must be reviewed by RFC Reviewer and approved by RFC Decision Maker. (Notify via email "RFC Review Team" mi_rfc_review@cns-inc.com.)
- The RFC tickets will be reviewed and approved at the Monday and Thursday Production Scheduling meetings.
- Change request submitted outside regular Monday and Thursday morning review is considered as Emergency which requires Operations Management approval.

- Emergency requests can be made through the RFC ticket outside of the normal Production Schedule meeting, but they must meet the following criteria before being considered:
  - They cannot wait until the next Production scheduling meeting
  - Be approved by the Operations Management
  - Emergency requests will go through regular review process after Operations Management approval
  - Email Operations Management and RFC Review Team that an RFC needs to be reviewed and approved
  - The CM and DBA team will not process any requests not approved through the RFC process
  - During the Production Scheduling meeting, the status of all the previous week's requests will be reviewed and updated

Performance Optimization

Applications

Team CNSI best practices are created based on the experience earned from various successful implementations such as in Michigan and Illinois, with a focus on SaaS Operations in addition to leveraging practices as defined in industry standards like ITIL and CMMI. These will be further refined to cater to the needs of the Montana implementation. Typical performance optimization activities include tuning Java Virtual Machine (JVM), implementing horizontal and vertical scaling as needed to meet the requirements, and data archival on file systems of Application Servers to maintain optimum performance.

Databases

Team CNSI's solution includes a comprehensive and complete system performance monitoring framework which helps to optimize it. A combination of Oracle Enterprise Manager (OEM) and various other Oracle tools and solutions provide monitoring capabilities covering all layers of hardware and software components to improve performance.

Team CNSI constantly monitors the database performance tuning using various techniques which include:

DB Instance Tuning: Ensures the instance is properly tuned by allocating sufficient memory to database structures, determining I/O requirements, and modifying the resources accordingly to avoid bottlenecks that could lead to performance problems.

SQL Tuning: Involves frequently visiting the long running SQL statements and identifying the SQLs that are responsible for high resource utilization and impact the overall system performance, and tuning them to meet the SLAs.

OEM: Proficient in Oracle Enterprise Manager which helps to properly tune all aspects of the database management using inbuilt features like AWR, ADDM, ASH for SQL, and database tuning.

CTR: An in-house centralized repository cloud-based tool built to run the scheduled maintenance jobs across all the databases in all the environments to keep up the database health good. Some of the tools include:

- Hourly stats jobs for core real-time tables
- Daily/weekly transactional and optimizer table maintenance jobs
- Monthly purge and archive jobs during a specified downtime
- Frequent data usage reports which helps to analyze the system data usage and plan the future usage
- Alert mechanism to trigger alerts to respective teams during any issues

Oracle TFA: Use Oracle Trace File Analyzer which helps to analyze and collect diagnostic data, which is a crucial step to resolving problems that may occur with the Database. It collects data across cluster nodes and consolidates everything in one place which comes handy when debugging any issues.

Oracle APM: Team CNSI Leverages Oracle APM which collects, organizes, and publishes the rich set of data that is collected via its repository. It is part of a comprehensive repository, a software library, and tracking of additional information for managing problems and incidents which also integrates with Enterprise Manager. This integrated approach in the Enterprise Manager repository enables integrated tools to be built, erasing the artificial boundaries between application performance management, configuration management and change management. In addition, because the repository is built on Oracle Database, technologies such as Data Guard and Real Application Cluster can be used to ensure that the database is highly availability and scalable.

Database Management

Team CNSI's EvoBrix architecture has become robust, highly available, scalable, and portable with our continued learning from more than a decade in the MMIS industry. Our database design incorporates MITA principles, as is suitable for an MMIS application, and our data model is designed to support the highest levels of data integrity, security, and control while reducing the burden of management. Team CNSI's proven, MITA-aligned data model, powered by Oracle, creates a robust solution that can fully address the requirements of the State today and support its needs in the future. The data model was designed within each business area to ensure that all data requirements of that business area are fully captured. The business areas are then integrated to create the larger, complete EvoBrix database which supports all functions required of an MMIS.

Team CNSI uses various tools and techniques to effectively manage the database. Figure 3.10.4-43 shows the high-level architecture and interactions with the centralized repository tool which monitors, maintains, and manages all the databases from a central location.

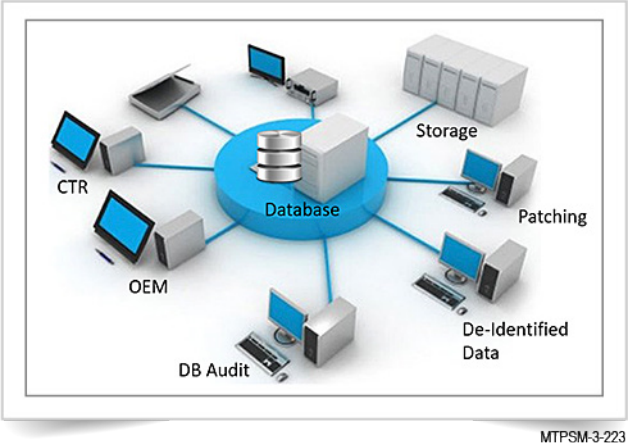


Figure 3.10.4-43. Centralized Repository Tool. A custom tool which monitors, maintains, and manages all the databases from a central location.

CTR: Centralized repository tool is a custom tool built based out of cloud architecture which monitors, maintains and manages all the databases from a central location. All the jobs are scheduled to run at the certain time based on the requirements. Adding a new database to the monitoring list is as easy as adding a row to a table.

Some of the tasks that it performs include:

- Hourly stats job for core real time tables for the best screen response times
- Daily/weekly stats job for all other transaction tables
- Weekly/Monthly Optimizer stats which helps to maintain the data dictionary
- Monthly Purge activity to archive the older data
- Defragment the tables that are highly fragmented
- Modify the passwords of core schemas periodically as per the DB audit requirements
- Automated user management

OEM: Team CNSI database administrators and system administrators use OEM to maintain, monitor, and configure proactive alerts for Oracle databases, SOA Suite, and Application Servers. OEM has been architected in such a way that the Team CNSI's Network Operations Center (NOC), located in our Center of Excellence (COE), provides a 24x7x365 monitoring of infrastructure and applications. NOC triages issues to the appropriate operations team for corrective action. By monitoring trending data, we can determine if a system will have issues down the road. For example, if we see that a system is spiking on central processing unit (CPU) usage and memory on a regular basis, that system may require a hardware upgrade or optimization to remove capacity concerns.

DB Patching: To meet all the audit standards and to keep the environment secure, Team CNSI DBAs apply CPU patches to all the databases every quarter. Proper testing of the patch happens across lower environments before patching the production to avoid all patch related issues.

Performance Tuning: Team CNSI uses the latest techniques and all available tools to tune the databases and the everyday SQLs to keep up the SLA. OEM plays a major role while tuning the system by enabling different reports such as AWR, ADDM, ASH, and advisory tools, which give more details to debug the issue.

Database Refresh: Team CNSI ensures that all the environments are synced up with the latest data after every production release. The whole database refresh process is highly automated to keep up with the timelines and keep downtime as short as possible. Automation happens using the Oracle Recovery Manager and a restore/recover process.

Data De-identification: De-identification is the process of removal of specified PHI as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information, as in PII, to identify the individual. Team CNSI uses a fast, reliable, and secure in-house built data de-identification solution that comes with templates out-of-the-box. Using this tool, all the transaction data that moves to the development databases will be de-identified and secured.

Database Audit: Team CNSI ensures that the database complies with all industry standards, such as those from the Center for Internet Security (CIS). A custom-made audit tool is used to scan all the databases to check for vulnerabilities and send the results to the necessary teams in the form of reports. These reports are used to analyze and make necessary changes for remediation. This tool is updated periodically with the latest audit requirements and run across all the databases periodically.

Encryption: All network traffic flowing out of databases is fully encrypted using Oracle Network Encryption. This protects all PII and PHI data from snooping on the network. Data at rest encryption is done using Oracle Transparent Database Encryption (TDE). All encryption is fully in compliance with MARS-E, CMS, and NIST standards for data security. Any data transfer into and out of the system uses only secure encrypted data transfer tools. All access by personnel to the backend systems is via encrypted VPN connections as well. The different encryptions that are being used are:

- Network Encryption: Encrypts network traffic to/from the database to application servers
- Data at Rest Encryption: Data present in database files are encrypted at rest
- SAN Storage Encryption: Protects data when it leaves physically secure SAN
- RMAN Encryption: Encryption happens during the database RMAN backup
- Encrypted Flat Files: Flat files are encrypted with a password before sharing

Software, Hardware, and Tools (e.g., patches, upgrades, and replacement)

Database Patching: To meet all the audit standards and to keep the environment secure, Team CNSI's DBA Team applies Oracle Critical Patch Update patches to all the databases, once every quarter during the monthly maintenance window. Critical Patch Update Patches are collections of security fixes for Oracle products. These Patches are applied within 60 days of their release, in accordance with CIS Benchmarks. Proper testing of the Critical Patch Update Patches happens across non-production environments first, before patching the production instances. In addition to Critical Patch Update Patches, Team CNSI will also apply the Oracle Patch Set Updates (PSU) Patches in a timely manner. These PSU patches are patches for known database issues and bugs and they are applied within six months of their release. They are also tested in lower/non-production environments first, before being applied to Production databases. All patching activities are planned in advance and they will be carried out only during scheduled outage windows.

Making Corrections or Changes to Maintain the Integrity of the System or the Data Within It

Data Integrity refers to the accuracy and consistency of data stored in a database, data warehouse, data mart or other construct. The integrity of data is guarded by specific business rules called data integrity constraints. The rules that apply in the real world to events, actions, manipulations, and situations are translated into constraints that apply to the data handled in information systems.

Data Integrity is maintained in various way based on the scenarios. Team CNSI uses Oracle features and tools and custom tools to maintain the Data Integrity by keeping it highly secure.

Oracle Flashback Technique

This solution performs point-in-time recovery from human errors. It also let users view past states of database objects or to return database objects to a previous state without using point-in-time media recovery.

The following features are an integral part of Team CNSI's Flashback solution:

- Flashback Database: Rewinds database back in time
- Flashback Query: Retrieve data for a time in the past
- Flashback Version Query: Retrieve metadata and historical data for a specific time interval
- Flashback Transaction Query: Retrieve metadata and historical data for a given transaction or for all transactions in each time interval
- Flashback Transaction: Roll back a transaction and its dependent transactions while the database remains online

Database Archiving: Team CNSI ensures that the data gets archived periodically there by results in storage savings. There are various scheduled jobs that runs weekly/monthly to archive the older data which is not required for daily operations. This data is stored in the binary format and gets compressed, encrypted before moving to the archive area. Also, this data can also be retrieved if needed in the future.

Data Manipulations: A dedicated team is assigned to perform any database related deployments who works 24X7. Any immediate data changes including emergency data rollback/cleansing corrupt data will be performed this team to avoid any data issues. All the changes are recorded using version control for future use.

DataGuard: Team CNSI sets up Oracle Data Guard for production to keep it ready for disaster recovery. Oracle Data Guard ensures high availability, data protection, and disaster recovery for enterprise data.

©2017 CNSI

Data Guard provides a comprehensive set of services that create, maintain, manage, and monitor one or more standby databases to enable production Oracle databases to survive disasters and data corruptions. Data Guard maintains these standby databases as transactionally consistent copies of the production database. Then, if the production database becomes unavailable because of a planned or an unplanned outage, Data Guard can switch any standby database to the production role, minimizing the downtime associated with the outage. Data Guard can be used with traditional backup, restoration, and cluster techniques to provide a high level of data protection and data availability.

Security: Team CNSI implements various encryption techniques starting from the network layer to filesystem. Techniques include Transparent Data Encryption (TDE), Network Encryption, SAN Encryption, and file-level OS encryption.

TDE: Team CNSI uses Oracle TDE, which encrypts sensitive application data on storage media completely transparent to the application. It is encrypting the data in the data files so that in case they are obtained by other parties, it will not be possible to access the clear text data. In the databases where TDE is configured, any user who has access on an encrypted table will be able to see the data in clear text because Oracle will transparently decrypt the data for any user having the necessary privileges. Tablespace level encryption is enabled and all the tables that have PHI/PII is identified and moved to the encrypted tablespaces.

N/W Encryption: All the database connections and the associated data that transfers across the network is encrypted via algorithms such as AES256. This is enabled at the host level, which means all of the sqlnet connections arriving to the databases hosted in that server are network encrypted. This setting is enabled across all the environments keeping the databases secure.

SAN Storage Encryption: Protects data when it leaves physically secure SAN.

RMAN Encryption: Encryption happens during the database RMAN backup.

Encrypted Flat Files: Flat files are encrypted with a password before sharing.

ASM Redundancy: ASM redundancy is one of the key features of Oracle ASM, and means that the data is striped across multiple disks, thus safeguarding the data against the loss of any one disk. There are different levels of redundancy but NORMAL and HIGH levels are typically used.

- **NORMAL:** Data is striped across two disks using NORMAL redundancy which means there is one duplicate copy of data at all times which can be used during any physical disk failures. NORMAL is chosen for all Development, Test, and UAT databases.
- **HIGH:** Data is striped across three disks using HIGH redundancy which means there are two duplicate copies of data at all times which can be used during any physical disk failures. HIGH is chosen for all Production databases.

Performing the Activities Above to Maintain Customizations Implemented as Part of an Approved Enhancement

Any specific customization made for Montana, such as Functional Specification Documents, Training Documents, and Online Help Files, would be documented where appropriate and made available. If a change is needed for Online Help Files, it is typically rolled out with a scheduled code release after appropriate testing and due approvals from all the stakeholders.

Perform Incremental Integration Services

Team CNSI follows the processes mentioned in its iVision360 document as its SDLC. Built into this process is the Iteration model, where every change is built in an incremental mode on an existing baseline of the Product. Each of the incremental change is made after appropriate approvals in a very controlled manner so that it can be thoroughly tested and fixed prior to Production rollout. When the time comes for the next iteration, the previous snapshot becomes the baseline, making sure all integration changes approved in the design phase are accommodated and tested.

OMC05

The Contractor shall provide a notification web page that displays when the system is unavailable for scheduled maintenance or unscheduled outages.

Scheduled Outage Banner

Team CNSI utilizes the Provider Portal to Banner Messages for Scheduled outages. The State will initiate the request to post a banner message via an OTRS ticket and a Team CNSI will open Operational change request (RFC) to ensure that the banner message is posted on the Provider Portal website. Figure 3.10.4-44 shows an example banner message for a planned outage on the Provider Portal.

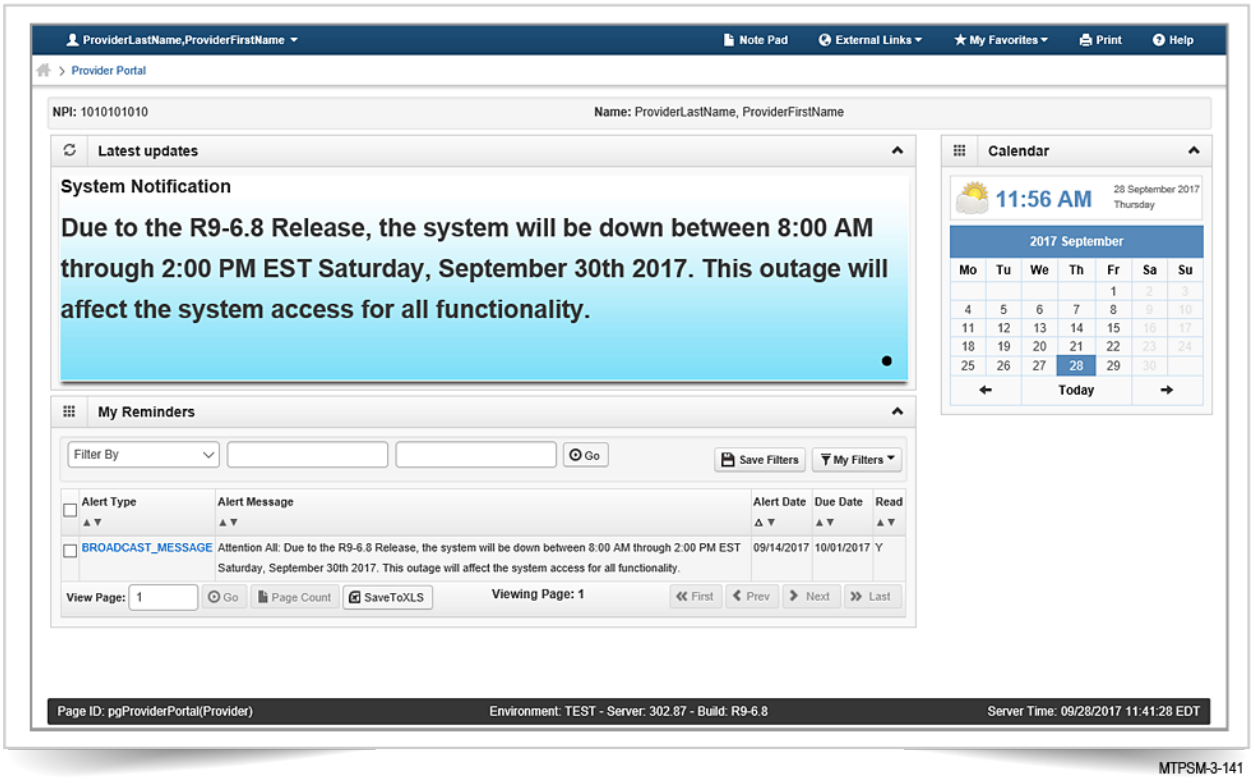


Figure 3.10.4-44. Example Banner Message for a Planned Outage. Banner messages are posted on the provider portal.

Unscheduled Outages

Unscheduled outages messages are posted at a web server level. These messages are posted if there is an unscheduled outage or as a result of emergency maintenance. Figure 3.10.4-45 shows an example banner message as a result of evoBrix being unavailable for unplanned maintenance.

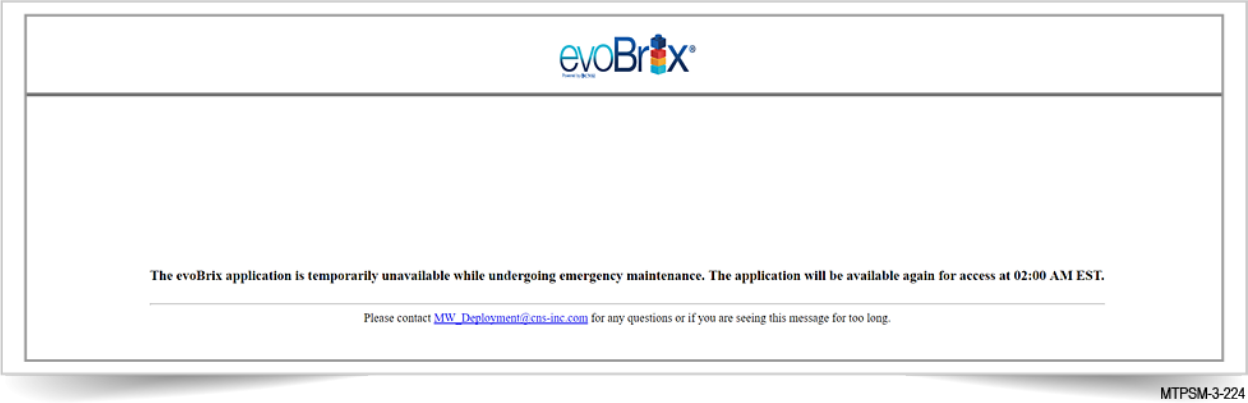


Figure 3.10.4-45. Example Banner Message for an Unplanned Maintenance. Banner messages are posted in the event the application is temporary down due to unplanned maintenance.

OMC06

The Contractor shall have processes in place to restrict access when inappropriate system access or misuse is detected.

Team CNSI has a documented access control policy with roles and responsibilities that stipulate access to information system resources shall be based upon job function and standards for appropriate use, as documented in the Team CNSI Information Security Policy and Standards. Authorization to perform specific functions or to use specific resources will be granted according to the principle of least privilege: granting no individual more authority than reasonably required to perform assigned duties. The Security Policy and Standards document also constitutes what procedures to the organizations should take when system access is to be restricted when misuse is detected.

When inappropriate system access or misuse is detected or reported, an OTRS ticket will be logged by operations support staff containing the details of the incident and the user account in question will be suspended pending an investigation. The incident and suspension will be communicated to the user's supervisor and the user will be informed of the account suspension. Team CNSI's Information Security Manager and the DPHHS Security representative will also be informed.

Team CNSI's Information Security Manager will then work with the DPHHS Security representative to conduct a review of the incident. They will jointly produce a report of the incident with recommendations. Recommendations may include reinstatement of the account, continued account suspension, or termination of the account depending on the results of the investigation. The report will be shared with the user's supervisor as well as key project stake holders. Once a final determination is made, the OTRS ticket will be updated with the action to be taken and operations support staff will work with the DPHHS Security representative to update the user account status accordingly.

Since security incidents are considered confidential, the incident report will be encrypted and password protected and stored in a secure location for future reference.

OMC07

The Contractor shall test and implement all production ready patches, upgrades, and releases for all software, firmware and operating systems in a timely manner, in coordination with other modules.

Team CNSI has developed an extensive operational system and support infrastructure comprised of well-documented processes and procedures. Team CNSI's approach is built on an ITIL framework augmented by our own best practices refined over years of collective health care administration operations experience in managing large and complex projects. A key part of aligning with ITIL involves designing processes or "services" so changes are tested and introduced into an operations environment in a controlled and systematic manner. ITIL services represent a comprehensive set of practices, policies, procedures, and processes that enable us to focus on business and system value by providing consistent, predictable, and measurable results.

Team CNSI will provide an electronic notification via email to the release stakeholders including detailed release notes for Major and Minor version, patches, updates and fixes deployed to the test, state and production environments. The details of notification will be defined in the state approved release management process.

COTS Products

Each of the COTS products (e.g., Oracle Database, Cognos, EngageOne, Avaya, and Siebel) and hardware (Virtual Machines, Routers, and Servers) are also treated as CIs, and the current version is recorded as part of the product baseline. Configuration changes and patches that need to be applied to maintain optimum performance levels per the project requirements are discussed between all the concerned stakeholders in CCB, scheduled and implemented as part of the agreed Release and Maintenance cycle. Results are captured at each stage.

A major release for a COTS product/hardware would typically include major changes to the feature set of the tools, adherence to new framework and/or standards, or becoming cloud-enabled. Minor changes to COTS products/hardware typically involve patches to fix identified issues reported by the user community in general or fixing any security vulnerabilities that are discovered.

If a business rule implementation involves change to a hardware/software (COTS) CI along with source code CI, each of the respective change would be recorded in the assigned CMDB for that CI Type. For example, if it involves change to source code CI, it would be recorded in a combination of SVN and Jira/As-One/OTRS, hardware/COTS in iTOP CMDB and so on. These configuration changes are then tracked, controlled, and promoted per the agreed release cycle between Team CNSI and DPHHS. This process enables traceability/mapping for a given change request all the way from initial request to final implementation and closure in terms of functionality and documentation. The process has been refined through several iterations as needed, after incorporating lessons learned from Team CNSI's successful rollouts of 4010, 5010, ICD-10, ACA mandates on our CHAMPS and ProviderOne programs, thereby providing a proven process model.

OMC12

The Contractor shall notify the appropriate user community, as defined by the State, of system events (e.g., major system changes and system outages).

The Team CNSI operations team uses a defined communication process to effectively communicate outages to the DPHHS and trading partners. The email communications as well as banner messages posted to the Provider Portal are used to effectively communicate an outages and/or system downtime in advance.

All planned outages are communicated in advance. The notification period will vary depending on the type of outage. For Planned outages, Team CNSI's Operations Support Team will deploy a banner message to notify the system users of the outage. Team CNSI also sends an email communication to the stakeholder notifying them of the release and/or outage (see the below table).

For unplanned outages, Team CNSI will also send an email communication to the stakeholders notifying them of release and/or outage (see the below table). An example may be "Unexpected Downtime" which requires only 30 minutes' notice. Unplanned Outages may or may not require a Banner message depending on the impact and duration.

Team CNSI will continue to discuss the releases and outages in Tier 2 CCB and document them within the minutes. The HealthBeat calendar will also be available for use by state staff to provide a single view of all related events and outages. Figure 3.10.4-46 depicts the template for the communication types for notifying the appropriate users and stakeholders.

S#	Title	Description	Timeframe	Notification Method
1	Emergency Deficiency	Notifies the recipients that the system is down or severely impaired due to unexpected incident.	Within 15 minutes after the incident	Email
2	Emergency Deficiency - Resolution Plan	Notifies the recipients about the plan to restore all down or severely impaired functionality	Within 2 hours of the incident	Email
3	Emergency Deficiency Resolved	Notifies the recipients that the system function is restored to normal operating conditions. Includes a high-level root cause of the incident and the system impact.	Within 1 hour after the incident is resolved	Email
4	Monthly Maintenance - Outage	Notifies the recipients that the system will be down for maintenance during the scheduled monthly maintenance window.	5 working days prior to the outage	Banner Message Broadcast Message Email
5	Monthly Maintenance - Completion	Notifies the recipients that the monthly maintenance was completed after the sanity check.	Within 8 hours after the outage window	Email
6	Major release deployment - Outage	Notifies the recipients that the system will be down for the release deployment during the scheduled major release deployment.	2 weeks prior to the outage	Banner Message Broadcast Message Email
7	Major release deployment - Completion	Notifies the recipients that the major release deployment was completed after the sanity check.	Within 16 hours after the outage window	Email
8	Intermediate/Emergency release deployment - Outage	Notifies the recipients that the system will be down for the Intermediate/Emergency release deployment.	At least 2 days prior to the outage	Email
9	Intermediate/Emergency release deployment - Completion	Notifies the recipients that the Intermediate/Emergency release deployment was completed after the sanity check.	Within 8 hours after the outage window	Email

Figure 3.10.4-46. Team CNSI Communication Process. Provides time notification to the State and user community.

OMC15

The module Contractor shall provide help desk services to provide level 0 (customer self-service) level 1(basic support), level 2 (moderate support) that includes as appropriate, escalation to the State and level 3 (technical/integration) support related to the functionality of the module's scope of work. Level 1 help desk is the first point of contact and is responsible for logging the issue and, if possible, assisting the user.

Help Desk for System Issues and Requests

Team CNSI provides a tiered support structure to respond to requests and ensure that incidents and requests are resolved efficiently. Incidents may be for general support, application processing, and technical inquires submitted by DPHHS and business operations staff. Team CNSI Help Desk availability is during normal business hours as defined by the state and aligned to state holidays as appropriate. Additionally, our NOC team provides 24x7x365 support to perform continuous monitoring and ensure that issues are proactively addressed no matter when they occur. In addition, the Help Desk is available on-call on a 24x7x365 basis to support critical processing and application issues. Help Desk staff are trained to support a wide range of expected issues and inquiries and will route tickets to the appropriate support tier and team if they cannot resolve the issue. Our focus on training and continual improvement will enable our help desk staff to provide answers and responses to typical requests such as general and technical support and questions, password reset procedures, and application and software support.

Help Desk Support for DPHHS and Team CNSI Business Operations

Our Help Desk solution varies based on the stakeholder seeking support. Team CNSI business operations and DPHHS will have a single phone number to directly call the Help Desk for support. Users will also have the ability to email and log tickets via the OTRS web application. Figure 3.10.4-47 shows the support tiers and the corresponding support teams.

Support Level	Support Level Description	Support Teams	Responsibilities	Availability
0	Self-Service	OTRS	■ Web-based ticketing system ■ Instant visibility of tickets to all support tiers	■ 24x7x365
1	Basic	NOC/Help Desk	■ Log tickets and perform triage and ticket routing ■ Monitor system performance and operations processes ■ Support requests, application processing operations, access requests, and technical inquiries ■ Escalate tickets to Tier 2 or Tier 3 based on defined procedures	■ 24x7x365
2	Moderate	Operations Support	■ Manage and support all operational activities ■ Monitor and maintain SLA compliance ■ Track, facilitate, and coordinate tickets and operations processes ■ Oversee operations processes including access requests, Incident Management, Event Management, Release Management, Change Requests, and SLAs ■ Escalate tickets to Tier 3 based on defined procedures	■ On Call (24x7x365)
3	Technical/ Integration	Application Services	■ Triage, prioritize, and support tickets, incidents, and requests ■ Follows the DevOps model and collaborates closely with their business counterparts and CCB teams	■ On Call (24x7x365)
3	Technical/ Integration	Infrastructure/ Data Services	■ Monitor, maintain, and provide incident response for infrastructure and data services	■ On Call (24x7x365)

Figure 3.10.4-47. Help Desk Support Tiers. Team CNSI's Help Desk structure and processes enable responsive and effective support services.

Team CNSI's primary ticketing system, OTRS, is used by the Help Desk to track and manage all tickets. OTRS also provides web interface for users to submit Help Desk requests. Team CNSI's processes ensure 100 percent of tickets are entered in OTRS and are tracked to closure. The following information is typically recorded for each ticket:

- Caller name
- Caller phone number
- Caller email
- User ID (if applicable)
- Application subsystem (if applicable and known)
- Extent of problem (individual user encounter, multiple user encounters at site, entire site)
- Problem/inquiry description
- Additional details related to call (screenshots, last screen/tab/navigation activity before problem Help Desk SLA Monitoring and Reporting

Team CNSI's Help Desk support team follows the incident and request fulfilment processes, outlined in Section 3.10.4 Operations, Maintenance, and Configuration, Service Operations, subsections Request Fulfillment and Incident Management.

Help Desk SLA reports are generated using data from OTRS and HealthBeat SLA Dashboard. Team CNSI's HealthBeat and Cognos reports will provide the main delivery mechanism for SLA reporting and Help Desk monitoring.

OMC16

The Contractor shall provide online help for external and internal users.

Team CNSI has implemented context-sensitive online help that instructs the user how to complete specific tasks within the repository. Online Help is a software program designed to display context sensitive, procedural information to end users of a software application or an operating system. Each screen in the evoBrix solution has an associated online help page that contains information about that screen. The help page displays when the user clicks the Help button on the screen. Once help is opened, the user can browse or search for information on other screens or for steps to complete specific tasks.

Figure 3.10.4-48 and Figure 3.10.4-49 illustrate how Online Help is delivered in an HTML format using WinHelp (.HLP files).



Figure 3.10.4-48. Online Help "Screen Help" Page. Each page provides navigation steps and a reference to related topics.



Figure 3.10.4-49. Online Help "Procedural Help" Page. Each page provides navigation for the procedural steps and links to optional tasks and related topics.

OMC17

The Contractor shall provide 1,500 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 1,500 system enhancement pool hours are included in the offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.

The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

Team CNSI will accommodate the request to provide 1,500 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 1,500 system enhancement pool hours are included in the offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.

Team CNSI agrees that the unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

OMC18

The Contractor shall notify the Department when updated reference materials (e.g., Requirements Matrices, Manuals, System Documentation, System Design Documentation, User Documentation, Business Rules Catalog, and Training Materials) are available for review.

Team CNSI will be utilizing SharePoint site as the Project Documentation Repository, users can set alerts for any material they need to monitor. Team CNSI will notify DPHHS project leadership and designated DPHHS project team members when new or revised deliverables are posted. This includes any component of formal documentation Team CNSI will provide. Team CNSI will utilize the same principle and will notify DPHHS when new or updated training materials are available in SharePoint. Business rules are housed in each Detail Specification Design Document which is also housed in SharePoint website. Please refer to section 3.10.2.1 Project Management for details on the SharePoint Repository.

OMC19

The Contractor shall provide 24x7 access to the Department for all reference materials (e.g., Requirements Matrices, Manuals, System Documentation, System Design Documentation, User Documentation, Business Rules Catalog, and Training Materials).

As mentioned in Requirement OMC18, Team CNSI utilizes the SharePoint Project Documentation Repository to house all project documentation, which will be available 24x7. SharePoint is a secured repository; users only have access to materials they are authorized to see, change, upload, or download. The SharePoint Project Documentation Repository delivers superior project data management, accessibility, and security. Please refer to section 3.10.2.1 Project Management for details on the SharePoint Repository. The Repository is web-enabled and configured expressly for effective project management. It will be available 24x7 to authorized users. It supports the ability to capture and manage key project information including:

- Deliverables and other project documents
- Action items
- Risks
- Issues
- Change requests
- Events
- Contacts
- Development Iteration Planning

Deliverables and other project documents are stored with full history and version control. Users “check out” a document (or other item) while making updates, which ensures that no other user can change the item until it is checked back in. The Project Documentation Repository provides the ability to view previous versions of a document. Authorized users can revert the current document back to a previous version when needed.

Access is defined by user, type, and level. For example, a specific user may be granted read-only access to risks and issues but may have read and update access to change requests. The access types include deliverables and other project documents, action items, risks, issues, change requests, events, and contacts. The access levels within each type are read (R), read and update (RU), create read and update (CRU), and create read update and delete (CRUD).

Specific user access can also be defined for each individual document. For example, a specific user may be able to access the PMP, but may not be granted access to the Data Conversion Plan. Further, a user with access to a document may be granted the ability to only view the document, but not download it, while another user may be granted the access to view and download the document.

The Project Documentation Repository supports the ability to define teams of users, such as DPHHS and IV&V. Document access controls can then be defined at the team level.

OMC21

The Contractor will provide 500 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 500 system enhancement pool hours are included in the Offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours.

Team CNSI will accommodate the request to provide 500 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 500 system enhancement pool hours are included in the Offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

Team CNSI agrees that the unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours.

3.10.5 Key Personnel and Resources

The Offeror must provide key personnel to be assigned to the DDI and Certification phases of the project. At a minimum, key personnel shall include a Project Manager, Contract Manager, Testing Lead, Integration Lead and a Certification Lead. DPHHS will review and approve all key personnel.

The Offeror shall provide key personnel for the Operations, Maintenance and Configuration phase of the Project. At a minimum, key personnel shall include a Project Manager, Technical Manager and a Contract Manager. The Offeror must identify other key personnel for the Operations, Maintenance and Configuration phase of the project. DPHHS will review and approve all key personnel.

For all phases of the Project, the Offeror's Project Manager will be required to perform work at the Primary Project location (Helena, Montana) unless approved by DPHHS to work remotely. Other Offeror

staff working remotely, must be available to work in Helena, Montana at the Department's request for functions necessary to support the scope of work (e.g., risk review meetings, root cause analysis sessions, integration planning, release planning, operational readiness reviews, UAT, implementation, and production deployment). For any work performed at a location other than the Helena, Montana, the Offeror must identify the specific location (city, state, country), describe the type of work to be performed, and the percent of the total hours for that type of work at that location.

The Offeror must propose a staffing approach to meet each of the requirements detailed in Attachment F, Requirements Matrix.

Team CNSI has carefully selected a team of professionals that provide deep industry expertise and knowledge of our proposed solution. We believe it is critical to introduce the Operations, Maintenance, and Configuration ("Operations") staff during the DDI and Certification phase to ensure a smooth transition into operations, and our structure and staffing will demonstrate that philosophy. Key members of the DDI and Certification team will transition into the core Operations team after the system goes live, and will be augmented by additional operations staff to form the full system operations organization. Team CNSI will operate transparently to assure operational readiness during the DDI and Certification phase. This transparency is critical for not only ensuring on-time and smooth operations go-live, but also for preparing the provider community to minimize post-Implementation challenges. We will also augment our Operations team, as needed, during Turnover.

Our MT PSM program effort will be led by Ms. Diana Grogan, an accomplished Project Manager with more than 20 years of technical, business planning, and management expertise that spans systems planning and implementation, large project management, and production systems support for a variety of commercial and government organizations. A certified PMP, Ms. Grogan will ensure MT PSM success by leveraging PMBOK best practices and knowledge of the Medicaid and provider enrollment environments. She has been successful through adept management of proven business processes while leveraging technology to meet the business needs of clients. Ms. Grogan will be supported by a cadre of highly-skilled key personnel who have performed in similar roles on other relevant contracts.

With clearly defined roles and responsibilities and irrespective of company affiliation, our key personnel will work seamlessly under the direction of Ms. Grogan, who will be Team CNSI's primary point of contact for DPHHS for all project-related matters and will oversee the day-to-day activities of the project. Reporting to the Vice President of Delivery for Medicaid Services, Ms. Grogan has the authority, accountability, and visibility needed to ensure successful project delivery. She will coordinate, schedule, and implement activities in a manner that maximizes stakeholder management, collaboration, and communication. She will also serve as a liaison for certification, collaborating with other contractors and stakeholders.

Team CNSI's personnel work as an integrated team that is focused on successfully delivering our PSM solution, while meeting the established quality standards within the timeline and budget. These resources bring extensive experience in multiple implementations of evoBrix modules in multiple states, including multi-tenant, SaaS-based implementations for Michigan and Illinois. They were also instrumental in designing, building, and implementing our evoBrix Cloud-enabled application and the Cloud infrastructure it resides on. This experience has been invaluable, and has led to the development of a large collection of assets for future implementations. Team CNSI feels strongly that assigning knowledgeable resources who possess direct experience implementing our proposed solution and bring a philosophy of collaboration will help reduce implementation risk for DPHHS.

Our key and other resources bring deep experience with systems solutioning, configuration, and implementation. An intrinsic advantage of SaaS implementations is that they are highly repeatable, since infrastructure, application code, and artifacts are already in place and governed by a standardized and

proven process. Team CNSI resources will heavily leverage the existing human, technology, and process assets to successfully deliver our PMIS solution. Technical resources will be paired with business analysts throughout DDI and Certification to ensure that all solution, configuration, and implementation decisions are made in the most operationally efficient manner. Assigning O&M resources throughout DDI also helps mitigate the potential for any post-implementation challenges that result when operational management is brought in too late in a project. Team CNSI's project organization is structured to provide clear lines of reporting as well as appropriately interfacing with DPHHS stakeholders and other Module contractors.

A listing of our proposed key personnel is provided in Figure 3.10.5-1, while detailed information regarding specific experience and expertise of each of these personnel is provided under our response to the requirements of RFP Attachment F, specifically, KR01 to KR30.





©2017 CNSI | 3.10-459

[redacted]

Collectively, Team CNSI's key personnel bring an expert level of program, business, and system knowledge that will be critical as Montana embarks on its PSM initiative, whether it pertains to insight into system scalability and flexibility requirements for addressing growing volumes, the architecture needed for reducing manual intervention and increased automation; reducing complexity of maintenance; or for soliciting stakeholder involvement and input to ensure our solution and services meet the State's program goals. More importantly, these key personnel will leverage their lessons learned on multiple similar engagements to guarantee a successful State-PSM vendor partnership.

KR01

The Contractor can use off-shore and near-shore resources. However, offshore or near shore resources cannot develop security controls. The Contractor shall advise the Department when work is being completed by offshore or near shore resources. The Contractor shall ensure that all Contractor practices and procedures, including but not limited to secure coding practices are used by all resources.

To remain at the forefront of technology innovation, Team CNSI constantly looks to improve its products and services. Continuous improvement also benefits our customers by ensuring that their investment in our solutions provides them with the most modern, updated, and future-proof system for their needs. The primary asset we leverage for effecting this continuous improvement is our Center for Technology and Innovation (CTI), located in India and the Center of Excellence (COE) in our headquarters in Rockville, MD. As we have done on other state MMIS implementations, Team CNSI will leverage either of these resources, depending on the preference of specific customers and their contractual restrictions. In either scenario, the benefits to the customer remain unchanged. For our MT PSM work, CTI resources will be utilized for upgrading and updating our evoBrix PMIS core framework only and will not be involved in developing any security controls. In conformance with the State's requirements, CTI resources will only have access to de-identified data, ensuring that no PHI/PII is sent offshore. We will inform the Department if, when, and what work will be performed by our CTI resources.

Team CNSI's technical processes are standardized across all locations and practices across the organization, therefore, CTI resources also follow the same secure procedures and coding practices that are followed by all our resources in our various US offices.

KR02

The Contractor, and any of its subcontractors, shall work cooperatively with module Contractors and Department staff to ensure the success of the program.

Collaboration has been the hallmark and guiding philosophy of Team CNSI's work on all our projects. We have successfully collaborated with customers, stakeholders, and module/IV&V vendors on our MMIS implementations in Washington, Michigan, Illinois, and Utah, and on our federal contracts with the CMS. We leveraged this philosophy of close collaboration and cooperation with State department staff and other contractors while supporting the state of Michigan's successful Inter-Governmental Agreement (IGA) with Illinois for Cloud PMIS implementation for the latter. Like these other

engagements, we understand that the MT PSM project involves several internal and external stakeholders, such as the SI/ESB and incumbent services contractors who will require timely and accurate program status. We will provide all stakeholders and module contractors controlled access and direct visibility into our project tasks, schedule, deliverables, status, and risks. We will also establish formal, informal, and ad hoc communication methods, while leveraging existing relationships, and establishing new ones, with DPHHS and other contractors to work together as a team in support of the common goal of meeting the Department's MT PSM project vision.

KR03

The Contractor shall help prevent project delays and address them if they occur. This includes assurances that sufficient resources and knowledgeable, experienced staff are available to meet the required project schedule.

Team CNSI's management approach ensures on-time, on-budget, quality delivery of our projects based on a logical and comprehensive method for managing the associated project activities, resources, schedules, and quality. With more than one million person-hours of experience managing projects for state and federal health IT, Team CNSI has its management processes in place for alignment to DPHHS standards.

As detailed in our Management Approach in Section 3.10.2 of our response, Team CNSI's Project Manager will develop a Project Schedule that details the activities, tasks, and milestones required for the implementation of our evoBrix PMIS solution and subsequent operations. Prior to implementation, the PM also establishes milestones and dates for deliverables, cross-team dependencies, and key activities. Details for the activity definition, sequencing, and durations are defined in a highly iterative manner during the proposal stage with functional and technical teams providing input to the management team.

Upon contract award, Team CNSI key personnel will collaborate with their respective counterparts at DPHHS and module contractors to finalize the schedule and integrate milestones, activities, and understand the multi-vendor dependencies. When the Department approves the schedule, our PM will establish the baseline. Ms. Grogan will manage any changes to the baseline through Team CNSI's change management process. Each week, Ms. Grogan will update the schedule and complete a detailed review of progress. This will help her to identify potential risks, and develop mitigation plans from a system perspective.

Risk Management, Quality Assurance/Control, and Change Management are three critical pillars of Team CNSI's overall project management approach to deliver services on-time. Our Project Manager will utilize an Integrated Master Schedule (IMS) to assign work for achieving task completion and resource allocation needed for the various phases and aspects of this project. Our key resources also utilize a Risk Register to identify, asses, and manage risks to acceptable levels through a Review and Update process. Team CNSI's knowledgeable staff has been utilizing these processes to successfully deliver and operate several claims and encounter processing projects similar in size, scope, and complexity to the MT PSM project.

KR04

The Contractor shall provide sufficient personnel to administer and execute required project activities, including approvals, during development, implementation, and operations.

Team CNSI has successfully implemented several projects that are similar to the MT PSM project. This experience has provided us the insight necessary to staff, manage, and execute these projects. As discussed in detail in our Project Management section (3.10.2), we will leverage these management processes, best

practices, and skilled key and project personnel to achieve project success for DPHHS. The management section also details the full labor mix and project organization during the development, implementation, and operations. As we have done on all our similar projects, we will provide and ensure sufficient personnel to administer and execute the activities required (including approvals) during all phases.

Team CNSI maintains a project-specific staff management approach of resources assigned to the project, which includes assigning resources, defining roles and responsibilities, and then providing project-specific training. Our process begins with the determination of staffing needs, knowledge, and skills for each role. Appropriate staff is either recruited or re-assigned from other projects where they have fulfilled their roles. We will then work with DPHHS and Module contractors to identify staff members who will be key contacts for collaboration and integration. Upon completion of this step, Team CNSI will define the roles and responsibilities appropriately and secure management approvals. The final step in our process involves conducting project orientation and project-specific training for assigned project staff members, including any training required by DPHHS.

KR06

The Contractor shall provide key personnel that at a minimum include the Project Manager, the Contract Manager, the Testing Lead, Integration Lead and a Certification Lead during the DDI and Certification Phases of the Program. Key personnel shall not hold more than one key role unless otherwise approved by the Department. The Department will review and approve all key personnel.

Team CNSI is providing all the key personnel required by the PSM RFP for the DDI and Certification phase of this program. A description of their roles is provided in Figure 3.10.5-2, while professional summaries for each are provided below in response to the relevant RFP requirements. Complete details regarding their employment history, education, and other accomplishment are provided in their resumes in Section 4.2.3.

Title	Name	Project Role – DDI and Certification Phase
Project Manager	Diana Grogan	■ Manages the Solution, Configuration, and Implementation (SCI) of the PSM solution ■ Supports the Contract Manager in communicating with DPHHS Leadership, Executive Sponsor Committee, MPATH Stakeholder Committee, module vendors, and other stakeholders ■ Responsible for the resolution of issues impacting the timeliness of deliverables ■ Facilitates the interaction of all parties to reduce risk and maximize benefits of deliverables ■ Leads the governance and involvement of the Project Management Office (PMO) during all phases of the SCI
Contract Manager	Fred Fiola	■ Team CNSI's senior representative for the contract ■ Serves as the primary point of contact for the DPHHS Steering Committee, Executive Sponsor Committee, MPATH Stakeholder Committee, and other State stakeholders ■ Responsible for Team CNSI's business relationship ■ Accountable for Team CNSI's activities related to contract deliverables, project management, and subcontractors
Testing Lead	Phil Carino	■ Coordinates and plans testing activities for the PSM project ■ Ensures detailed, process driven, and fully documented testing procedures for all implementations and configuration changes within the Montana Healthcare Programs enterprise ■ Responsible for planning, managing and executing comprehensive testing, to include unit, system, regression, parallel, integration and UAT ■ Ensures the test environment is configured per the requirements of development and test teams ■ Coordinates with DPHHS regarding test data collection and development ■ Monitors and reports on discrepancies

Title	Name	Project Role – DDI and Certification Phase
Integration Lead	Kanwal Sandhu	■ Coordinates with business improvement teams to support and guide them through system-related changes ■ Creates routines to convert data from multiple sources to the PSM solution ■ Creates routines to convert data from the legacy system to operate the PSM ■ Executes the crosswalk of data to all components of the PSM ■ Evaluates performance metrics against service factors; institutes actions to correct shortcomings or further streamline the process, as necessary ■ Identifies opportunities for business improvement with respect to tools, staff, training, process, procedures and work instructions
Certification Lead	Michele Chamberlin	■ Assists the State staff with pre-certification activities ■ Oversees the certification or credentialing programs of the account ■ Oversees the development of standards and testing materials for compliance with the CMS Certification checklist

Figure 3.10.5-2. Key Personnel. Team CNSI's Proposed Key Personnel for the PSM DDI and Certification Phase.

Team CNSI has assigned qualified resources to staff each of the key roles for this project. As a standard practice, we do not assign our key personnel to more than one key role. If such course of action makes the best sense on this project, we will work with the Department to obtain their approval. We also understand that DPHHS will review and approve all key personnel prior to their assignment to this project.

KR07

Key personnel described in the proposal shall become named resources on the project and are subject to the following requirements:

a. Key personnel shall not be transferred or removed without prior approval of the Department.

b. The Department will approve key personnel assigned to the Contract.

c. The Department reserves the right to request removal of any Contractor staff or subcontractor staff, if applicable, assigned to the project, and the Contractor shall comply with any such request immediately.

d. If a vacancy occurs in a key role, the Contractor shall fill the position in compliance with identified SLAs.

As we do on all our projects, Team CNSI is proposing key personnel that will become named resources on this project. The requirements for key personnel set forth in this RFP are typical of the health IT and other government contracts we have performed on, and we routinely comply with such requirements. For meeting these requirements on the MT PSM project, Team CNSI accepts that our key resources will be subject to the following requirements:

- Key personnel shall not be transferred or removed without prior approval of the Department
- The Department will approve key personnel assigned to the Contract
- The Department reserves the right to request removal of any Team CNSI staff, if applicable, assigned to the project, and Team CNSI will comply with any such request immediately
- If a vacancy occurs in a key role, Team CNSI will fill the same in compliance with identified SLAs

KR08

The Contractor must designate a Project Manager to represent and oversee the day-to-day activities of the project. This individual shall serve as the Department's primary point of contact for matters relating to the project and serve as a liaison for certification, collaborating with other contractors, and stakeholders.

Our PSM program effort will be led by Ms. Diana Grogan, an accomplished Project Manager with more than 20 years of technical, business planning, and management expertise that spans systems planning and implementation, large project management, and production systems support for a variety of commercial and government organizations. A certified PMP, Ms. Grogan will ensure PSM success by leveraging PMBOK best practices and knowledge of the Medicaid and provider enrollment environments.

Ms. Grogan has the authority, accountability, and visibility needed to ensure successful project delivery. She will coordinate, schedule, and implement activities in a manner that maximizes stakeholder management, collaboration, and communication. She will also serve as a liaison for certification, collaborating with other contractors and stakeholders.

KR09

The Contractor's Project Manager must meet the following qualifications including:

a. A minimum of seven (7) years' project management experience managing projects of similar size and scope, preferably in Medicaid or the healthcare industry. This experience must include relevant experience within the last three (3) years from the release date of the RFP.

b. Project Management experience should include each phase of the system development life cycle.

c. Project management certification through the Project Management Institute (PMI) is preferred.

[redacted]

©2017 CNSI | 3.10-464

[redacted]

KR10

The Contractor must designate an Integration Lead to manage the design, configuration/build, integration, defect management, and implementation of the Contractor's scope of work.

Team CNSI is proposing Mr. Kanwal (Ken) Sandhu as our Integration Lead for this project. Mr. Sandhu is a diligent technical manager with a proven success record leading all phases of diverse technology projects. He possesses over 18 years of experience in computer programming and infrastructure enterprise projects. Mr. Sandhu is an expert in Agile and Waterfall project management methodologies, and is known for his ability to produce high-quality deliverables that meet timelines and budgetary targets.

KR11

The Contractor's Integration Lead must meet the following qualifications including:

a. Minimum of five (5) years leading system design and integration projects, including the technical design and implementation of projects similar in size and scope to this project.

b. Experience must involve directing multi-discipline technical teams producing integration solutions (e.g., Service Oriented Architecture, network, hardware and software).

c. A Bachelor's Degree in Information Systems Engineering, Computer Science, or a related field is preferred.

[redacted]

[redacted]

KR12

The Contractor must designate a Testing Lead to coordinate all testing activities.

Mr. Phil Carino is Team CNSI's proposed Testing Lead for the PSM engagement. He has a demonstrated 21-year track record of success driving Quality Assurance and best-in-class quality performance by leveraging experience in quality management, technical leadership, business analysis, development, and test engineering.

He has proficiency in all phases of the software development life cycle complemented by robust client engagement and problem-solving skills. Mr. Carino is also a facilitative team leader and motivational mentor with excellent communication skills that have enhanced stakeholder relations and cultivated collaborative working cultures that embrace interdepartmental cohesion, transparency, and efficiencies.

KR13

The Contractor's Testing Lead must meet the following qualifications including:

a. Minimum of three (3) years' experience leading testing activities for a project similar in size and scope to this project.

b. In-depth understanding of the testing lifecycle and all artifacts required to successfully validate the system.

[redacted]

©2017 CNSI | 3.10-466

KR14

The Contractor must designate a Contract Manager to be the single point of contact for matters concerning the Contractor's performance under the Contract. This person shall have the authority to make decisions that are binding to the Contract, shall be responsible for timely completion of the project, and shall be responsible for meeting all contractual obligations.

Team CNSI's Contract Manager for the MT PSM program effort is Mr. Fred Fiola, who brings more than 25 years of service delivery experience on State Medicaid programs. As the Fiscal Agent Contract Manager for the state of Missouri Medicaid Program, he served as the first point of contact for the Department of Social Services and the Medicaid Department, Missouri HealthNet. On this engagement as well, Mr. Fiola will be Team CNSI's single point of contact for contract performance for DPHHS and other stakeholders, and will have the authority to make binding decisions on our contractual obligations.

KR15

The Contractor's Contract Manager must have a minimum of five (5) years' contract management experience managing related services with similar budgets, preferably in Medicaid or the healthcare industry and for a project similar in size and scope to this project.

[redacted]

KR16

The Contractor shall submit two (2) references for each of the key personnel being proposed for the project. Each reference should depict relevant and current experience for work completed no more than seven (7) years prior to the date of this RFP.

References for each key personnel are provided in Figure 3.10.5-3.

[redacted]

KR17

The Contractor must demonstrate that it can commit an adequate level of technical and human resources sufficient to complete the project within the required time frame and to meet the quality requirements outlined in this RFP. Furthermore, the level of technical and human resources which the Contractor agrees to commit to the project at the time of proposal must be maintained throughout the life of the project at a necessary level to complete the scope of work.

Team CNSI is led by prime contractor CNSI, who possesses a track record of delivering and operating Medicaid systems in multiple states for over 20 years. CNSI is a recognized leader in providing SaaS technology to the Medicaid market, with a multi-state SaaS Provider Management solution currently in operations. CNSI has been involved in the healthcare and health IT industry since 1998, expanding our role from mere support of a legacy system to developing the first-of-its-kind MMIS platform. Over 80% of CNSI's revenues are derived from health IT and today, we participate in a majority of the health IT initiatives underway across the nation. These include the Affordable Care Act (ACA), HITECH, payment

reform, Meaningful Use, transition to managed care, consumer engagement, and integrated care for the dually eligible.

For this important initiative, CNSI has teamed with Noridian Healthcare Solutions, LLC (Noridian), a well-known vendor in the Medicaid and Medicare market with a record of service excellence, currently holding the record for national provider satisfaction in Medicare administrative services, and a longtime partner with CNSI. As a trusted partner to CMS for decades, Noridian brings 50 years of experience in claims processing, mailroom services, contact center start-up and operations, training, and provider enrollment and management. Noridian has also been serving the Montana provider community for over 11 years, and supports providers in several of the NASPO participating states, including North Dakota, South Dakota, Wyoming, and Oregon.

Team CNSI represents a strong blend of Medicaid industry expertise and innovative technology, delivered seamlessly through a single organization. Our decades of experience in delivering healthcare solutions and services, guided by our lean methodologies and processes, provide us with a clear vision and roadmap to deliver the PMIS solution to Montana and its constituents. The people we are proposing for Montana bring more than two decades of Medicaid implementation experience collectively. These resources bring both technical and functional expertise, as well as a wealth of knowledge implementing MMIS solutions in the states of Michigan, Washington, Illinois, and Utah. This experience has provided them with insight into the key requirements, as well as lessons learned, for a successful PSM implementation in Montana. Team CNSI agrees to maintain the proposed level of technical and human resources throughout the life of the project at a necessary level to complete the scope of work.

KR18

The Contractor's staff shall have sufficient experience appropriate for their role.

The staff being proposed by Team CNSI have been performing in the same or similar capacity on their most recent project experience. They have been a part of CNSI's decade of operational experience managing nearly 750,000 active provider enrollments and processing over 500 million claims and encounters among the states of Michigan, Washington, Illinois, and Utah. Our SaaS service model has become CNSI's primary focus for delivering MMIS services to its customers. Moreover, the cloud-based evoBrix solution being offered to DPHHS was the first in the nation to become fully ACA-compliant and has been supporting over 400,000 active provider enrollments in a multi-tenant SaaS platform for the states of Michigan and Illinois since July 2015. Our proposed staff has had the opportunity to work in, and learn from, these pioneering technological efforts, and will bring that unique insight and domain expertise to their PSM work.

KR19

The Contractor must supply a Personnel Background Check Attestation (written documentation) of a favorable background check for Contractor personnel who might reasonably be expected to access sensitive and confidential member data contained in any system accessed during the course of the Contract. The Department may request the removal of staff for disqualifying offenses. Contractor must describe their process for performing background checks for non-US citizens or Green Card holders.

Following a structured interviewing and rating process, Team CNSI conducts background checks for all potential employees, including non-US citizens and Green Card holders, according to the security level requirements of the position. Team CNSI's Human Resources (HR) Department has written policies and

©2017 CNSI

procedures for conducting a background investigation, a search of the General Services Administration's (GSA's) Excluded Provider List System (EPLS), Office of Inspector General's list of excluded individuals and entities, the U.S. Treasury Office of Foreign Assets Control (OFAC), and reference checks for prospective employees.

We realize that the best candidates are not available for long, so our managers are trained to complete a thorough candidate review process within a short time frame. Offers are extended to the top candidates as soon as possible; however, these offers are always contingent upon successful completion of a satisfactory background check. For any personnel who might be expected to access sensitive and confidential member data contained in any system accessed during our PMIS contract, Team CNSI will supply a Personnel Background Check Attestation, in written form, of a favorable background check. We also understand and accept that the DPHHS may request the removal of staff for disqualifying offenses.

KR20

The Contractor's Project Manager shall be required to perform work at the State's primary project location (e.g., city, state), unless approved by the Department to work remotely.

For all phases of the Project, Ms. Grogan will perform work on-site at the State's primary project location (in this case, Helena, MT), unless approved to work off-site by DPHHS.

KR21

The Contractor's staff shall be available Monday through Friday as early as 7:00 AM MST and as late as 6:00 PM in the time zone of the participating State.

Team CNSI understands this requirement and will ensure that our staff will be available Monday through Friday as early as 7:00 AM MST and as late as 6:00 PM in the time zone of the participating State.

KR22

For any work performed at a location other than the primary Project site, the Contractor must identify the specific location (city, state, country), describe the type of work to be performed, and the percent of the total hours for that type of work at that location.

In addition to the primary Project site, Team CNSI's MT PSM project effort will be performed at the following locations:

- Base work locations include Helena, MT; Lansing, MI; Rockville, MD; and Chennai, India (when needed, and in conformance with the requirements described in response to KR01). The work performed and the percent of total hours for that type of work at that location are detailed in Figure 3.10.5-4.
- Option A work locations include Helena, MT; Lansing, MI; Rockville, MD; and Chennai, India. The work performed and the percent of total hours for that type of work at that location are detailed in Figure 3.10.5-5.
- Option B work locations include Helena, MT; Fargo, ND; Lansing, MI; and Rockville, MD. The work performed and the percent of total hours for that type of work at that location are detailed in Figure 3.10.5-6.

Base Location	Type of Work to be Performed	% Total Hours
Lansing, MI	■ Solution architecting ■ Business architecting ■ Development ■ Data conversion ■ Interface development ■ Technical writing ■ Quality assurance ■ Project Scheduling and Monitoring ■ Data modeling ■ Reports development ■ Letters/Correspondence development	■ 2% ■ 2% ■ 15% ■ 10% ■ 10% ■ 2% ■ 4% ■ 1% ■ 1% ■ 5% ■ 5% Total = 57%
Rockville, MD	■ Database management ■ Configuration management ■ Testing ■ Development ■ Project controls ■ Release management	■ 2% ■ 5% ■ 10% ■ 5% ■ 1% ■ 2% Total = 25%
Chennai, India	■ Development of framework and common components	Total = 8%

Figure 3.10.5-4. Base Work Locations. Details regarding the type of work to be performed and the percentage of total hours allotted to that type of work for each Base Work location.

Option A Location	Type of Work to be Performed	% Total Hours
Lansing, MI	■ Solution architecting ■ Business architecting ■ Development ■ Interface development ■ Technical writing ■ Quality assurance ■ Project scheduling ■ Data modeling ■ Reports development ■ Letters/Correspondence development	■ 5% ■ 2% ■ 12% ■ 10% ■ 2% ■ 2% ■ 3% ■ 4% ■ 5% ■ 5% Total = 50%
Rockville, MD	■ Database management ■ Configuration management ■ Testing, ■ Development, ■ Project controls ■ Release management	■ 2% ■ 5% ■ 12% ■ 7% ■ 2% ■ 2% Total = 30%
Chennai, India	■ Development of framework and common components	Total = 12%

Figure 3.10.5-5. Option A Work Locations. Details regarding the type of work to be performed and the percentage of total hours allotted to that type of work for each Option A location.

Option B Location	Type of Work to be Performed	% Total Hours
Lansing, MI	■ Solution architecting ■ Business architecting ■ Development ■ Interface development ■ Technical writing ■ Quality assurance ■ Project scheduling	■ 2% ■ 5% ■ 10% ■ 8% ■ 2% ■ 2% ■ 1% Total = 30%
Rockville, MD	■ Database management ■ Configuration management ■ Testing ■ Development ■ Project controls ■ Release management	■ 2% ■ 2% ■ 5% ■ 2% ■ 1% ■ 1% Total = 25%
Fargo, ND	■ Business operations ■ Call Center support	■ 21% ■ 20% Total = 41%

Figure 3.10.5-6. Option B Work Locations. Details regarding the type of work to be performed and the percentage of total hours allotted to that type of work for each Option B Work location.

KR23

The Contractor's staff working remotely, must be available to work in the State's primary project location at the Department's' request for functions necessary to support the scope of work (e.g., risk review meetings, root cause analysis sessions, integration planning, release planning, operational readiness reviews, UAT, implementation, and production deployment).

Team CNSI will also ensure that staff working remotely will be available to work in Helena, Montana at the Department's request for functions necessary to support the scope of work.

KR24

In the event that key personnel resign or are terminated, the Contractor shall provide the Department with immediate notice of the vacancy and an action plan for backfilling the position until a replacement is found and approved by the Department. A key personnel position must not be vacant for more than fourteen (14) consecutive days. The Contractor may not fill vacant key personnel positions with other existing key personnel without approval by the Department. The Department will also have the authority to approve proposed replacements of key personnel by the Contractor.

We understand the critical nature that key personnel play on projects, and the negative impact their resignation or termination can have. As we do on all our projects, Team CNSI will leverage its proven recruiting process, described in the introduction to this section, to ensure:

- The Department is immediately notified of the vacancy
- An action plan for backfilling the position is provided and approved by the Department
- A suitable replacement is found prior to 14 consecutive days of the vacancy

Team CNSI will not fill vacant key personnel positions with other existing key personnel without obtaining prior approval from the Department. We also accept that DPHHS will have the authority to approve proposed replacements of our key personnel.

KR25

The Contractor's key personnel and/or management replacement must meet the minimum qualifications for the position. The Contractor shall provide a detailed resume for a proposed key personnel and/or management replacement. Replacements are subject to Department approval prior to any assignment.

Team CNSI assures DPHHS that replacements for any key personnel will meet the minimum qualifications for the position they are being proposed for. We will furnish DPHHS with a detailed resume of the proposed replacement and obtain Department approval prior to assigning them to any work.

KR26

The Contractor shall provide the appropriate level of knowledge transfer/training to Contractor staff.

Team CNSI takes a multi-faceted approach to ensure that staff can perform their roles effectively and efficiently on the project. We believe, that well-trained employees have higher satisfaction with their jobs, are more productive, and provide better results, all of which improve project outcomes and customer satisfaction. We also understand that complex projects require that staff understand their roles and can perform them individually and as a member of the team.

Team CNSI staffs its project teams with professionals that have specific domain knowledge to perform their roles as well as experience in Medicaid. As a result, the focus of training is primarily concerned with orientating staff how evoBrix satisfies CMS Medicaid requirements. To ensure that each project team is fully functional, Team CNSI performs an assessment of staff competency levels and potential training needs. Because each project team brings a mix of both seasoned professionals with long term experience on Team CNSI projects and may also include new professionals or mature professionals who are new to the organization, the training needs of each project form a unique profile which is evaluated and remediated as required. Individual training plans are incorporated and monitored through our Staff Management Plan, a sub-plan of the Project Management Plan. Team CNSI prepares staff for the role they play on the project by providing overview training of standard policies and procedures, training on tools and methodologies that project will employ, and through mentoring partnerships between experienced staff and those who are new. Team CNSI project leadership ensures that companywide training requirements, such as Health Insurance Portability and Accountability Act (HIPAA), are met by staff as well as any necessary project-specific training.

For project-specific training, Team CNSI begins with a "Project Bootcamp" experience for all the staff assigned to the initiative. Bootcamp is a training and communication activity that serves to level set the knowledge base of the team assigned to deliver the project. Each boot camp experience has some unique features that are tailored to the requirements of the project. During boot camp, team members review policies, procedures and deliverables that will be required for the project. Experienced staff assist to accelerate growth of newer staff and start operating as a seamless unit.

At the corporate level, Team CNSI offers CNSI University to newer hires which provides several foundational trainings to level set staff with the basic information needed to operate within the company.

Training programs that may be required for project team members based upon need include:

- **iVision 360 Program** – The iVision360 SDLC methodology described within this training serves to meet the needs of delivering complex Medicaid Management Information Systems (MMIS) and is able to be tailored to meet each project's needs accordingly.
- **MMIS/Medicaid Program** - As CNSI employees, an understanding of basic Medicaid concepts can give us a running start as we develop tools for this key customer group. This knowledge acts as a foundation, giving the big picture of what Medicaid is and how it functions.
- **evoBrix Solution Overview** – Team members assigned to implement Team CNSI's evoBrix platform are provided an overview of the solution and key features and functions. Focus is on how evoBrix can be configured to satisfy Medicaid requirements.

KR28

The Contractor must designate a Certification Lead to coordinate all certification activities.

Team CNSI is proposing Ms. Michele LaMar-Chamberlin to perform the role of Certification Lead on our PSM project work. She brings more than 15 years of experience in the Medicare and Medicaid environments to the Department, with an additional five years of experience in commercial health insurance. Ms. LaMar-Chamberlin has been involved in the certification efforts of CNSI's Washington MMIS ProviderOne™ system, where she was responsible for identifying the system features that supported the MECT checklists for the provider subsystem. She also participated in the certification effort for CNSI's MMIS implementation in the state of Michigan, reviewing the adequacy of the State's responses and evidence presented for multiple checklist activities.

Additionally, Ms. LaMar-Chamberlin is a CMMI Development L1.3 Associate, and a registered CMMI appraisal team member. In her current role as a Senior Manager in the PMO, she is also the State of Michigan's primary point of contact for overall quality concerns.

KR29

The Contractor's Certification Lead must meet the following qualifications including:

a. Minimum of three (3) years' experience certifying systems against industry standards for projects similar in size and scope to this project.

b. In-depth understanding of the most current MECT certification lifecycle required to successfully validate the system.

[redacted]

[redacted]

KR30

The Contractor shall provide key personnel that at a minimum includes a Project Manager, Contract Manager and a Technical Manager for the Operations, Maintenance and Configuration phase of the project. Key personnel shall not hold more than one key role unless otherwise approved by the Department. The Contractor must identify other key personnel for the Operations, Maintenance and Configuration phase of the project. The Department will review and approve all key personnel.

Team CNSI is providing all the key personnel required by the PSM RFP for the Operations, Maintenance, and Configuration phase of this program. Highlights of their skills and experience is provided in Figure 3.10.5-7, while complete details regarding their employment history, education, and other accomplishment are provided in their resumes in Section 4.2.3.

Title	Name	Project Role – Operations, Maintenance, and Configuration Phase
Project Manager	Diana Grogan	■ Manages the Solution, Configuration, and Implementation (SCI) of the PSM solution ■ Supports the Contract Manager in communicating with DPHHS Leadership, Executive Sponsor Committee, MPATH Stakeholder Committee, module vendors, and other stakeholders ■ Responsible for the resolution of issues impacting the timeliness of deliverables ■ Facilitates the interaction of all parties to reduce risk and maximize benefits of deliverables ■ Leads the governance and involvement of the Project Management Office (PMO) during all phases of the SCI
Contract Manager	Fred Fiola	■ Team CNSI's senior representative for the contract ■ Serves as the primary point of contact for the DPHHS Steering Committee, Executive Sponsor Committee, MPATH Stakeholder Committee, and other State stakeholders ■ Responsible for Team CNSI's business relationship ■ Accountable for Team CNSI's activities related to contract deliverables, project management, and subcontractors
Technical Manager	Jim Schloss	■ Manages of operations activities, ensuring functional and technical support for delivery of all services ■ Schedules and provisions resources to positions within the business and technical units ■ Meets all SLAs and performance standards ■ Communicates issues/problems that impact the State's ability to meet defined business goals ■ Manages the Systems Operations team to perform functional integration reviews and checkpoints ■ Provides business process and functional expertise to all team members ■ Collaborates with DPHHS and Team CNSI to communicate analysis of change requests for impact and cost
Business Operations Manager	Martha Kittrell	■ Leads the Operations support under Option B Provider Services ■ Responsible for conducting provider evaluation and maintaining site visits ■ Provides oversight and management of the provider call center for new and revalidation applications

Title	Name	Project Role – Operations, Maintenance, and Configuration Phase
		and enrollments ■ Oversees staffing to review provider information, maintenance requests, and all supporting materials to verify provider changes prior to updating the provider records ● Reviews and approves/denies low risk, high volume enrollments per Agency criteria ■ Ensures the provision of services to support the collection of financial packet and information from providers and entering the information into State financial systems
Application Services Manager **(Additionally Proposed Key Resource)**	Rejoice Chemmannur	■ Manages the implementation of software applications to enable and/or support the delivery of client services ■ Responsible for proactive evaluation of software and systems upgrades to enhance the delivery of services ■ Manages network and hardware installations to ensure timely delivery of services without interruption
Infrastructure Manager **(Additionally Proposed Key Resource**)	Girish Salpekar	■ Manages the FedRAMP cloud infrastructure ■ Oversees Team CNSI's DBA, CM, and System Administration teams ■ Leads initial setup and maintenance of the cloud infrastructure ■ Leads requested changes, updates, and modifications to cloud infrastructure

Figure 3.10.5-7. Team CNSI's Proposed Key Personnel for the PSM Operations, Maintenance, and Configuration Phase.

Team CNSI's Project Manager and Contract Manager, Ms. Grogan and Mr. Fiola, respectively, will continue to perform in their capacities during the Operations, Maintenance, and Configuration phase. For the DPHHS, this will equate to continuity in work practices, domain knowledge, relationships, and the appropriate amount of authority and priority, as our teams transition from DDI and Certification to system operations. We are also proposing Mr. Jim Schloss as our Technical Manager, for the Operations, Maintenance, and Configuration phase, to oversee all Team CNSI project activities for our system and technical operations. Our Operations, Maintenance, and Configuration organization also includes a Business Operations Manager to oversee the services required under Option B.

Team CNSI's operations model also requires a single point of accountability and communication for DPHHS in the areas of Technical Operations, Applications Services, and Cloud Infrastructure Support. For achieving this, we are proposing additional personnel, in addition to the required key resources, as under:

- ***Application Services Manager***: Overall responsibility for operational support, monitoring, and maintenance of all applications
- ***Infrastructure Manager:*** Overall responsibility for cloud infrastructure support, monitoring, and maintenance

As previously mentioned in response to KR06, Team CNSI has assigned qualified resources to staff each of the key roles for this project. As a standard practice, we do not assign our key personnel to more than one key role. Should such a course of action makes the best sense on this project, we will work with the Department to obtain their approval. We also understand that DPHHS will review and approve all key personnel prior to their assignment to this project.

3.10.5.1 Resource Allocation Schedules

Offerors must complete the Resource Allocation Schedules provided in Attachment H, Resource Allocation Schedules. These schedules serve as the representation of Offeror's plan for staffing the project by resource type. Offeror should include additional information as necessary to explain the Offeror's resource allocation. If the Offeror has one or more subcontractors, the Offeror must submit a

Schedule A and Schedule B with a comprehensive total for all FTE and hours representing the effort of the prime contractor and all subcontractor work in total. In addition, a separate Schedule A and Schedule B for each contractor (prime contractor and subcontractor) must be submitted.

Table 3.10.5.1 Resource Allocation Schedules (These schedules are provided in Attachment H, Resource Allocation Schedules).

List of Resource Allocation Schedules	
Schedule	*Title*
Schedule A	*Number of Full Time Equivalent*
Schedule B	*Number of Hours*

All schedules must be completed in full at the time of submittal. The resource types listed in the schedule are not exhaustive, nor should the Contractor assume that DPHHS is requesting resources from each category. Use any resource type listed above and/or add resource types necessary to successfully deliver the scope of work.

Schedule A: This schedule details the number of full time equivalents the Offeror plans to allocate to the project by phase and by resource type.

Schedule B: This schedule details the number of resource hours the Offeror plans to allocate to the project by phase and by resource type.

Team CNSI's Attachment H includes additional worksheets to depict the total hours and resources needed to implement Option A and Option B, along with running System Operations for MT PSM, Option A and Option B respectively.

Per the RFP Requirements and associated Question and Answer documents, Team CNSI is submitting a total of six resource allocation schedules. The six schedules are shown in Figure 3.10.5-8.

List of Resource Allocation Schedules	
Schedule	**Worksheet Title**
Schedule A - Total FTEs PMIS Base + Option A + Option B (Team CNSI Total)	Sch A Total FTEs by Phase
Schedule B - Total Hours PMIS Base + Option A + Option B (Team CNSI Total)	Sch B Total Hrs by Phase
Schedule A - Total FTEs PMIS Base + Option A + Option B (Prime (CNSI) only)	Sch A Prime FTEs by Phase
Schedule B - Total Hours PMIS Base + Option A + Option B (Prime (CNSI) only)	Sch B Prime Total Hrs by Phase
Schedule A - Total FTEs PMIS Base + Option A + Option B (Team member Noridian Only)	Sch A Sub FTEs by Phase
Schedule B - Total Hours PMIS Base + Option A + Option B (Team member Noridian Only)	Sch B Sub Total Hrs by Phase

Figure 3.10.5-8. Team CNSI Resource Allocation Schedules. Team CNSI has provided prime contractor (CNSI) and Team CNSI member Noridian's resource allocations separately and in aggregate for the base PMIS and Options A and B.

Team CNSI follows a methodical process to develop resource estimates. Our approach is to begin with our high-level work breakdown structure (WBS) used for our previous PMIS implementations in Washington, Michigan, Illinois, and Utah. Team CNSI then used its project schedule and cost information from our previous PMIS implementations, as input, to determine the necessary resource levels as presented in the Schedules in Appendix H.

We considered the State's RFP requirements and performed an initial mapping to our evoBrix PMIS solution. This exercise provided Team CNSI the information necessary to determine the fit with the State's requirements and areas where solution analysis, configuration, and state-specific implementation is needed.

Our process included the following factors:

- Top-down analysis: Team CNSI begins our estimating process by looking at the entire scope of the project defined in the RFP and iteratively refining our examination to include a progressively more detailed context. This "drill down" approach allows us to consider only the material that is relevant to the particular context in which we are working. At the highest level, the context includes only the major software components and the interfaces between them. Anything that occurs entirely within a particular part of the system is encapsulated within a single component representing that part of the system. At each succeeding level, we define the details of what happens within each component, as well as what information is contained in the interfaces.
- Bottom-up analysis: Team CNSI also completes a bottom-up analysis based on the business areas and RFP requirements. We deconstruct and organize the business requirements of the RFP and assign the requirements to the estimating team for each business area. During the bottom-up analysis, we ask standard questions of each team lead developing the solution for each business area. These questions are designed to uncover major scope areas and establish activity duration estimates based on our comparison to previous systems we have built. The questions of the estimating survey include:

    - How many requirements are provided for each area?
    - What degree of effort is needed to configure the solution?
    - How many system components exist and will need minor modifications?
    - How many screen components, reports, correspondences, and interfaces are new and required specifically for the MT PSM? Here we estimate the level of complexity for each screen (high, medium, low).
    - To what extent will we need to change to the evoBrix data model? On a scale of 1 to 10, with 10 being the most complex, what is the level of complexity of the change?
    - Are there any unique challenges with respect to data conversion?
    - What types of training materials are required?
    - How many training sessions are necessary to support the deployment and operations of the MT PSM implemented for the State?
    - What are the assumptions pertaining to the business area?
    - What are the risks pertaining to each business area?

- Knowledge from previous projects: Team CNSI has specific experience in conducting similar tasks for multiple provider implementation projects. This experience allows us to develop detailed resource estimates based on actual results. For example, we have data on the resources required to conduct solution analysis, configuration, testing, UAT, deployment, and CMS Certification. Our estimating approach includes reviewing this data and comparing past experience with expected effort for the MT PSM.

We made the following planning assumptions for the phase by phase review of resources required to support the project:

- Project management is a critical discipline. Our resource allocations show that Team CNSI management resources and key personnel are allocated evenly throughout the life of the project.
- The early stages of the project are heavy on analytical resources and the later stages of the project emphasize testing, training, and implementation resources.

©2017 CNSI

- Certification requires up-front commitment to develop the certification plan. However, most of the certification activity will occur post-go-live to support data collection and CMS certification meetings.
- The resources are allocated based on the phase of the project. Developers are assigned once the requirement and design phases are complete, while testers are assigned once the development has reached a milestone wherein meaningful, testable code can be deployed into the system test environment for testing.
- The system operations support resources and Key resources for the system operations phase are allocated to the project once production operation of the MT PSM begins. Our Resource Allocation worksheets show the resources necessary for supporting system operations.

Team CNSI is providing a bid that encompasses the base PMIS as well as Options A and B. Therefore, we have provided specific information regarding the additional business operations staff required to support these two options. Team CNSI member Noridian, will operate the solution for B.

As shown in Figure 3.10.5-9, the implementation of MT PSM will occur in seven months. The Initiation and Requirements Phase is for a duration of one month; Design, Build and Configuration is for a duration of four months. Out of the four months, the first month is dedicated for design while the last three months are for build and configuration.

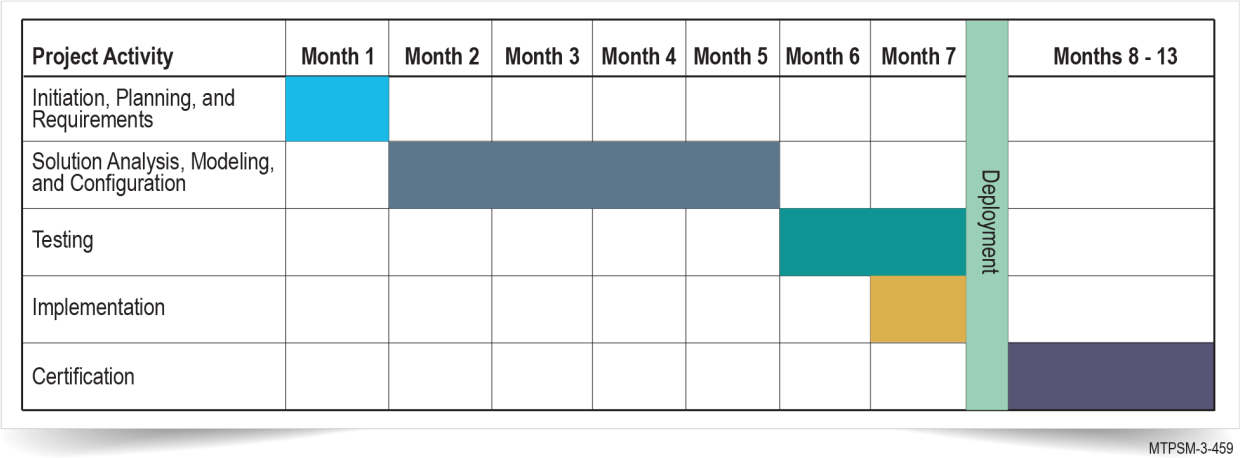


Figure 3.10.5-9. High-Level MT PSM Timeline. Team CNSI proposes a seven-month project duration leading to the initial implementation of the MT PSM. Certification cannot occur any earlier than six-months post-deployment.

There will be an overlap between the testing phase and deployment/implementation/certification phase. Testing will occur for a duration of two months while implementation planning and cutover activities will begin on the last month of implementation. The resources needed for each phase are identified in the Attachment H spreadsheets.

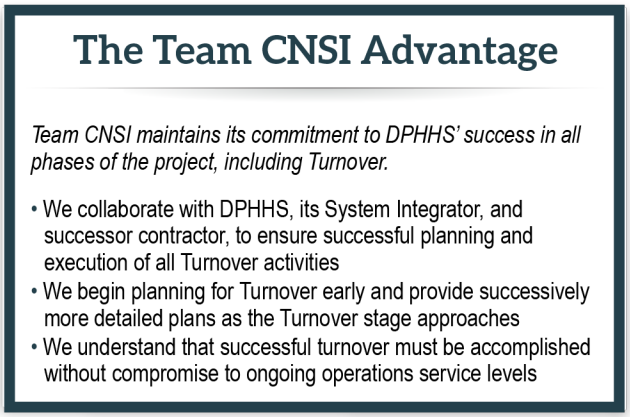
3.10.6 Project Closeout and Turnover

At least twelve months prior to the end of the contract, the Contractor will provide an initial turnover plan to detail how the Contractor will manage the completion and closure of all work for the Contract and deliver project artifacts, including deliverables, data, and anything needed to operate and maintain the integrity of the Montana Healthcare Programs and systems.

Transition activities will be dependent upon the nature of the solution or services, which may include but is not limited to:

- *State Owned and hosted*
- *State Owned and Contractor hosted*
- *State Leased software and State-hosted*
- *State Leased software hosted by a third party*
- *Software as a Services (SaaS)*

The Contractor must demonstrate that all contractual requirements have been met, transition operational tasks to a new Contractor and/or DPHHS completed, and provide lessons learned from the project prior to the end of the contract term. The Offeror must describe their approach to meet each of the Project Closeout and Turnover requirements defined in Attachment F, Requirements Matrix.



Team CNSI values its long-term relationships with our customers. Those relationships are built on quality performance and have persisted even when we no longer have a direct business responsibility to them. Because every customer and every project is important to us, we strive to build and sustain a reputation as a contractor that is fully supportive of our customers, regardless of the contract phase we are performing. DPHHS is relying on Team CNSI to continue to fully support its programs and stakeholders by meeting all operations performance requirements, while collaborating with the succeeding contractor to ensure their full understanding of the evoBrix PMIS operations. Our goal is to perform a seamless turnover with no negative impact on continuing operations and services.

We will perform turnover activities with the same careful attention, planning, and execution that the State will have come to expect based on our performance throughout the MT PSM operations. We fully support that the DPHHS may require Team CNSI to turn over complete and up-to-date systems, documentation, fiscal intermediary responsibilities, and materials; to provide training in use, functionality, and processes for the successor; to correct any deficiencies known prior to or discovered during the turnover process; and ensure that the turnover is completed in a timely manner and with no adverse impact on the user community and other key stakeholders. DPHHS will find that Team CNSI is fully cooperative, responsive, and compliant at all levels with the State's requests as expressed in the RFP to ensure that the State's goals are achieved.

The key ingredient to a successful turnover is people. Ensuring the right person, with the right training, is in place is the focus of the Turnover activities. During the planning phase of the MT PSM project, Team CNSI will work with DPHHS to define schedule for turnover planning and execution. We understand that the turnover must address, as applicable, State owned and hosted solutions, State owned and vendor-hosted solutions, State leased and hosted solutions, State leased and third-party hosted solutions, and software as a service (SaaS) solutions. Our approach, for the evoBrix Provider Management Information System (PMIS) as configured for the State, is a SaaS (PMIS) solution. Team CNSI is also including Option A- and Option B-specific turnover activities in this section. Where the requirements for turnover differ for Option A and Option B, we have noted this in our turnover activity descriptions.

Team CNSI's turnover activities include the following:

- Governance Structure – provide organizational chart and roles and responsibilities to support the turnover activities.
    - Provide current organizational chart.
    - Produce a staff list of current resources, expertise, responsibilities, and hours dedicated to their role.
- Documentation – Provide documentation for new staff. Team CNSI actively maintains documentation of system functionality, procedures, and lessons learned throughout the projects. Therefore, Team CNSI will provide this early in the transition. New resources may then leverage this documentation as a reference both during and after the turnover period.
    - Provide current version of business operations procedures. (Option B-specific)
    - Provide current version of the technical approach. (Option A and Option B)
    - Use OTRS ticketing system to gather common issues and how they were resolved, and use Jira to assist with technical understanding of issue resolution.
    - Provide current documentation of lessons learned for the project.
- Training – Provide training to new resources. (Option A and Option B only)
    - Team CNSI uses OTRS for incident management and Jira for defect and release management. These systems will be used for scenario training. OTRS tickets can provide examples of what to expect and can be used to demonstrate the issue through resolution.
    - Functional role training – Formal training will be provided for each functional role by those who are currently performing the duties. This will be invaluable to the new resource
    - Practical application "Doing" – Part of the transfer process is allowing the new resource to perform the work. Most people learn best by doing. Team CNSI members will work closely with their replacements.
- Shadowing – Following training, Team CNSI will support shadowing opportunities for the replacement staff, helping them develop the knowledge necessary to perform their duties. Team CNSI's goal is to build a strong team that will succeed in performing their duties. (Option A and Option B only)
- Monitoring – Team CNSI will follow Project Management best practices to monitor and report the progress of the Turnover activities. This includes providing readiness assessments as the project nears the final stages.
- Work in progress – It is expected that there will be work in progress that will need to be taken over by the new team. Team CNSI will work with the replacement vendor to plan and transfer these activities leveraging, when possible, shadowing opportunities to work together during the handoff.

- OTRS and Jira will be a valuable source of information to determine inflight issues and priorities.
- System data and files as appropriate
- IVR Activities (Option B)
- Active Call Center Incident Reports (Option B)

PTO01

The Contractor shall provide a turnover approach and the services required for the transition of operations, services and module components.

Team CNS will provide a Turnover Plan that defines the turnover approach and identifies all the activities and services required for the transition of business operations and services operations we support. We will plan for and provide support for data conversion from the evoBrix PMIS solution to DPHHS' selected replacement solution. Team CNSI will prepare a comprehensive work breakdown structure and schedule supporting the Turnover Plan.

The Turnover Plan and related schedule will be developed during the second full year of operations and delivered to DPHHS at least six months prior to the end of the contract as required in Requirement PTO02.

PTO02

At least six (6) months prior to the final Contract year (including option years that have been exercised) and at least six (6) months prior to the end of any contract extension(s), the Contractor shall provide the following:

a. An updated Turnover Plan.

b. Complete and update system and user documentation.

c. Statement of the resources that would be required by the Department or another contractor to fully take over solution, technical, and business functions outlined in the Contract(s). This includes quantity and types of resources and volume of tasks to support the scope of work.

d. Operational tasks and procedures as necessary to support ongoing operations of the solution.

e. Lessons learned report.

f. List of incomplete tasks, such as system defects, modifications or enhancements, mass adjustments, reference updates, and configuration requests.

g. A detailed description of the services that would be required by another Contractor to fully take over system, technical, and business functions outlined in the Contract.

The Department reserves the right to request this information at any time throughout the Contract.

At least six months prior to the final contract year, Team CNSI will provide a Turnover Plan that defines:

- A final Turnover Plan and schedule
- Updated user and business process documentation (Option B-specific)
- A detailed statement of the resources required to take over operation of the business functions of the solution including:
  - Number and type of resources
  - Tasks and task volumes

©2017 CNSI

- Business process and procedure documentation for the operational tasks performed by Team CNSI (Option B-specific) sufficient for a third party to operate the solution
- A "lessons learned" report
- A list of incomplete tasks, such as reference updates, open customer service ticket, and other in-process or pending operational tasks required for turnover
- For Option B only, a detailed description of the services that would be required for another contractor to fully take over the business functions outlined in the contract.

The table of contents of a proposed plan that will be tailored for the MT PSM turnover is provided in Figure 3.10.6-1.

Table of Contents

Signature Page ..... **i**
Table of Contents ..... **ii**
Revision History ..... **iii**
1. Turnover Plan Overview **1-1**
1.1 Plan Purpose and Scope 1-1
1.2 Document Structure 1-1
1.3 Audience and Intended Use 1-2
1.4 References and Standards 1-2
1.5 Abbreviations and Acronyms 1-3
2. Organization, Staffing, Roles, and Responsibilities **2-1**
3. Turnover Plan Details **3-1**
3.1 Turnover to Operations Management and Oversight 3-2
3.2 Entry Criteria 3-2
3.3 Turnover Planning 3-2
3.4 Contingency Planning 3-3
3.5 Operational Readiness Assessments 3-3
3.6 Outreach and Communication Approach 3-4
3.7 Operations Turnover 3-6
3.8 Quality Assurance Activities 3-6
3.9 Exit Criteria 3-7
4. Transition Tools and Methods/Technologies **4-1**
5. Supporting Material **5-1**
5.1 Communications 5-1
5.1.1 Documentation and Reporting 5-1
5.1.2 Coordinating with Stakeholders 5-1
5.2 Orientation and Training 5-1
5.3 Turnover Plan Change and Configuration Control 5-1
5.4 Records Management 5-1
5.5 Transition Process Evaluation 5-2
5.6 Turnover Plan Maintenance and Update 5-2

MTPSM-3-216

Figure 3.10.6-1. Team CNSI's Turnover Plan Table of Contents. Team CNSI's Turnover Plan provides a road map to transition system data and, for Option Business operations to the successor contractor.

Team CNSI understands that the Department reserves the right to request this information at any time throughout the contract.

PTO03

The Contractor shall provide a Monthly Turnover Report reflecting transition activities during the turnover period.

Team CNSI will provide a monthly Turnover Report reflecting the status of transition activities during the turnover period. Team CNSI will work with DPHHS and its new contractor to ensure that the report accurately reflects the necessary activities and their status throughout the turnover period. The status report will include the following:

- Recent accomplishments, milestones met, and deliverables completed
- Plan for the upcoming period including major tasks, milestones, and deliverables
- Status of any risks being tracked
- Status of any issues being tracked
- An extract of the turnover schedule providing status of each major step

PTO04

The Contractor shall provide operational procedures that describe how maintenance is performed for the solution.

Since Team CNSI is offering the PMIS as a SaaS solution, the Team CNSI and the State will engage in collaborative discussions to determine the scope of turnover needed for the PMIS. For Option B, Team CNSI actively maintains operational procedures throughout the MT PSM project and will provide the current version of the documentation we use to perform our operational activities

PTO05

The Contractor shall cooperate with the successor contractor while providing all required turnover services. This will include meeting with the successor and devising work schedules that are agreeable for both the Department and the successor contractor.

Team CNSI approaches Turnover with the same commitment to DPHHS success as we do to the initial implementation of our solution. We will work collaboratively with DPHHS, its System Integrator, and the successor contractor to define the activities and schedule for an effective transition. This includes initially meeting with the successor contractor to develop a mutually agreeable schedule. Once the schedule is finalized, Team CNSI will work with the successor contract as defined in the agreed schedule to review progress and ensure understanding of the turnover material we provide. DPHHS's satisfaction with Team CNSI's services applies to all phases of the project, including Turnover.

PTO06

The Contractor must transfer solution and services documentation and all data requested by the State to the State.

Team CNSI actively maintains operational documentation throughout the MT PSM project. Team CNSI will transfer all applicable solution and services documentation as part of the Turnover efforts. In addition, we will transfer all data requested by the State to the appropriate receiving entity.

Additional activities apply for Option A and B:

For Option A, this involves transfer of relevant screens, web services, and the Edifecs EDI software.

For Option B, the CRM and IVR software licenses along with the current versions of the business services documentation will be transferred.

PTO07

The Contractor shall deliver a Turnover Results Report that documents completion of each step of the Turnover Plan.

Team CNSI will deliver a Turnover Results Report that documents completion of each step of the Turnover Plan. Team CNSI will include the Turnover Results Report as repeating deliverable within the monthly status report.

3.10.7 Project Deliverables and Documentation

The documentation deliverables outlined in Table 3.10.7 have been identified for this scope of work. DPHHS will review deliverable requirements and make changes to required deliverables based on Commercial-Off-the-Shelf (COTS)/Software-as-a-Service(SaaS) versus non-COTS/Non-SaaS software. For each documentation deliverable the Contractor shall follow the guidelines outlined in the Documentation Standards in the Procurement Library. The Contractor will submit documents that meet the specific deliverable acceptance criteria as outlined in the Deliverable Expectation Document for the specific deliverable. All deliverables must be approved by DPHHS. Project artifacts and information will be shared on the CMS Reuse Repository. The Offeror must describe their approach to meet each of the Documentation requirements defined in Attachment F, Requirements Matrix.

High quality, accurate, and timely deliverables are a critical element of the successful provision of services to the State of Montana.

The Team CNSI Advantage

The proven iVision360 SDLC Deliverble Management Process meets all DPHHS deliverable requirements.

- Tailorable for SaaS implementations
- Scales up or down to accommodate project scope and life span
- Incorporates PMI and CMMI best practices
- Proven in four PMIS implementations

MTPSM-3-192

To respond to the requirements provided in this RFP, Team CNSI provides the full set of deliverables from its highly structured iVision360 software development lifecycle and project management methodology. This framework is based on industry best practices, including the PMI PMBOK, and has been assessed at SEI CMMI Level 3. It is the same project management methodology framework that we used in the successful Michigan, Illinois, Utah, and Washington implementations.

This methodology is proposed here specifically to meet detailed documentation requirements. However, in consideration of the accelerated timeline of seven months for implementation and our proven Software-as-a-Service (SaaS) delivery model, Team CNSI believes the documentation requirements for deliverable expectation documents, associated deliverables and associated approval cycles may be prohibitive to rapid implementation in such a short time frame. Based upon the time line, availability of state resources to perform reviews, and due to the nature of the solution being a SaaS model, we believe documentation will require a more lean, agile approach in the end with tailoring to accommodate the progression through phases of a seven-month project life cycle. For example, we would suggest that the requirement for deliverable expectation documents be reviewed and allowance made for substituting pre-existing templates as the DED.

The iVision360 framework includes a deliverable management process that leverages progressive review steps, as shown in Figure 3.10.7-1.

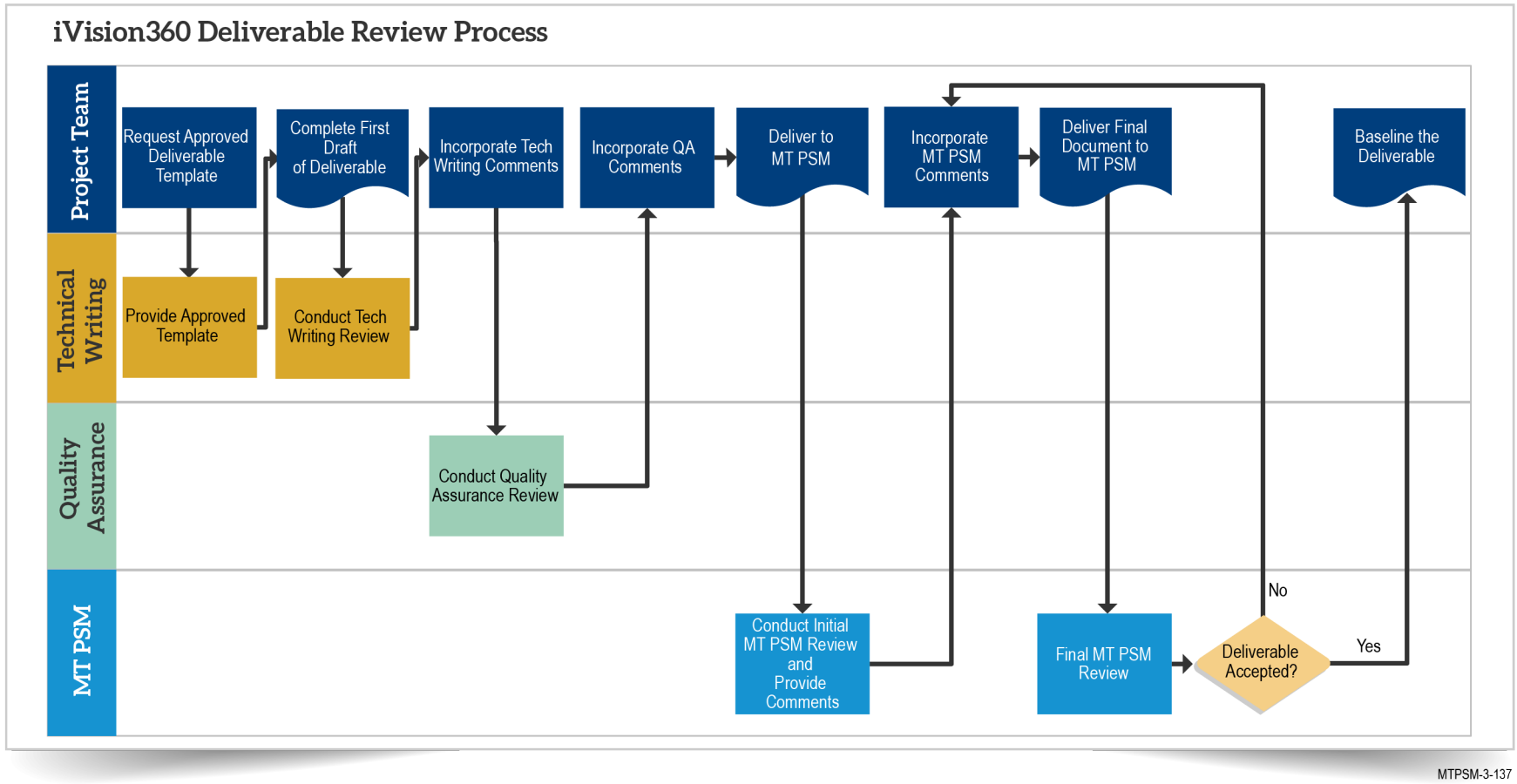


Figure 3.10.7-1. The iVision360 Deliverable Management Process. Integrating progressive review steps through the delivery process has been proven to increase the rate of initial acceptance of a deliverable.

This proven approach to deliverable review and management helps reduce the overall risk to the State, provides high-quality results on schedule, and ensures compliance with the requirements stated in the Montana Program for Automating and Transforming HealthCare (MPATH) Documentation Standards, including:

- Providing consistent structure to all deliverables
- Adhering to document naming conventions and version control
- Ensuring high-quality work products

Documentation Requirements

Team CNSI has addressed all requirements defined in RFP Table 3.10.7. The alignment to iVision360 and approach are highlighted in Figure 3.10.7-2. For the majority of the documentation requirements, Team CNSI recommends reviewing requirements with DPHHS to tailor existing templates and documentation to requirements. In addition, Team CNSI recommends using the

Deliverable	iVision360 Deliverable Name	Approach	Requirement Number
Project Management Plan	Project Management Plan	■ Tailor existing template ■ Submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan Team CNSI recommends all management plans be included in the Project Management Plan (PMT18) to accommodate the time line. These would include at a minimum: ■ DOC15 Communications Plan ■ DOC18 Change Management Plan ■ DOC24 Staffing Management Plan ■ DOC38 Risk Management Plan ■ DOC40 Issue Management Plan	PMT18
Project Work Plan	Project Management Plan	■ Tailor existing template ■ Submit Deliverable Expectations Document ■ Deliver in MS Word format with schedule attachment in MS Project ■ Submit as per the Project Work Plan	PMT19
Communication Plan	Communication Management Plan	■ Tailor existing template ■ Submit in Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC15
Quality Management Plan	Quality Management Plan	■ Tailor existing deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC16
Risk Management Plan	Risk and Issue Management Plan	■ Tailor existing template ■ Submit in Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC38
Issue Management Plan	Risk and Issue Management Plan	■ Tailor existing template ■ Submit in Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC 40

Deliverable	iVision360 Deliverable Name	Approach	Requirement Number
Change Management Plan	Change Control Plan	■ Tailor existing template ■ Submit in Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC18
Defect Management Plan	System Test Plan	■ Tailor existing deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC22
Staffing Plan	Staff Management Plan	■ Tailor existing template ■ Submit in Deliverable Expectations Document ■ Deliver in MS Excel format ■ Submit as per the Project Work Plan	DOC24
Data Management, Conversion, and Migration Plan	Conversion Plan	■ Tailor existing template ■ Submit in Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC03
Application, Configuration and Maintenance Plan	Configuration Management Plan, Iteration Plan, Release Schedule	■ Tailor existing template and deliverable ■ Submit in Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel appendices ■ Submit as per the Project Work Plan	DOC04
User Interface Style Guide	Detailed System Design Document	■ Tailor existing deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC46
User Documentation	Online help, Detailed System Design Document	■ Create template leveraging existing deliverable and online help ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC07
Operations Procedure Manual	Not Available	■ Create deliverable template ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	DOC42
Business Continuity and Disaster Recovery Plan	Disaster Recovery Plan	■ Create deliverable leveraging existing documentation ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC08, DOC09, DOC10
Operations Maintenance and Configuration Plan	Configuration Management Plan, Release Schedule, Operations Dashboards	■ Create deliverable leveraging existing documentation ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC12
Turnover Plan	Not Available	■ Create template ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC37
Updated Turnover Plan	Not Available	■ Update approved deliverable ■ Deliver in MS Word format using track changes ■ Submit as per the Project Work Plan	PTO02

Deliverable	iVision360 Deliverable Name	Approach	Requirement Number
Technical Documentation	Detailed System Design Document	■ Create template leveraging existing deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC19
System Design Documentation	Detailed System Design Document	■ Tailor existing template and documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC14
System Documentation	Detailed System Design Document	■ Tailor existing template and documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC29
Master Test Plan	Test Plan	■ Tailor existing template and documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC26
Training Plan	Not Available	■ Create template ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC27
System Test Plan	System Test Plan	■ Tailor existing deliverable and documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC28
Module Implementation Plan	Implementation Plan	■ Tailor existing template and documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	DOC13
Solution Architecture Document	System Architectural Diagrams	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	DOC21
Attachment - L-Technology Matrix	Not Available	■ Update Attachment L ■ Deliver in MS Excel ■ Submit as per the Project Work Plan	DOC44
Turnover Results Report	Not Available	■ Create template ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	PTO07
Monthly Status Report	Status Report	■ Tailor existing documentation to create proposed status report ■ Review proposed format with DOHHS ■ Update and submit in MS Word format ■ Submit monthly	PMT17
System Security Plan	Security Plan	■ Create template from existing documentation ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	DOC01

Deliverable	iVision360 Deliverable Name	Approach	Requirement Number
CMS Information Security Program Plan of Action and Milestones (POA&M)	Not Available	■ Create deliverable if necessary based on security risk assessment findings	SEC55
Risk Assessments	Not Available	■ Create deliverable annually and as needed	SEC11
Requirements Traceability Matrix (RTM)	Requirements Traceability matrix Gap Traceability Matrix	■ Tailor existing template and documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Excel format ■ Submit as per the Project Work Plan	RQM06
CMS Certification Checklists	Not Available	■ Tailor CMS Checklist documentation ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Excel format ■ Submit as per the Project Work Plan	CERT02
Certification Plan	Certification Plan	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	DOC02
Operational Readiness Checklist	Implementation Checklist	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	IA06
Operational Readiness Test Results	Implementation Checklist	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	IA04
Penetration Test Report	Not Available	■ Create deliverable ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	SEC15
Performance Test Results	Volume/Performance Test Results	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	TEST04
System Test Results	System Test Results	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	TEST04
Parallel Test Results	Parallel Test Results	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	TEST04
Regression Test Results	System Test Results	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	TEST04
Integration Test Results	System Test Results	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	TEST04

Deliverable	iVision360 Deliverable Name	Approach	Requirement Number
Disaster Recovery/Business Continuity Test Report	Disaster Recovery Test Results	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	OCM03
Monthly Turnover Report	Status Report	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	PTO03
Subcontractor Usage Report	Not Available	■ Create deliverable ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	SUB05
System Enhancement Pool Report	Not Available	■ Create deliverable template ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Excel format ■ Submit monthly	PMT29
Business Rules Catalog	Detailed System Design Document	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	BR03
Certification Crosswalk	Certification plan	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	CERT01
Personnel Background Check Attestation	Not Available	■ Create deliverable template as necessary ■ Deliver in MS Word format ■ Submit as necessary	KR 19
Interface Control Documents (ICD)	Detailed System Design Document	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	INR07
Deliverable Review and Acceptance Process	Project Management Plan	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	PMT15
Data Dictionary	Detailed System Design Document	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	DM11
Conceptual Data Model	Detailed System Design Document	■ Tailor existing documentation to create deliverable ■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	DM55
Implementation Letter	Delivery Letter	■ Tailor existing documentation to create deliverable ■ Deliver in MS Word format ■ Submit as per the Project Work Plan	IA01
Security Audit Report	Not Available	■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	SEC22

©2017 CNSI

Deliverable	iVision360 Deliverable Name	Approach	Requirement Number
Service Organization Control (SOC) 1 Type II Reports	Not Available	■ Create and submit Deliverable Expectations Document ■ Deliver in MS Word format with MS Excel attachments ■ Submit as per the Project Work Plan	SEC73

Figure 3.10.7-2. Deliverable List. Team CNSI. Team CNSI leverages existing templates and deliverable reviews to ensure high-quality delivery.

Deliverable Review Process

Team CNSI's iVision360 methodology defines a proven, highly-structured process for managing deliverables, starting from the initial draft through final approval and publication. In addition, Team CNSI's Quality Management Plan identifies procedures for ensuring the quality of documents from inception to delivery (e.g., peer review process, project quality review, and release process). This plan also includes process evaluation and improvement guidelines applicable to evaluating and improving document management processes and outputs. Core outcomes of this internal review process include the following:

- Verify that the document satisfies acceptance criteria
- Confirm that the content is correct
- Verify that the content is complete
- Validate consistency between the deliverable sections
- Ensure that all approval conditions have been satisfied and that the document is approved
- Verify consistency across other deliverables

Each step of the procedure is explained below, including the process for a formal deliverable. These steps are also used when making major updates or changes to an existing document. The project schedule dictates the rigor and time each step can remain in process along with considerations for the size and complexity of the deliverable. More detailed deliverables require more time at each phase from production through reviews. Team CNSI will work with the state to compare their requirements with the constraints of the project to determine the best path forward for each deliverable.

Produce Initial Draft

The initial draft of a formal deliverable will be produced and designated for internal review. The Team CNSI deliverable author creates the initial deliverable draft and publishes the deliverable into the Project Portal (SharePoint). Then, the author notifies reviewers that the deliverable is ready for internal review and provides the schedule for the internal review activities in accordance the master project schedule.

Initial Review Preparation

An internal review consists of a peer review or an informal review. A peer review is a formal review of specific deliverables, such as the Summary Gap Analysis Report or the design documentation, by designated Team CNSI subject matter experts. During the peer review, the entire deliverable is examined for completeness. Peer reviewers ensure that all facts, figures, diagrams, and requirements have been correctly incorporated and adequately cover the topic of the deliverable. The detailed steps of the peer review process are defined in the iVision360 framework. For a peer review, the Team CNSI deliverable owner is responsible for setting up, notifying participants, and conducting the peer review with the peer review moderator. The peer review notice gives information regarding the deliverable that is being reviewed, the designated review location(s), time(s), and, most importantly, directions on the location of the peer review items in the project portal. During the preparation time, the peer review members review

the material prior to the peer review session. Each reviewer prepares a set of comments and questions to be discussed at the meeting.

Conduct Informal/Peer Review

For an informal review, the reviewer conducts their review and sends his or her feedback to the owner indicating what needs to be addressed. For a peer review, the moderator initiates discussion regarding each comment and question from each reviewer. In that peer review, the recorder (usually the author) compiles the set of comments in a review log.

Produce Next Draft

The author incorporates all agreed upon comments and suggestions from the informal review or peer review session. Once all review feedback is incorporated into the deliverable, the author sends the document back to the reviewer (for an informal review) or to the verifier(s) listed in the peer review issue log (if a peer review is involved).

Technical Writing Review

The Technical Writing (TW) team verifies the format and structure of the deliverable, ensures the correct template is used, and corrects any grammar errors. This team also ensures the glossary, acronyms, and referenced documents apply to the deliverable.

The TW team notifies the author of the results of the TW review. If any major comments or rework is required, the team requests that the corrected deliverable be returned for a second TW review. Otherwise, the author addresses minor comments, then submits the deliverable to the Quality Assurance (QA) team for review.

Quality Assurance Review

After receiving notification from the author, the QA team performs a QA review to verify that the deliverable is complete and consistent with the deliverable template and that all applicable comments from the peer review session have been addressed. If the QA review results in the identification of major discrepancies, the deliverable is returned to the owner for correction. Otherwise, the deliverable is prepared for delivery to DPHHS.

Delivery to DPHHS

Once the deliverable passes the QA review, the author prepares the document for delivery by creating the delivery notification and ensuring all applicable deliverable attachments have been published to the project portal (SharePoint). Team CNSI then notifies DPHHS that the deliverable is available in the Project Portal for DPHHS review.

DPHHS Initial Review

DPHHS reviews are scheduled to avoid multiple conflicting simultaneous deliverable reviews. The review focuses on completeness and ensures that topics are covered sufficiently per the acceptance criteria and review timeframes established for the deliverable. The duration of the initial review is time scaled based on the size and complexity of the deliverable. DPHHS provides their review comments to Team CNSI within the review cycle defined in the project schedule. Upon completion of the DPHHS review process, the DPHHS project manager (PM) or designee gathers all comments from the reviewers and consolidates them (including de-duplication) into a single deliverable comments form. After all

comments are consolidated, the DPHHS PM or designee notifies Team CNSI that the comments have been consolidated into a consolidated deliverable comments form that has been published in the Project Portal and is ready for review. Upon receiving the notification from DPHHS, Team CNSI reviews the comments. The primary objective of the comment review is to assess the magnitude of the required changes. If review comments are not complex, authors will proceed to fix the review comments and produce the final deliverable draft for DPHHS approval. Complex review comments may require a meeting with DPHHS to confirm the required changes.

Produce the Final Draft and Deliver

The final draft incorporates agreed-upon comments from DPHHS. Once the applicable DPHHS comments have been incorporated, the Team CNSI document owner performs a final review to ensure all comments have been addressed, publishes the revised version to the Project Portal, and notifies the management team that the deliverable is ready for final delivery. The management team confirms that the correct version of the deliverable, the delivery letter, and all applicable deliverable attachments have been published to the project portal. Team CNSI then notifies DPHHS that the deliverable is available in the project portal for final review and approval.

DPHHS Final Review and Deliverable Approval

DPHHS reviews are scheduled to avoid multiple conflicting simultaneous deliverable reviews, and the duration of the final review is time-scaled based on the size and complexity of the deliverable. DPHHS verifies that all comments have been incorporated into the final draft and approves the deliverable following the agreed upon acceptance guideline in the deliverable acceptance criteria. If further discrepancies are found, a meeting is held between DPHHS and Team CNSI to discuss the issues, and the deliverable process returns to the "DPHHS Initial Review" step.

Baseline the Deliverable

The baseline is a formal deliverable signed by DPHHS, signifying acceptance of the deliverable per contractual criteria. After receiving DPHHS approval of the deliverable, it is baselined by accepting all tracked changes and deleting all comments in the document. The baselined deliverable and DPHHS comment log is published to the Project Portal and then uploaded to the CMS Reuse Repository and is available at any time to be viewed by anyone with authorization to access the deliverable.

DOC01

The Contractor shall develop, execute, maintain and deliver for the State's approval, a System Security Plan (SSP) that will document the current level of security controls within the module scope of work that protects the confidentiality, integrity and availability (CIA) of the solution and its information. This is a living document and will be updated no less than annually and when new vulnerabilities are identified and mitigated and when additional functionality and/or components are implemented. The System Security Plan must be approved before any State data is transferred or entered into the solution. The State must approve all revisions of the System Security Plan. If the Contractor's solution is hosted by the State, the State will provide supporting information to the Contractor to complete the SSP.

The SSP must address the following topics:

• Adherence to the State's requirements outlined in the "Security and Privacy Controls Requirements" document, included in the Procurement Library;

• Compliance with the Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Safeguards (ARS) to assess CIA and NIST SP 800-53 Rev 4;

• Data center physical security, complying with the Federal Information Processing Standards'

©2017 CNSI

Automatic Data Processing Physical Security and Risk Management (FIPS PUB.31);

- Network segmentation, access controls, and forensics;
- Perimeter security;
- Application security and data sensitivity classification, including Protected Health Information (PHI) and Personally Identifiable Information (PII);
- End-point protections such as multiple redundant firewalls and host-based intrusion detection systems;
- Identification and prevention of the use of prohibited functions, ports, protocols, and services;
- Network, firewall, server and other security-related configurations and changes;
- Intrusion detection and prevention;
- Network scanning tools;
- Host hardening;
- Internet filtering;
- Remote access;
- Encryption of data at rest and in transit;
- User authentication and directory services;
- Interfaces and exchange of data with external entities;
- System penetration testing;
- Management of operating system and security patches;
- Anti-Virus and malware detection and email gateways;
- Assessment and testing of system and code modifications; and
- Allowable internal and external communication protocols.

Team CNSI understands the importance that underlines the requirement to maintain comprehensive security documentation throughout the MT PSM project. Based on our experience and documentation from our Medicaid projects in Michigan, Washington, Illinois, and Utah, Team CNSI will collaborate with the State of Montana to tailor Team CNSI's Security Plan to meet DPHH requirements, including:

- Alignment to the Security and Privacy Controls Requirements
- Completes with CMS Acceptable Risk Safeguards
- Data Center physical security and compliance with Federal Information Processing Centers
- Network access controls and monitoring
- Application security and data classification
- End-point protections, such as redundant firewalls
- Identification and prevention of the use of prohibited functions
- Network, firewall, and server security configurations
- Intrusion detection and prevention
- Network scanning tools
- Host hardening
- Internet filtering
- Remote access controls
- Data encryption
- User authentication
- Interfaces and exchange of data with external entities
- System penetration testing
- Management of operating system and security patches

©2017 CNSI

- Anti-Virus and malware detection and email gateways
- Assessment and testing of system and code modifications
- Allowable internal and external communication protocols

Figure 3.10.7-3 provides the Security Plan table of contents from an actual deliverable which is generally used in other MMIS projects.

Table of Contents

REVIEW LOG ..... **vi**
1. INTRODUCTION **1**
2. SYSTEM IDENTIFICATION **1**
2.1 SYSTEM NAME/TITLE 1
2.2 RESPONSIBLE ORGANIZATION 1
2.3 DESIGNATED CONTACTS 2
2.4 ASSIGNMENT OF SECURE RESPONSIBILITY 3
2.5 SYSTEM OPERATIONAL STATUS 3
2.6 DESCRIPTION OF OPERATIONAL/SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS 4
2.6.1 Identify Management and User Authentication and Authorization 4
2.6.2 Data Center Cloud Hosting 4
2.6.3 Network Access to Backend Systems 4
2.7 SYSTEM INTERCONNECTION/INFORMATION SHARING 4
3. SECURITY CONTROLS DETAIL AND COMMENT **5**
3.1 ACCESS CONTROL (AC) FAMILY 5
3.2 AWARENESS AND TRAINING (AT) FAMILY 32
3.3 AUDIT AND ACCOUNTABILITY (AU) FAMILY 35
3.4 CERTIFICATION, ACCREDITATION AND SECURITY ASSESSMENTS (CA) FAMILY 41
3.5 CONFIGURATION MANAGEMENT (CM) FAMILY 45
3.6 CONTINGENCY PLANNING (CP) FAMILY 61
3.7 IDENTIFICATION AND AUTHENTICATION (IA) FAMILY 71
3.8 INCIDENT REPSONSE (IR) FAMILY 80
3.9 MAINTENANCE (MA) FAMILY 92
3.10 MEDIA PROTECTION (MP) FAMILY 92
3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) FAMILY 100
3.12 PLANNING (PL) FAMILY 108
3.13 PERSONNEL SECURITY (PS) FAMILY 115
3.14 RISK ASSESSMENTS (RA) FAMILY 121
3.15 SYSTEM AND SERVICES ACQUISITION (SA) FAMILY 125
3.16 SYSTEM AND COMMUNICATIONS PROTECTION (SC) FAMILY 142
3.17 SYSTEM AND INFORMATION INTEGRITY (SI) FAMILY 153
3.18 INFORMATION SECURITY PROGRAM (PM) FAMILY 170
4. PRIVACY CONTROLS DETAIL AND CONTROL IMPLEMENTATION DESCRIPTION **179**
4.1 AUTHORITY AND PURPOSE 180
4.2 ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT (AR) 182
4.3 DATA QUALITY AND INTEGRITY (DI) 190
4.4 DATA MINIMIZATION AND RETENTION (DM) 191
4.5 INDIVIDUAL PARTICIPATION AND REDRESS (IP) 194
4.6 SECURITY (SE) 199
4.7 TRANSPARENCY (TR) 201
4.8 USE LIMITATION (UL) 202
5. APPENDICES AND ATTACHMENTS **205**
5.1 APPENDIX A – IRS REQUIREMENTS FOR SAFEGUARDING FTI 205
5.2 APPENDIX B – EQUIPMENT LIST 182
5.3 APPENDIX C – SOFTWARE LIST 190
5.4 APPENDIX D – DETAILED CONFIGURATION SETTINGS 191
5.5 APPENDIX E - GLOSSARY 194
5.6 APPENDIX F – ACRONYMS AND ABBREVIATIONS 199

MTPSM-3-205

Figure 3.10.7-3. Security Plan Table of Contents. Team CNSI will collaboratively review and tailor the Security Plan to meet Montana's requirements.

Team CNSI will leverage our existing, well documented System Security Plan as the starting point. We acknowledge that the System Security Plan is a living document and will be updated no less than annually and when new vulnerabilities are identified and mitigated and when additional functionality and/or components are implemented. Team CNSI will ensure that the System Security Plan will be approved before any State data is transferred or entered into the solution.

DOC02

The Contractor shall develop and maintain a Certification Plan that defines the contractor's approach to CMS certification. It must describe the processes and procedures that will be used to manage Certification requirements. The Certification Plan must comply with the most current MECT process to

ensure the system will meet all certification requirements.

System certification from CMS is a shared goal of DPHHS and Team CNSI. Team CNSI brings the experience and tools at contract award to ensure this goal is achieved on the first attempt. We minimize risks by providing evoBrix module components that have been previously certified by CMS in Michigan and Washington.

Team CNSI begins early in the project by working with DPHHS to tailor the Certification Plan we have used in our prior certification efforts. Team CNSI will work with DPHHS to finalize the support approach for certification under the most current MECT process and synchronize our efforts. Team CNSI will then prepare the Certification Plan for the MT PSM solution. A sample table of contents from a prior certification effort is shown in Figure 3.10.7-4.

Table of Contents

1. Introduction 1
1.1 Document Purpose 1
1.2 Document Organization 1
1.3 Reference to Other Documents 2
1.4 Audience 2
2. Certification Overview and Assumptions 7
2.1 Certification Definition 7
2.2 Relationship between Certification Plan and MECT 8
2.3 Roles and Responsibilities 8
3. Certification Approach and Methodology 9
3.1 Draft and Final Certification Plan 9
3.2 The Process 9
3.2.1 Initial Assessment 9
3.2.1.1 Identification of SCI Certification Stakeholders 9
3.2.1.2 [redacted] to MITA Crosswalk Evaluation 10
3.2.1.3 Initiating Preemptive Remedation for SCI Phase 11
3.2.2 Activities During SCI 12
3.2.2.1 Managing Crosswalk Updates 12
3.2.2.2 Managing Certification Checklist Reevaluation 13
3.2.2.3 Pre-implementation Certification Readiness Review 14
3.2.2.4 Establish the Certification Evidence Repository 15
3.2.3 Preparation for formal Certification Request 16
3.2.3.1 Identify Critical Success Factors 16
3.2.3.2 Commission Certification Team 17
3.2.3.3 Construct Initial Certification Schedule 17
3.2.3.4 Conduct Certification Team Orienation 18
3.2.3.5 Data Collection, and Monitoring 18
3.2.3.6 Perform Periodic Progress Reporting 19
3.2.3.7 Conduct Certification Readiness Review 19
3.3 Request to CMS for Certification Review 20
3.4 Review Preparation 20
3.5 CMS Certification Review 21
3.6 Certification Disposition 22
3.6.1 Potential Remediation Activity 22
3.6.2 Final Certification Disposition 22
4. Appendices 23
4.1 Appendix A – Acronyms and Terms 23
4.2 Appendix B – Deliverable Acceptance Criteria 24

MTPSM-3-206

Figure 3.10.7-4. Team CNSI's Sample Certification Plan Outline. Using a proven plan, Team CNSI provides support for the enterprise certification effort throughout the project. We use our historical documentation data store and evoBrix to MITA crosswalk to launch certification efforts early, which reduces risks to DPHHS.

DOC03

The Contractor shall develop, submit, and maintain a Data Management, Conversion and Migration Plan to include the following:

a. A data management strategy that will support integration, optimization, quality, stewardship, standards, and governance of data.

b. description of appropriate skill sets, processes, technologies/tools, and any naming conventions followed.

c. Approach to conversion, cleansing and migration.

d. Approach to risk management for data conversion effort.

e. Approach for testing migration or converted data;

f. Approach to reporting the number of records successfully converted vs. errors or exceptions.

g. Approach for cleansing data to prepare it for loading to the proposed solution that is refined as necessary.

h. Approach to resolving data conversion errors and issues.

i. Approach for supporting the Department validation of converted data.

j. Tasks, timelines, and responsible parties for all conversion and migration tasks.

k. Entrance and exit criteria for each phase of the effort.

Conversion and management of the legacy data is an integral component of the MT PSM project. Team CNSI has successfully accomplished data conversions for the states of Maine, Washington, Michigan, Utah, and Illinois. The technical and management processes used on those large-scale initiatives to support conversion and a smooth data transition are documented in Team CNSI's data conversion plan. Specifically, the plan documents:

- The processes and tools to be used for the Data Conversion activity.
- Conversion, cleansing and migration approach.
- Risk management and mitigation approach for data conversion issues.
- Approach for testing converted and migrated data.
- Stakeholder involvement in the data conversion process.
- The standardized source file layouts and the periodic extracts from the source system for supporting iterative data conversion runs.
- Generation of exception/reconciliation reports. The comprehensive conversion reporting mechanism for exception handling and reconciliation will provide statistics of the converted data, as well as provide a monitoring mechanism during the iterative conversion runs to ensure that the data transformation occurred in an iterative and increasingly improved fashion over the course of the execution of the implementation. As the source system is a live system, the iterative process will also account for source data getting generated during the project timeline.
- The testing mechanism for the converted data, both through the backend as well as through the application itself.
- Data cleansing activities based on the exception and reconciliation reports, ensure the source data gets incrementally refined and transformed during conversion from the source to the target system.
- Generation of the final Go-Live conversion report and post-Go-Live report to address any conversion-related questions.

Team CNSI will work collaboratively with DPHHS to tailor this successful data conversion plan to meet Montana requirements and prepare the Data Management, Conversion, and Migration Plan. A sample table of contents from a prior data conversion effort is included in Figure 3.10.7-5.

Table of Contents

Section 1 – Preface....1
1.1 Purpose....1
1.2 Scope....1
1.3 Audience....1
1.4 Referenced Documents....1
Section 2 – Overview....2
Section 3 – Conversion....3
3.1 Tools and Technology....3
3.2 Conversion Process Flow....3
3.3 Environments....4
3.4 Conversion Job Structure....5
3.5 Exception Handling....6
3.6 Testing and Validation of Converted Data....7
Section 4 – Provider Enrollment Core Data Overview....9
4.1 Provider Enrollment Data Model Overview – Major Entities....9
Appendix A – Glossary....11
Appendix B – Acronym List....12

MTPSM-3-207

Figure 3.10.7-5. Team CNSI's Sample Data Conversion Plan Outline. Team CNSI brings to Montana a proven approach and plan for data conversion and management.

DOC04

Prior to beginning design and configuration/build activities, the Contractor must develop and submit to the State an Application Configuration and Maintenance Plan that describes the Contractor's approach to applications configuration and enhancements including:

a. Approach to conducting design sessions or walkthroughs.

b. Approach to conducting sprints or iterations.

c. Configuration management.

d. Schedule of major and minor releases.

e. Tasks, timelines, and responsible parties for design and configure/build tasks.

f. Approach to system enhancements

g. Programming and coding standards

The plan must be maintained through the system implementation. Revisions must be approved by the State.

Team CNSI has established processes supporting the Solution, Configure, and Implementation (SCI) methodology for design, configuration, and build having worked with both Illinois and Utah on recent successful provider projects and earlier MMIS implementations in Washington and Michigan. These processes are documented in our iVision360 framework supported by the Configuration Management Plan. Team CNSI will tailor these documents and provide a consolidated Application Configuration and Maintenance Plan prior to the commencement of the solution phase. This deliverable will contain:

- Approach for conducting the solution analysis and modeling sessions
- Approach and roles and responsibilities for configuration iterations
- Configuration management processes, tools, and roles and responsibilities
- Enhancement and release planning and schedule
- Programming and coding standards

Team CNSI acknowledges and accepts that the Application Configuration and Maintenance Plan will be maintain through system implementation.

DOC46

The Contractor shall provide a User Interface Style Guide or equivalent document defining the design standards for user interfaces. The User Interface Style Guide must demonstrate how the solution meets the most current MECT user interface requirements including:

a. User ability to customize or make adjustments (e.g. language support, font size) to portal presentation.

b. Users utilizing scripting languages and/or assistive technology have the ability to access the information, field elements, and functionality required for electronic form or page completion and submission including directions and cues.

c. User Interface organization so documents are readable without requiring an associated style sheet. completion and submission of forms, to display content or create interface elements.

d. User Interfaces identifying row and column headers for data tables.

e. User Interfaces informing users when a timed response is required and given sufficient time to indicate more time is required.

f. User Interfaces providing a method that permits users to skip repetitive navigation links.

g. User Interfaces provide text titles for frames to facilitate frame identification and navigation.

h. User Interfaces use markup to associate data cells and row/header cells for data tables that have two or more logical levels of row or column headers.

Team CNSI's proposed PMIS solution is documented primarily in the form of Detailed System Design Documents (DSDDs). The DSDDs provide functional details on the user interface. Team CNSI will leverage this document and create the User Interface Style Guide for the MT PSM project, including:

- Configuration options for the portal presentation, such as language support and font size
- Use of scripting languages or other tools to access the information, field elements, and functionality required for electronic form or page completion and submission
- User interface organization
    - Completion of forms
    - Display content
    - Interface elements
- Row and column headers for data tables
- User interfaces informing users when a timed response is required and given sufficient time to indicate more time is required
- User interfaces providing a method that permits users to skip repetitive navigation links
- User interfaces provide text titles for frames to facilitate frame identification and navigation
- User interfaces use markup to associate data cells and row/header cells for data tables that have two or more logical levels of row or column headers

DOC07

The Contractor shall provide during the initiation phase of the project and maintained throughout the project user documentation.

The State requires User Documentation for use by a novice business user to understand the automated system or application from a business function perspective. The Contractor shall provide comprehensive, well-organized user documentation. The Contractor's User Documentation shall include

at a minimum:

• Written in a procedural step-by-step format. (Instructions for sequential functions must follow the flow of actual activity).

• Manuals that helps users understand the purpose and operation of the module/module component(s) for each business process/major program/functional area.

• Acronyms used in user instructions must be identified and must be consistent with windows, screens, reports, and the data element dictionary.

• Cover system navigation, online help, and policies and procedures.

• The documentation must be available on-line and provide an on-line search capability with context-sensitive help.

• Provide the ability to produce a PDF version upon request

• Use version control to retain historical versions of documentation and revisions must be clearly identified.

• User documentation must be written and organized so that novice users can learn from reading the documentation how to access the on-line windows/screens, read reports, and perform all other user functions.

• User manuals must contain a table of contents and an index.

• Definitions of codes used in various Sections of a user manual must be consistent.

• Descriptions of error messages for all fields incurring edits must be presented and the necessary steps to correct such errors must be provided.

• Abbreviations must be consistent throughout the documentation.

• Each user manual must contain a Section describing all reports generated within the subsystem, which includes the following:

1.) A narrative description of each report.

2.) The purpose of the report.

3.) Definition of all fields in the report, including detailed explanations of calculations used to create all data and explanations of all subtotals and totals.

4.) Definitions of all user-defined, report-specific code descriptions; and a copy of representative; and pages of each report.

• Instructions for requesting reports or other outputs must be presented with examples of input documents and/or screens.

• Instructions for making on-line updates must clearly depict which data and files are being changed.

Team CNSI's proposed PMIS solution is documented primarily in the form of DSDDs. These documents provide users a sequential series of steps to the functionality available in the solution. The DSDDs are organized in a logical manner to provide users clearly documented navigation and process documentation. The overall organization of the DSDDs is described in Figure 3.10.7-6.

DSDD Part	Description
Part 1 - Overview	Part 1 provides an overview of the functional module including: ■ A description of the business process and functions within the module ■ Module context diagram that shows the interactions between the module and other external system of modules ■ Design assumptions, constraints, and dependencies ■ User Interface model, including layouts for the following components ● Web page ● Dialog page

DSDD Part	Description
	• Search page • Detail page • Screen • Data Models • Report layouts • Correspondence layouts
Part 2 - Use Cases	Part 2 consists of one or more logical group that define the module functionality and interfaces: ■ The functional use cases defining business functionality in step by step main and alternate flow ■ Business rules defining the system actions ■ System and Error Messages, including names and descriptions ■ Special Design Constraints
Part 3 - Appendices	Part 3 consists of appendices with specific detailed design content, such as: ■ Definition of profiles or standard actors used in the use cases ■ Medicaid Information Technology Architecture Business Architecture Traceability Matrix ■ Applicable edits or audits ■ Configuration values ■ Transaction mapping documents ■ Glossary and Acronym List

Figure 3.10.7-6. Organization of DSDD Part. The DSDD defines the solution functionality in logical manner for users.

Team CNSI will post the DSDDs to the online document repository, so it may be accessed, printed in PDF format, and searched by users online. As a deliverable, the DSDDs will be governed by Team CNSI's Configuration Management Plan, and all revisions will be tracked through the revision history and notification sent when updated versions are posted throughout the project lifecycle.

The evoBrix PMIS solution also offers a user guide that is organized by procedures to facilitate use of the system. The procedures in the guide are formatted as job aids that provide end users with the steps needed to complete procedures for their role. The guide can be tailored and updated as functionality evolves in addition to online help that users may access to receive information on the screen fields, definitions, and business features.

DOC08

The Contractor shall develop and maintain annually, a Business Continuity and Disaster Recovery Plan that must be in place before any Department data is transferred or entered into the solution. The Plan must contain procedures for data backup, restoration, and emergency mode operations in the event of:

a. Hardware or Software Failures;

b. Human Error;

c. Natural Disaster; and/or

d. Other unforeseeable emergencies.

The Business Continuity and Disaster Recovery Plan must be approved by the Department.

Team CNSI proposes a model for disaster recovery (DR) and business continuity successfully used in our other Team CNSI Medicaid solutions, including Washington, Michigan, Illinois, and Utah. The model of DR is called a "warm" DR and is divided into different priorities of recovery with the most critical coming first. For example, the provider enrollment and supporting transactional components will be of

highest priority for business restoration in the DR facility. If production experiences a declared disaster whether that be from hardware or software failure, human error, natural disaster, or other unforeseeable emergencies, all the users of the Montana solution will be redirected to the DR site. In other Team CNSI Medicaid solutions that have been operational since 2010, Team CNSI successfully planned and executed annual DR testing. These proven processes are documented in the Business Continuity and DR Plan which will be tailored in collaboration with DPHHS. A sample table of contents from another DR effort is included in Figure 3.10.7-7.

Table of Contents

Section 1 – Introduction....1
1.1 Purpose....1
1.2 Applicability....2
1.3 Related Contingency Plans....2
1.4 Scope....3
1.5 Non-[redacted] Cloud Components....6
1.6 References and Requirements....6
1.7 Record of Changes and Plan Maintenance....8
Section 2 – Concept of Operations....9
2.1 System Description....9
2.2 [redacted] Cloud Mission-Essential Functions....9
2.3 [redacted] Cloud Backup Procedures....24
2.4 State Application Hosting Environment....24
Section 3 – Implications of the [redacted] Cloud Hosting Environment....31
3.1 Options for [redacted] Cloud....31
3.2 The Duties of the [redacted] Cloud Disruption Response Team....34
3.3 Organization and Responsibilities....35
3.4 Line of Succession....38
3.5 Plan Training....39
3.6 Plan Testing....39
3.7 Plan Maintenance....40
Section 4 – Notification and Activation Phase....42
4.1 Notification Sequence....42
4.2 Damage Assessment....43
4.3 [redacted] Cloud DRP Activation Decision....43
4.4 Plan Activation....44
4.5 Notification Procedures....45
Section 5 – Recovery Operations....47
5.1 Disruptions....47
5.2 Recovery Phase, [redacted] Cloud Support System and/or Telecommunications....48
5.3 Recovery Phase, [redacted] Cloud User Facilities....49
5.4 Recovery Phase, [redacted] Cloud Users....51
5.5 Recovery Phase, [redacted] Cloud User Facilities and [redacted] Cloud Users....52
Section 6 – Reconstitution Phase....53
6.1 Reconstitution Phase, [redacted] Cloud Support System and/or Telecommunications....54
6.2 Reconstitution Phase, [redacted] Cloud User Facilities....56
6.3 Reconstitution Phase, [redacted] Cloud Users....57
6.4 Plan Deactivation....59
Appendix A – Acronyms....61
Appendix B – IT Standard Operating Procedures....65
Appendix C – Business Impact Analysis....66
Appendix D – Related Contingency Plans....67
Appendix E – Emergency Management Plan....68
Appendix F – Occupant Evacuation Plan....69

MTPSM-3-208

Figure 3.10.7-7. Team CNSI's Sample Disaster Plan Outline. Team CNSI brings DR Plan is proven in multiple Medicaid implementations.

DOC09

The Contractor's Business Continuity portion of the plan must include the following:

a. Identification of the core business processes involved in the production solution. For each core business process include:

1) Identification of potential failures for the process;

2) Risk analysis;

3) Impact analysis; and

4) Definition of minimum acceptable levels of service/output.

b. Definition of triggers for activating contingency plans.

c. Procedures for activating any special teams for business continuity.

d. A plan for recovery of business functions, units, processes, human resources, and technology

infrastructure.

e. Communication protocols and process for restoring operations in a timely manner.

Section 2 of Team CNSI's proven Business Continuity and DR Plan, as shown Figure 3.10.7-7, defines the core mission-critical functions, recovery timeline intervals, and other details that define the trigger and response expectations in the event of a disaster event. Section 3 of the plan defines the disaster response procedures. Team CNSI will work collaboratively with DPHHS to outline Montana-specific business continuity components that will be documented in the plan, including:

- Identification of potential events or failures that will trigger a disaster declaration
- Analysis of the risk and risk responses
- Analysis of the impact
- Agreement on the acceptable levels of service and outputs
- Definition of the threshold that will trigger contingency plans
- Documentation of the procedures for engaging the recovery teams
- Agreement on the plan to recover the mission-critical business functions
- Definition of the communication processes used during a disaster event

DOC10

The Contractor's Disaster Recovery portion of the plan must address, at a minimum:

a. Retention and storage of backup files and software;

b. Hardware backup for critical solution components;

c. Facility backup;

d. Backup for any telecommunications links and networks;

e. Backup procedures and support to accommodate the loss of any online communications;

f. A detailed file backup plan, procedures, and schedules, including rotation to an off-site storage facility.

g. The off-site storage facility must provide security of the data stored there, including protections against unauthorized access or disclosure of the information, fire, sabotage, and environmental considerations.

h. An enumeration of the prioritized order of restoration for Contractor's proposed solution.

i. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Team CNSI has supported operational Medicaid systems since 2010 and has successfully used the disaster plans to annually test the DR process and procedures. This Business Continuity and DR Plan, as outlined in Figure 3.10.7-7, will be tailored to accommodate Montana-specific content, including:

- Retention and storage of backup files and software for Montana
- Back-up of Hardware critical to the MT PSM solution components
- Defined Montana facility back-up, including telecommunication links and networks
- Back-up procedures for online communications
- Detailed backup plan and procedures for rotation to off-site storage facility
- Documented security protocols for back-up sites
- Prioritized mission-critical functions for restoration
- Defined plan for short-term uninterruptible power support to facilitate orderly shutdown of solution components in the event of power failure

DOC11

The Contractor shall update all project documentation (e.g., system design documentation, user and training documentation) as necessary throughout all phases of the project.

Throughout all phases of the MT PSM project, Team CNSI will continue to comply with all relevant DPHHS processes and protocols for maintaining project documentation. Scheduled documentation reviews and updates are planned in the Project Work Plan. When updates are made, the document owner checks out the deliverable from the project repository, makes the necessary revisions tracking the changes, and submits the document through the review and approval process. Upon DPHHS approval, Team CNSI accepts all the tracked changes and baselines the documents and also uploads a copy of the baselined document into CMS Reuse Repository.

DOC12

The Contractor shall provide and maintain an Operations, Maintenance and Configuration Plan for the Department's approval that describes post-implementation processes for areas such as:

a. Architecture/hosting operations.

b. Monitoring daily operations performance.

c. Performing routine maintenance.

d. Maintaining user documentation.

e. Online help approach and documentation, as appropriate.

f. Configuration and change management.

g. Approach to enhancements and other new requirements.

h. Maintaining system documentation.

i. Maintaining training documentation.

j. Archiving requirements.

k. Tasks, timelines, and responsible parties for design and configure/build tasks.

l. Reporting status against relevant Service Level Agreements (SLAs)

m. Schedule of major and minor releases.

The Department must review and approve all revisions of the Operations, Maintenance and Configuration Plan.

Used during our successful implementations in Michigan, Washington, Illinois, and Utah, Team CNSI's change management approach is proven and defines the process and procedures to effectively document and address change requests in collaboration with DPHHS throughout the project. Team CNSI's approach to change management is currently documented in our iVision360 framework, Configuration Management Plan, and Release Plan. Team CNSI will consolidate and tailor these documents into the Operations, Maintenance and Configuration Plan for the MT PSM project. We will work with DPHHS to review deliverable requirements and make recommendations for the deliverable based on providing evoBrix PMIS SaaS.

This deliverable will contain the following:

- Processes and procedures for monitoring daily operations performance
- Schedule and process for performing routine maintenance
- Process for maintaining user, system, and training documentation
- Activities planned to maintain online help, as appropriate
- Processes and procedures for configuration and change management in operations (post-deployment)
- Approach to documenting and prioritizing enhancements and other new requirements
- Process to archive implemented requirements
- Tasks, timelines, and responsible parties for design and configure/build tasks for operational releases
- Process for reporting status against relevant Service Level Agreements (SLAs)
- Schedule of major and minor releases in operations (post-deployment)

DOC13

The Contractor shall develop a Module Implementation Plan in conjunction with the State that describes, at a minimum:

a. The rollout approach, including phased implementation, if necessary.

b. Overall integration approach

c. Approach to continuous integration of other modules or data from other data providing entities.

d. The proposed implementation schedule.

e. The rollback strategy.

f. Communication and Contractor support procedures.

g. Contractor and State roles and responsibilities.

h. Operational Readiness Checklist(s) that defines, in advance, the go/no-go decision, and all aspects of Contractor, solution, and State readiness.

i. All critical tasks that are required for cutover.

j. Post cutover monitoring.

k. The onsite and offsite user support provided by the Contractor and State during the initial solution implementation.

l. Solution acceptance procedures.

m. Tools and processes to ensure overall quality.

n. Describe post implementation production deployment process and activities.

Using our proven framework tailored for the MS PSM implementation is much more efficient and reduces the risks associated with implementation of a system as complex as evoBrix. As a result, the MT PSM solution Implementation Plan is based on Team CNSI's highly successful implementation plans from our other MMIS implementations. These plans have been executed in multi-vendor, multi-agency implementations with great success.

Working with DPHHS, interface partners, and solution stakeholders, Team CNSI develops the Implementation Plan that includes roles and responsibilities, communication protocols, quality tools and processes, onsite and offsite implementation support, acceptance procedures, and post implementation monitoring processes and activities. A key component of the Implementation Plan is the 60 day and 30 day checklists. This identifies the critical tasks, task owners, and scheduled dates for the critical activities that support the implementation. The Implementation Plan also defines a final implementation calendar, production cutover checklists, and implementation readiness metrics, for use in the readiness assessment checkpoint meetings.

The checklists include the following items:

- Verification of user acceptance test (UAT) progress and objectives
- Confirmation of hardware and software installation for Production and DR sites
- Confirmation of network infrastructure and single sign on integration
- Confirmation of database setup and configuration
- Confirmation of hardware, software, and facility security procedures
- Execution of initial and final data conversion and population of the production environment
- Monitoring of training progress and confirmation of training completion
- Demonstration of backup and recovery features
- Monitoring staff readiness metrics
- Monitoring provider readiness metrics
- Monitoring organizational readiness metrics

Alongside the readiness checklists, Team CNSI includes detailed cutover tasks as part of the solution implementation and transition to operations plan. This plan detail provides information concerning when legacy systems and operations processes terminate and when corresponding processes in the new system begin. The cutover plan includes such things as porting scanning over from the old system to the new, processing the final enrollments in the old system, and starting application processing in the new system, with provider conversion occurring between those steps.

A sample table of contents from a prior implementation effort is included in Figure 3.10.7-8.

Table of Contents

Contents ..... **ii**
Tables ..... **iii**
Section 1 – Preface **1**
1.1 Purpose 1
1.2 Scope 1
1.3 Audience 1
1.4 Referenced Documents 1
Section 2 – Overview **2**
2.1 Background 2
Section 3 – Project Implementation Approach and Methodology **3**
3.1 General Approach 3
3.2 Collaborative Implementation Planning 3
Section 4 – Implementation Plan **4**
4.1 Roles and Responsibilities 4
4.2 Implementation Checklists 7
Section 5 – Contingency Planning **9**
Appendix A – Implementation Checklist **10**
Appendix B – Implementation Calendar **11**
Appendix C – Smoke Test Plan **12**
Appendix D – Glossary **13**
Appendix E – Acronym List **14**

MTPSM-3-209

Figure 3.10.7-8. Team CNSI's Sample Implementation Plan Outline. Team CNSI brings to Montana a proven implementation plan that will be tailored for the MT PSM deployment.

DOC14

The State defines System Design Document (SDD) as documentation that describes how the functional and nonfunctional requirements recorded in the Requirements Response Matrix transform into more technical system design specifications from which the system is configured and built. The SDD documents the high-level system design and the low-level detailed design specifications.

The SDD describes design goals and considerations, provides a high-level overview of the system architecture, and describes the data design associated with the system, as well as the human-machine interface and operational scenarios. The high-level system design is further decomposed into low-level detailed design specifications for each system component, including hardware, internal communications, software, system integrity controls, and external interfaces.

The SDD documents and tracks the necessary information required to effectively define architecture

and system design in order to give the development team guidance on the architecture of the system to be developed. Design documents are incrementally and iteratively updated during the system development life cycle and includes proprietary contractor material (this excludes proprietary information related to COTS products). Its intended audience is the project manager, project team, and development team. The Contractor shall provide and maintain system design documentation that includes at a minimum:

- A description of each component, their purpose, including basic functions and the business areas supported
- User stories/use cases
- User interface design
- Physical database design
- A module system diagram, including all components, identifying all business process diagrams, data flows, systems functions, and their associated data storage
- Configurations
- Job streams within each module, identifying programs, inputs and outputs, control, job stream flow, operating procedures, and error and recovery procedures.
- A network schematic showing all network components and technical security control
- Listing of the edits and audits applied to each input item and the corresponding error messages.
- Interface Control Documentation
- Narrative descriptions of each of the reports and an explanation of their use must be presented.
- Definition of all fields in reports, including a detailed explanation of all report item calculations.

Team CNSI's proposed PMIS solution is documented primarily in the form of DSDDs. These documents define the module components of the solution and will be provided during the MT PSM initiation phase. The DSDDs are organized into three parts to define the features and functions of each module. This organization is described in Figure 3.10.7-9.

DSDD Part	Description
Part 1 - Overview	Part 1 provides an overview of the functional module including: ■ A description of the business process and functions within the module ■ Module context diagram that shows the interactions between the module and other external system of modules ■ Design assumptions, constraints, and dependencies ■ User Interface model, including layouts for the following components ● Web page ● Dialog page ● Search page ● Detail page ● Screen ● Data models ● Report layouts ● Correspondence layouts
Part 2 - Use Cases	Part 2 consists of one or more logical group that define the module functionality and interfaces: ■ The functional use cases ■ Business rules ■ System and Error Messages ■ Special Design Constraints
Part 3 - Appendices	Part 3 consists of appendices with specific detailed design content, such as: ■ Definition of profiles or standard actors used in the use cases

DSDD Part	Description
	■ Medicaid Information Technology Architecture Business Architecture Traceability Matrix ■ Applicable edits or audits ■ Configuration values ■ Transaction mapping documents ■ Glossary and Acronym List

Figure 3.10.7-9. DSDD Part Contents. The DSDD content is logically organized to define the features and functions of the module.

In addition to the DSDD contents listed in Figure 3.10.7-9, the evoBrix PMIS comes with provider operations manual, detailed processes, interface documentation, logical database model, security assessments, and reports as part of the SaaS offering.

Team CNSI believes that the following deliverables included in the requirement should be reviewed and may not be applicable in part or as a whole to the SaaS solution being proposed:

- Physical database design
- A module system diagram, including all components, identifying all business process diagrams, data flows, systems functions, and their associated data storage
- A network schematic showing all network components

DOC15

The Contractor shall develop and maintain a Communication Plan. The purpose of the Communication Plan is to provide a description of the communication that will occur on the project and how it will be managed. This includes details about various types and means of communication, communication channels, communication flow within the organizational structure, escalation, guidelines for meetings, dissemination of knowledge, and communication effectiveness. The Communication Plan shall ensure that the communication approach addresses communication across multiple vendors. Effective communication is a key element for the success of the project.

Team CNSI's recommends the Communications Management Plan be a component of our comprehensive Project Management Plan. Used in multiple healthcare projects, including Washington, Michigan, Illinois, and Utah, the communication plan identifies stakeholder needs and plans the delivery of the right information at the right time to reduce project risk and support successful delivery.

Effective communication is the responsibility of every project stakeholder and team member. Every individual is responsible for receiving and understanding project assignments and for communicating the status of his or her work within the organizational hierarchy. Every team member is also responsible for executing his or her portion of the communications processes outlined in the Communications Management Plan, including reading and understanding information that is distributed and resolving any problems with its content.

One of the key outputs to help ensure effective communication is the communication matrices. These are used to clearly identify stakeholders, timelines, method, frequency, and guidelines for communication and escalation. Examples of a regular reporting matrix and a regular events matrix are provided as Figure 3.10.7-10 and Figure 3.10.7-11.

Event	Purpose	Stakeholder Roles	Content	Method	Timing/ Frequency	Chairperson Role
Project Weekly Status Meeting	Project meeting to discuss project progress, risks, issues, and changes	Account Manager Project Manager PMO Director	Review current project activities and newly escalated issues, risks, change requests, and action items	Recurring meeting	Weekly	PMO Director
Steering Committee Meeting	Program status meeting to discuss progress on project status and program level tasks and operational performance metrics when applicable	Steering Committee Members Account Manager PMO Director	Schedule performance, action items and decisions, planned activities, risks and mitigation plans, and issues and corrective actions	Recurring meeting	Monthly	PMO Director

Figure 3.10.7-10. Regularly Schedule Events Matrix Example. This matrix is used to manage Team CNSI's event communications among stakeholders.

Report	Purpose	Stakeholders	Content	Method	Timing/ Frequency	Role Responsible
Project Status	Informs management of project status	Management	Scheduled events, upcoming events, recent achieved and upcoming milestones, major decisions, risks, and issues	Microsoft Excel Report	Weekly	Project Manager
Operations Status	Informs management of operations status	Management	Provider and call center performance metrics, system performance metrics, and schedule outages	PDF report	Weekly	Operations Manager

Figure 3.10.7-11. Regularly Scheduled Reports Matrix Example. This matrix is used to manage Team CNSI's Report communications among stakeholders.

Team CNSI will seek the input of DPHHS to account for and support all communications needs of Montana and ensue all pertinent project information is communicated to the right people on the project at the right time.

DOC16

The Contractor shall develop and maintain a Quality Management Plan. The Quality Management Plan identifies the quality standards for the project and how quality standards are measured. It includes the process steps and quality tools that will be used (e.g., templates, standards, and checklists).

Team CNSI's Quality Management Plan (QMP) encompasses all projected phases, and each phase has a distinct approach for addressing quality planning, quality assurance, and quality control, as well as ensuring continual process improvement. Quality assessment during the Solution, Configure, and Implementation (SCI) phases of the project focus on quality of the deliverables supporting implementation of the MT PSM solution and compliance with the methodology. Quality assessment following solution implementation focuses on the delivery of services to meet the service levels agreement parameters.

Team CNSI's QMP is structured to include each phase of the MT PSM solution and includes process steps, tools, and checklist. CNSI discontinued the traditional Design, Develop, and Implement (DDI) approach with the first release of its SaaS modular solution for Medicaid and now employs the SCI delivery methodology to implement the cloud evoBrix solution for each Medicaid client. Using the SCI methodology, Team CNSI deploys the modular solution to meet Montana's services needs with less risk and within the overall project timeline. Stages within SCI are planning, solutioning, configuration, and implementation. Each stage is further divided into work packages. Each work package includes quality processes with the appropriate measures to ensure quality outcomes.

The QMP details the required quality assurance (QA) reviews. Team CNSI incorporates these activities as part of the project plan and schedule and conducts QA audits and reviews throughout the project to:

- Verify conformance to standards, procedures, and utilization of approved templates
- Identify and document nonconformance, as well as provide continuous feedback to project staff and management on the results of QA activities
- Ensure nonconformance issues are corrected and measures implemented to avoid a repeat of the same or related issue

The QMP identifies specific activities to conduct during the SCI Phase of the project. Figure 3.10.7-12 identifies the sections of our standard QMP. Team CNSI's quality team meets with the project management team to identify audits and reviews points applicable to the MT PSM project, which are then used to tailor a plan for review and approval by DPHHS.

Table of Contents

Preface 1
Purpose 1
Scope 1
Audience 1
Referenced Documents 2
Section 1 – Overview 3
Section 2 – PPQA Activities 4
Section 3 – Process Audit 5
Section 4 – Work Product Reviews 7
Section 5 – Establish Resources and Tools 8
Section 6 – Establish Estimates and Budget 9
Section 7 – Training and Orientation 10
Section 8 – Metrics and Continuous Process Improvement 11
Section 9 – Process and Product Quality Assurance Artifacts 12
Appendix A – As-One Access 13
Glossary 14
Acronyms 15

MTPSM-3-211

Figure 3.10.7-12.Team CNSI's QMP Table of Contents. We tailor the detail content within each section of the QMP to the needs of the MT PSM project.

DOC18

The Contractor shall develop and maintain a Change Management Plan. The Change Management Plan must include the following elements.

a. Tools to support change management

b. Change management process steps

c. Escalation process

d. Training

e. Roles and Responsibilities

Team CNSI's recommends that Change Management Plan be a component of our comprehensive Project Management Plan. Our change management approach proactively anticipates and manages changes

throughout the project. Used during our successful implementations in Michigan, Washington, Illinois, and Utah, Team CNSI's change management approach is proven and defines the process and procedures to effectively document and address change requests in collaboration with DPHHS.

Team CNSI's Change Management Plan defines the steps and overall roles and responsibilities for change management activities. Team CNSI has a robust change management process, training, and supporting change management plan template which includes:

- Detailed process and workflow steps
- Assessment and escalation criteria and processes
- Change request tools and templates

Team CNSI will tailor its Change Management Plan to conform to Montana's requirements.

DOC19

The Contractor shall provide and maintain Technical Documentation including written description of module component(s) design, function and architecture that will provide guidance to system developers. Additionally, the Contractor must include a detailed list of all environments, each environments' IT technologies including software, middleware, hardware, utility applications, development tools, testing tools, and provides detailed information on the programming languages and protocols used.

Team CNSI's proposed PMIS solution is documented primarily in the form of DSDDs. The DSDDs provide technical details of functionality and are used by Team CNSI's technical team to configure the solution. This documentation details by module the features and functions for each component. The content of the DSDD is described in Figure 3.10.7-13.

DSDD Part	Description
Part 1 - Overview	Part 1 provides an overview of the functional module including: ■ A description of the business process and functions within the module ■ Module context diagram that shows the interactions between the module and other external system of modules ■ Design assumptions, constraints, and dependencies ■ User Interface model, including layouts for the following components ● Web page ● Dialog page ● Search page ● Detail page ● Screen ● Data models ● Report layouts ● Correspondence layouts
Part 2 - Use Cases	Part 2 consists of one or more logical group that define the module functionality and interfaces: ■ The functional use cases ■ Business rules ■ System and Error Messages ■ Special Design Constraints
Part 3 - Appendices	Part 3 consists of appendices with specific detailed design content, such as: ■ Definition of profiles or standard actors used in the use cases ■ Medicaid Information Technology Architecture Business Architecture Traceability Matrix ■ Applicable edits or audits ■ Configuration values

DSDD Part	Description
	■ Transaction mapping documents ■ Glossary and Acronym List

Figure 3.10.7-13. DSDD Contents. The DSDD content is used by Team CNSI's technical team to configure the solution.

In addition to the DSDD, Team CNSI will provide:

- A detailed list of all environments
- IT technologies for each environment, including software, middleware, hardware, utility applications, development tools, and testing tools
- Detailed information on the programming languages and protocols used

Team CNSI believes that some elements of the technical deliverable requirements should be reviewed and may not be applicable to SaaS solution being proposed.

DOC21

The Contractor shall provide a Solution Architecture Document. The Solution Architecture Document includes a technical explanation of all aspects of the solution including detailed architectural diagrams, data flows, component specifications, SaaS, COTS products and hosting environment details. The document will include architectural tradeoffs using the Architecture Tradeoff Analysis Method (ATAM) method or other suitable method for evaluating the proposed platform architecture relative to the enterprise goals to identify risks that would inhibit the achievement of Agency's business goals.

Team CNSI maintains System Architectural Diagrams that define the evoBrix solution in architectural diagrams, which includes data flows and other platform and component details. As per the Project Work Plan, Team CNSI will consolidate these diagrams and create the Solution Architecture Document for DPHHS review. This deliverable will consist of the following:

- Architectural diagrams
- Data flows
- Components specifications
- SaaS
- COTS products and hosting environment details

In addition, Team CNSI will document any architectural tradeoffs using the Architecture Tradeoff Analysis Method (ATAM) method or other suitable method for evaluating the proposed platform architecture relative to the enterprise goals to identify risks that would inhibit the achievement of DPHHS business goals.

DOC22

The Contractor shall develop and maintain a Defect Management Plan that describes the process of submitting, monitoring and resolving defects. The plan will detail the following:

a. Approach and tools utilized to assign, identify, prioritize, track, resolve, and test system defects.

b. Approach to defect severity categorization using an industry standard methodology.

b. Approach to reporting and documenting defects.

c. Describe how the Contractor will work collaboratively with other State healthcare programs enterprise vendors.

d. Describe the defect management processes related to all test types and levels in the RFP (e.g., the relationship between defect resolution and the coordinated test case execution).

e. Describe the defect management processes after implementation.

Team CNSI offers a highly efficient, multi-layered, comprehensive test approach that minimizes risk to DPHHS. Through previous MMIS implementation experiences in Michigan, Washington, Illinois, and Utah, Team CNSI refined the test strategy we are offering for the MT PSM project. Team CNSI's Defect Management Plan, a component of our Master Test Plan, provides our approach and methodology to manage submit, monitor, and resolve defects. Sections within this plan that will be tailored for Montana include based up on the evoBrix SaaS solution offering:

- Defect Management Policies
- Defect Management Process Description
- Defect Metrics

The defect management plan section will describe the approach for entering, documenting, categorizing, tracking, assigning and collaborating with other organizations to resolve defects. Defect Management process during implementation and post implementation will be delineated in the plan document.

DOC24

The Contractor shall submit and maintain a Staffing Plan as part of the Project Management Plan. The Staffing Plan must include:

a. Identify the roles and responsibilities by resource type throughout all phases of the contract, including identifying key and non-key personnel as well as FTE allocation for all personnel.

b. Staffing Levels (estimated by resource type by phase for the duration of the project) to be reported in the Resource Allocation Matrix.

c. Detail how the staffing levels shall achieve consistent, dependable service regardless of changes that may influence work volume.

d. Detail differentiated by Proposer staff, subcontractor staff, if applicable, and State project staff.

e. Identify total hours to be expended, per phase or effort, and for the entire project, by Proposer staff and by State project staff.

f. Tools and processes used to screen available staff and fill positions.

g. Expectations regarding onsite time for contractor resources

h. Process for temporarily and permanently replacing vacancies in key personnel and other manager/lead positions consistent with staffing SLAs.

Well-managed project staff management establishes the foundation for successful project performance by providing the right organizational structure, team members, and processes to consistently deliver quality products. It is important that all parties work together to understand the roles and responsibilities of each position and leverage the staff management processes throughout the life of the project.

Team CNSI's Staff Management Plan is a component of the comprehensive Project Management plan and has been used for our successful implementations in Michigan, Washington, Illinois, and Utah. Early

in the project, Team CNSI will work with DPHHS to tailor the Staff Management Plan for the MT PSM project. Project-specific details include:

- Governance and escalation structures and processes
- Defined roles and responsibilities, including differentiating between CNSI, Noridian, and State staff
- Project-specific staff management tools and processes
- Project hours and staffing level expectations
- Resource utilization and metrics reporting
- Onsite and remote staff support
- Staff vacancy continency plans

Figure 3.10.7-14 outlines the sections of the Staff Management Plan that will be tailored for the MT PSM project.

Table of Contents

Preface **1**
Purpose 1
Document Scope and Organization 1
Audience 1
Referenced Documents 1
Section 1 – Staff Management Approach **3**
1.1 Staff Management Approach and Methodology 3
1.2 Organizational Structure 4
1.3 Staff Acquisition 4
1.4 Staff Change Control 4
1.5 Orientation and Training 5
Appendix A – Supplementary Staff Management Approach **6**
Appendix B – Glossary **7**
Appendix C – Acronyms **8**

MTPSM-3-213

Figure 3.10.7-14. Team CNSI's Staff Management Plan Table of Contents. We tailor the detail content within each section of the Staff Management Plan to the needs of the MT PSM project.

DOC26

The Contractor shall develop, submit and maintain a Master Test Plan that describes the Contractor's plan for all testing activities, processes, types and levels. Testing must be as automated and self-documenting as possible (e.g., continuous unit testing). At a minimum, the Master Test Plan must address the following:

a. Overall testing strategy for the following testing types: unit testing, system testing, integration testing, regressing testing, parallel testing, performance and load testing, manual and automated and/or scripted testing, disaster recovery and end-to-end integration testing of COTS products if any.

b. Approach to planning and preparing the test/staging environment

c. Approach to conducting each test level.

d. Approach for supporting UAT.

e. Approach for testing nonfunctional requirements.

f. Approach to test documentation (e.g., test cases, test scripts, test case matrices added as design progresses).

g. Approach to quality control/quality assurance.

h. Approach to bi-traceability to requirements and design.

i. Tools, techniques, and methods.

j. Reporting mechanisms, traceability and metrics.

k. Defects and defects resolution.

l. Entrance and exit criteria for each test level including alignment with industry standards.

m. Configuration management for each test level

n. Testing roles and responsibilities

o. Acceptance Criteria shall include but is not limited to; no high or critical defects in code released to production and production releases will not be promoted if more than 5% of requirements have an open defect

Team CNSI's Master Test Plan encompasses all activities necessary to ensure that the software products configured for MT PSM are compliant with the project's design specifications and that the solution functions effectively in the proposed infrastructure environment. This test plan has been successfully used for our Washington, Michigan, Illinois, and Utah projects and includes defining and establishing the required infrastructure for the testing, testing the solution and its interfaces, testing with the converted data, managing defect resolution processes, and supporting user acceptance testing.

Other key aspects of the Master Test Plan are:

- Definition of strategy for all test phases, including unit testing, system testing, integration testing, regression testing, parallel testing, performance and load testing, manual and automated testing, DR, and end-to-end testing
- Test environment readiness and preparation activities and coordination
- The definition of the entry and exit criteria for each phase of testing
- The approach for constructing and executing test cases for each test phase
- Approach for testing nonfunctional requirements
- Traceability of gaps to the test cases
- Defect reporting, management, and reporting
- Configuration management for testing phases
- Testing roles and responsibilities
- Acceptance criteria

Team CNSI will work with DPHHS to tailor the Master Test Plan for the MT PSM project. Figure 3.10.7-15 provides an outline of Team CNSI's test plan.

Table of Contents

Preface **1**
Purpose 1
Document Scope and Organization 1
Audience 2
Referenced Documents 2
Section 1 – Overview **3**
Section 2 – Test Approach **4**
2.1 High-Level Test Approach 4
2.2 Plan Execution – Roles and Responsibilities 6
2.3 System Test Phases 8
2.3.1 System Testing 8
2.4 Test Cases 10
2.4.1 Peer Review 14
2.5 System Test Data 14
2.6 Test Execution 14
2.7 Defect Management 15
2.7.1 Defect Management Policies 15
2.7.2 Defect Management Process Description 16
2.7.3 Defect Metrics 24
2.8 Test Data and Security 26
2.9 Test Tools 28
2.10 Test Environments 28
Section 3 – Test Management and Reporting **30**
3.1 Test Management Overview 30
3.2 Test Readiness Reviews 34
3.3 System Test Status Report 32
3.4 Defect Reporting 34
Section 4 – Test Schedule **35**
Section 5 – Issues and Risks **36**
Appendix A – Test Entry Checklist **37**
Appendix B – Test Exit Checklist **38**
Appendix C – Test Environment Software Components **39**
Appendix D – Verification Methods **40**
Appendix E – Validation Methods **42**
Appendix F – Environment Request Form **43**
Appendix G – Glossary **44**
Appendix H – Acronyms **45**

MTPSM-3-214

Figure 3.10.7-15. Team CNSI's Master Test Plan Outline. Team CNSI has an established test plan that will be tailored for the MT PSM project.

DOC27

The Contractor shall develop and submit a Training Plan that, at a minimum, addresses the following:

a. Summary of training approach that focuses on the train-the-trainer methodology, objectives, and desired outcomes.

b. Training needs analysis, including an assessment of the target audience and their knowledge and skills.

c. Recommendations on type and delivery approach based on training needs analysis.

d. Summary of proposed training materials and documentation in addition to hands-on training.

e. Approach to maintaining training documentation and accompanying materials.

f. Approach to providing training necessary to support new functionality and/or major software releases that materially change the user interaction.

g. Approach to processing for incorporating feedback to improve train the trainer effectiveness over the course of the Contract.

Team CNSI recognizes that effective implementation training for Team CNSI, DPHHS, vendors, and providers is critical to maximizing acceptance, satisfaction, and use of a new system. Team CNSI uses the industry-standard Analysis, Design, Development, Implementation, and Evaluation (ADDIE) method to guide collaboration in tailoring our solution training to DPHHS' needs by leveraging plans, tools, and approaches that have been used in previous implementations.

Team CNSI collaborates with DPHHS to analyze the full scope of training needs and configure the appropriate implementation training strategy. The result of this activity is the Training Plan. The Training Plan is submitted to DPHHS for review and approval and includes:

- Training strategy, including objectives and desired outcomes

- Training approach and methodology, including train-the-trainers
- Summary and recommendations from the training needs analysis
- Training calendar and curriculum
- Proposed training documentation and materials
- Planned training delivery mechanisms
- Process for evaluating training results
- Procedures to manage updates to the training content

An example of a Training Plan is outlined in Figure 3.10.7-16. The Training Plan will be created for MT PSM.

DPHHS Implementation Training Plan
Table of Contents

1. Overview
2. Plan Scope
3. References
4. Glossary
5. Training Plan Policies
6. General Training Approach and Processes (ADDIE)
6.1. Analysis
6.1.1. Learning Objectives
6.2. Design
6.3. Development
6.3.1. Training Materials Development, Review, and Approval
6.3.2. Training Materials Storage and Control
6.4. Implementation
6.4.1. Methods of Training
6.5. Evaluation
7. Training Tools
8. Implementation Phase Training
8.1. Purpose/Objectives
8.2. Roles and Responsibilities
8.3. Audiences
8.3.1. DPHHS Staff
8.3.2. Providers
8.3.3. Team CNSI Staff
8.4. Reporting
8.5. Class Descriptions (Appendix A.3)
8.6. Registration Procedures
8.7. Implementation Phase UAT Training Calendar
8.7.1. UAT Readiness Training (Appendix A.2)
Appendix A – Team CNSI Implementation Phase Training Materials
A.1 Implementation Phase Training Schedules
A.1.1 Team CNSI
A.1.2 DPHHS
A.1.3 Providers
A.2 Implementation Phase Module Listing
A.3 Implementation Phase Course Overviews
A.3.1 Description
A.3.2 Method of Delivery
A.3.3 Intended Audience
A.3.4 Student Level
A.3.5 Training Materials Used

MTPSM-3-215

Figure 3.10.7-16. Sample Training Plan. Team CNSI leverages existing content and collaborates with DPHHS to tailor the best training plan to fit Montana's needs.

DOC28

The Contractor shall develop in collaboration with the Department, a System Test Plan that describes the Contractor's System Testing approach and includes at a minimum the following:

a. Test Coverage

b. Walkthroughs and Inspections

c. Test Data Considerations

d. Entrance Criteria

e. Exit Criteria

f. Configuration Management

g. Testing Documentation

h. Process Steps

i. Inputs to System Testing

j. Outputs for System Testing

k. Metrics

l. Pass/Fail Criteria

m. Suspension Criteria and Resumption requirements

n. Testing Deliverables

o. Testing activities

p. Resources, Roles and responsibilities

q. Testing Tools

r. Meetings and Communication

s. Acceptance Criteria shall include but is not limited to; no high or critical defects in code released to production and production releases will not be promoted if more than 5% of requirements have an open defect.

Team CNSI's System Test Plan, a component of the Master Test Plan, provides our approach and methodology to plan and conduct system testing which will be tailored for the MT PSM project. The objective of the System Test system testing is to confirm the configured solution work as designed. Testing is done in a functional manner where the test scenarios and procedures are organized in a logical progression to perform typical operational and system end-to-end activities. This testing is designed to cover all typical system processes and functions, including:

- System test approach and coverage
- Planned walkthroughs and inspections
- Test data set-up requirements
- Entrance and exit criteria
- Test documentation and metrics reporting
- Configuration management
- Testing execution steps and processes
- Required inputs and outputs from the testing
- Criteria for determining test case pass and failure
- Suspension Criteria and Resumption requirements
- Testing deliverables
- Resources, roles, and responsibilities
- Testing tools and activities
- Planned meetings, status reporting, and metrics communication
- Test completion or acceptance criteria

Team CNSI acknowledges and accepts that the system test acceptance shall be having less than 5% of requirements with open defects.

DOC29

The Contractor shall provide during the initiation phase of the project and maintain throughout the project, system documentation that at a minimum includes:

- A description of each component, their purpose, including basic functions and the business areas supported
- User stories/use cases
- Screen layouts, report layouts, and other output definitions, including examples and content definitions
- Physical database design
- A module system diagram, including all components, identifying all business process diagrams, data flows, systems functions, and their associated data storage
- Configurations
- Job streams within each module, identifying programs, inputs and outputs, control, job stream flow, operating procedures, and error and recovery procedures.
- A network schematic showing all network components and technical security control
- Listing of the edits and audits applied to each input item and the corresponding error messages.
- As applicable, listing and description of all control reports
- Interface Control Documents
- Narrative descriptions of each of the reports and an explanation of their use must be presented.
- Definition of all fields in reports, including a detailed explanation of all report item calculations.
- Operations Procedure Manual
- Data Dictionary

Team CNSI's proposed PMIS solution is documented primarily in the form of DSDDs. These documents for the modules applicable for the MT PSM solution will be provided during the initiation phase. The DSDD are organized into three parts to define the features and functions of each module. This organization is described in Figure 3.10.7-17.

DSDD Part	Description
Part 1 - Overview	Part 1 provides an overview of the functional module including: ■ A description of the business process and functions within the module ■ Module context diagram that shows the interactions between the module and other external system of modules ■ Design assumptions, constraints, and dependencies ■ User Interface model, including layouts for the following components ● Web page ● Dialog page ● Search page ● Detail page ● Screen ● Data models ● Report layouts ● Correspondence layouts
Part 2 - Use Cases	Part 2 consists of one or more logical group that define the module functionality and interfaces: ■ The functional use cases ■ Business rules ■ System and Error Messages ■ Special Design Constraints
Part 3 - Appendices	Part 3 consists of appendices with specific detailed design content, such as: ■ Definition of profiles or standard actors used in the use cases ■ Medicaid Information Technology Architecture Business Architecture Traceability Matrix ■ Applicable edits or audits ■ Configuration values

DSDD Part	Description
	■ Transaction mapping documents ■ Glossary and Acronym List

Figure 3.10.7-17. DSDD Part Contents. The DSDD content is logically organized to define the features and functions of the module.

In addition to the DSDD, Team CNSI will submit documentation of the following for the MT PSM solution during the initiation.

- Logical database model
- Operations Procedure Manual
- Data Dictionary
- Configurations - understood to mean List of Configuration Items
- Technical Security Controls

Team CNSI believes that the following deliverables included in the requirement should be reviewed and may not be applicable in part or as a whole to the SaaS solution being proposed:

- Physical database design
- A module system diagram, including all components, identifying all business process diagrams, data flows, systems functions, and their associated data storage
- A network schematic showing all network components

DOC37

At least twelve (12) months before the start of the final Contract year (including option years that have been exercised) the Contractor shall provide, a Turnover Plan to the Department. The Plan will include:

a. Proposed approach to turnover.

b. Tasks and subtasks for turnover.

c. Schedule for turnover.

d. Updated operational tasks and procedures during turnover.

e. Description of vendor coordination activities that will occur during the turnover task and implementation of the activities to ensure continued system and services as deemed necessary by the Department.

f. List of incomplete tasks, such as system defects, modifications or enhancements, mass adjustments, reference updates, and configuration requests.

g. A detailed description of the services that would be required by another Contractor to fully take over system, technical, and business functions outlined in the Contract. The description shall also include an estimate of the number and type of personnel required to support the technical platform and supporting services.

h. The data and documentation shall be organized in a format required by the State (e.g., by provider unique ID and provider name).

Team CNSI will perform turnover activities with the same careful attention, planning, and execution that DPHHS will have come to expect based on our performance during implementation and throughout the solution operations. We fully support the DPHHS requirement to turn over systems and operations duties. Team CNSI's past turnover experience is an asset to DPHHS because we use the lessons learned from prior contract transitions, both as an incumbent and as a successor, to identify what worked, and to

modify or eliminate what did not. Our turnover activities "officially" begin at least six months before the start of the final contract year with the submission if the Turnover Plan. The Turnover Plan defines:

- The approach for the turnover
- Tasks and subtasks for the turnover
- Turnover schedule
- Updated operational tasks and procedures
- Vendor coordination activities for the turnover period
- Identification of all the in-progress or future-planned tasks, such as system modification, adjustments, and reference updates
- Definition of activities and services required for the takeover of the system, technical, and business functions
- Updated data and documentation in the format as required by DPHHS

The table of contacts of a proposed plan that will be tailored for the MNT PSM turnover is provided in Figure 3.10.7-18.

Table of Contents

Signature Page i
Table of Contents ii
Revision History iii
1. Turnover Plan Overview **1-1**
1.1 Plan Purpose and Scope 1-1
1.2 Document Structure 1-1
1.3 Audience and Intended Use 1-2
1.4 References and Standards 1-2
1.5 Abbreviations and Acronyms 1-3
2. Organization, Staffing, Roles, and Responsibilities **2-1**
3. Turnover Plan Details **3-1**
3.1 Turnover to Operations Management and Oversight 3-2
3.2 Entry Criteria 3-2
3.3 Turnover Planning 3-2
3.4 Contingency Planning 3-3
3.5 Operational Readiness Assessments 3-3
3.6 Outreach and Communication Approach 3-4
3.7 Operations Turnover 3-6
3.8 Quality Assurance Activities 3-6
3.9 Exit Criteria 3-7
4. Transition Tools and Methods/Technologies **4-1**
5. Supporting Material **5-1**
5.1 Communications 5-1
5.1.1 Documentation and Reporting 5-1
5.1.2 Coordinating with Stakeholders 5-1
5.2 Orientation and Training 5-1
5.3 Turnover Plan Change and Configuration Control 5-1
5.4 Records Management 5-1
5.5 Transition Process Evaluation 5-2
5.6 Turnover Plan Maintenance and Update 5-2

MTPSM-3-216

Figure 3.10.7-18. Team CNSI's Turnover Plan Table of Contents. Team CNSI's Turnover Plan provides a roadmap to transition system and business operations to the successor contractor.

DOC38

The Risk Management portion of the Project Management Plan must describe at a minimum:

a. Proactive identification and analysis of risks before they become issues.

b. Development of risk avoidance, transfer, mitigation or management strategies.

c. Approach to monitoring, communicating, reporting of risk status including procedures for documenting, resolving, and reporting issues and risks identified by the Contractor, the Department or other project contractors.

d. Approach to root cause analysis.

e. The appropriate methods, tools, and techniques for active and ongoing identification and assessment of project risks.

f. Describe how risks will be quantified and qualified.

Risk are inherent in any project and arise from uncertainty surrounding project decisions and outcomes. A risk refers to the potential for adverse outcome or loss. Risks may become an issue if not effectively mitigated. The goal of risk management is to proactively maximize the positive affects while minimizing the negative results associate with project risks. Team CNSI follows risk management practices throughout the project's lifecycle as defined in the Risk Management Plan, a component of the Project Management Plan. The Plan includes:

- Processes to proactively identify, document, analyze, and mitigate risks
- Risk avoidance, transfer, mitigation, and management strategies
- Roles and responsibilities for reporting and managing project risks
- Procedures to monitor, communication, and report risk status to DPHHS and other project stakeholders
- Process for conducting root cause analysis
- Tools, methods, and techniques used in risk management
- Risk evaluation and prioritization ratings and criteria

Early in the project, Team CNSI will work with DPHHS to tailor the Risk Management Plan for the MT PSM project.

DOC40

The Issues Management Plan portion of the Project Management Plan must describe at a minimum:

a. Approach to issue management.

b. Issue management process steps including:

-Approach to prioritizing, tracking, escalating, communicating, reporting issues

-Approach to documenting, reporting, and resolving issues identified by the Contractor, the Department or other module contractors.

-Approach to impact analysis.

c. Tools, and techniques for active and ongoing identification and monitoring of project issues.

d. Roles and responsibilities.

e. Describe how issues will be quantified and qualified

Any member of the project team is able to identify and report issues. However, it is not adequate to just identify issues. To effectively address the conditions and events that can have a negative impact on the project, there must be a process to analyze these identified issues and develop resolution plan. Therefore, Team CNSI has established processes to manage project issues. These are documented in the Issue Management Plan, a component of the Project Management Plan. The Issue Management Plan defines:

- The roles and responsibilities for issue management for the MT PSM project
- The approach and process steps for issue management activities
- Criteria and process to prioritize, track, escalate, communicate and report status of identified issues
- Tools and procedures to document, report, and resolve issues
- Strategy to conduct impact analysis of issues, including methods to quantify and qualify issue impact

Early in the project, Team CNSI will work with DPHHS to tailor the Issue Management Plan for the MT PSM project.

DOC41

The Contractor shall provide a Deliverable Expectations Document (DED) for each deliverable that describes the purpose, content, applicable MECT minimum required content and industry standards (e.g., PMI, IEEE/ISO, CMS XLC) that are satisfied for each Deliverable. Each DED is a deliverable.

Team CNSI acknowledges and accepts that a Deliverable Expectation Document (DED) is required for each formal deliverable. With successful long running implementations in multiple states, Team CNSI has proven templates and sample documents to leverage in setting the expectations of content and acceptance criteria for each formal deliverable prior to submission. In order to accommodate the rapid cycle time required to implement within a seven-month time period, CNSI proposes that our templates serve as the DED document themselves. These can then be delivered, reviewed, modified for SaaS considerations, and approved rapidly to allow the fast ramp-up time required by the timeline that has been requested.

DOC42

The Contractor shall develop a comprehensive Operations Procedure Manual which shall provide guidelines for the operation and use of the module and/or module component(s). At a minimum, the Operations Procedure Manual shall contain policies, processes and workflows for the module and/or module component(s).

Team CNSI will create an Operations Procedure Manual for the MT PSM solution. The Operations Procedure Manual will describe our ongoing support and operations procedures. Manual creation will be coordinated within the multi-vendor environment and will be formatted in the following structure:

- System Overview
  - Functional System Overview
    - Application and System Dependencies
  - Physical System Overview
    - Physical Architecture
    - System Software to Hardware Specification
    - Special Server Conditions
    - System Firewall Specification
  - System User Overview
    - Estimated Users
    - Peek Processing Time
    - Hours of Operation
    - User Impacts for System Failures
  - Processing Overview
    - Data Flow Diagram
    - Data Sources
    - Data Refresh/System Updates

  - Reporting Requirements
  - Service Level Agreements

- Security and Privacy Overview

- Roles and Responsibilities
- Operations Procedures
- Data and Database Administration Procedures
- Configuration Management Procedures

The Operations Procedure Manual will also provide the framework for production and support processes, define day-to-day support, and included detail procedures for items including:

- Identifying the root cause of corrupted data, identifying the fix, and repairing any corrupted data that is associated with a problem
- Providing the State with a copy of the routine planned maintenance schedule no less than 30 calendar days in advance of the scheduled maintenance date for approval (including the process for presentation to the State and receiving concurrence from the State) and the scheduling of the maintenance so as not to disrupt the negotiated operational hours
- Developing an automated process for purging production Software as a Service (SaaS) platform files as determined by data governance decisions
- Include administration procedures and describe the scheduled operations of the production system, including specific instructions on things an operator needs to do to manage the system daily
- Descriptions of administrative tasks
- Instructions on how to run interface and database (DB) jobs
- What to do in abnormal situations; for example, an interface job failure or a system restart due to hung treads
- System documentation will also detail the following:

  - Operations procedures, including batch or background process schedules, dependencies, sequencing, and timing
  - Administrative tasks, including user administration, system security administration, reference data maintenance, creation of report templates, and maintenance of service provider data and contracts
  - Other reference materials and presentations required to supplement the training and support activities
  - A High Availability and DR Plan for the entire evoBrix solution driven by the State's Recovery Time Objectives
  - Application validation procedures
  - Server startup and shutdown procedures
  - Build documentation

DOC44

The Contractor shall maintain Attachment L- Technology Matrix, and deliver annually for the Department for review.

Team CNSI acknowledges and accepts the responsibility to maintain Attachment L - Technology Matrix. Team CNSI will update the document annually and deliver it to DPHHS for review.

3.10.8 Performance Standards

Performance standards for phases of the project are defined in Attachment F – Requirements Matrix. Performance standards as well as associated liquidated damages for unmet standards are also defined in Attachment J, Service Level Agreement Requirements. The Offeror must describe their approach to meet the Performance Standards requirements defined in Attachment F, Requirements Matrix and Attachment J, Service Level Agreements.

Team CNSI is committed to providing quality performance, ensuring DPHHS service level agreements (SLAs) are met. Our team brings a management strategy to align with DPHHS objectives and to consistently deliver our services. Team CNSI's methodology ensures streamlined and standardized methods for maintaining performance compliance. Our staff collaboratively works with the state throughout all phases of the project for transparency, accountability, and efficiency to ensure Team CNSI performance standards consistently exceed compliance with service level agreements.

The Team CNSI Advantage

Team CNSI's strategy ensures streamlined and standardized methods for maintaining performance compliance, while collaboratively working with DPHHS throughout all phases of the project. Team CNSI brings:

- Mature Quality Assurance processes for achieving excellence in service delivery
- High Availability infrastructure for maximum uptime
- Multi-tier mature operations support processes and organization
- Extensive automation of system processes
- Robust tools for managing operations and operational reporting

MTPSM-3-331

Highlights of our SLA compliance strategy include:

- **Commitment to Excellence.** Team CNSI brings a comprehensive set of practices, policies, procedures, and processes that will enable us to focus on business value by providing consistent, predictable, and measurable results.
  - Extensive project and quality management plans for accurate and timely deliverables
  - Innovative tools for managing, tracking, and reporting service level agreements electronically
  - Comprehensive business continuity and disaster recovery plans to ensure high availability
- **Quality Management**. Team CNSI has an extensive library of process assets, procedures, best practices, and templates to implement our operations management strategy and subsequent processes. Our Project Management team is staffed with years of proven experience in delivering quality and accuracy with iVision360. In addition, our SDLC model has recently underwent CMMI for Development, V1.3 assessment, and was assessed as Level 3 compliant. Team CNSI continually measures business processes and records, normalizes, and analyzes metrics data to provide insight into our performance. Our experience allows us to create internal metrics to support SLA timeframes.
- **High Availability and Disaster Recovery.** Team CNSI's evoBrix PMIS solution architecture, process redundancies, and maintenance procedures provide stability to DPHHS. Our business continuity and disaster recovery plan ensures Team CNSI's solution and services remain above 99.5% availability rate. We continually review business process availability requirements and aligns them with our ITIL framework. This ensures that cost-effective contingency plans are in place and tested on a regular basis to ensure that the business needs of DPHHS are met. Team CNSI's Availability Management plan includes but is not limited to the following aspects:
  - Designing high-availability, redundant systems to support mission-critical applications
  - Utilizing state of the art technology for Disaster Recovery operations
  - Testing system availability to meet all MPATH SLAs

- Monitoring and reporting high-availability to ensure that SLAs are being met

- **Proactive Support System.** Team CNSI's support staff utilizes a configurable set of tools (e.g., HealthBeat, SLA Dashboard, Seibel CRM, Automation Oracle Enterprise Manager, Building Management System, and Data Center Infrastructure Management) to monitor the system and assist in the day-to-day operations activities to meet SLAs. Our quality support service provides transparency in reporting, fulfilling user requests, resolving service failures, fixing problems, and carrying out routine operational tasks. Team CNSI's support structure consists of the following areas to ensure quality and proactive support is provided to DPHHS.

  - Project Teams
  - Call Center
  - Help Desk/Operations Support
  - Infrastructure

- **Innovative Solutions.** Team CNSI establishes solutions in all areas and phases of implementation of the evoBrix solution for measurable performance standards. Our performance strategy is also about monitoring performance measures with our SLA Automation tool and reporting dashboard, HealthBeat, in addition to other operations monitoring tools and reports. Focusing on metrics enables Team CNSI to make data-driven decisions and be *accountable* for our performance.

The following sections outline our strategy for monitoring and managing key categories of SLA compliance**.**

SLA Tracking and Reporting

Team CNSI's reporting solution contains several management and operational reports that are scheduled to run from the Online Transaction Processing System (OLTP) on a daily, weekly, monthly, or quarterly basis, as per business requirements. These reports will be made available through IBM Cognos BI Connection Portal for viewing and retrieval. The report outputs are archived and integrated into IBM Cognos BI Content Store and could be retained according to pre-defined retention policies. The daily and weekly reports, though they vary according to business requirements, are scheduled within the same day or the next business day of the reporting period and are expected to complete the same day. All monthly reports are scheduled to execute within the first business day following the reporting period and are expected to complete the same day. All quarterly reports are scheduled to execute within the first two business days following the reporting period and are expected to complete the same day.

Service Level Agreement (SLA) Automation Tool

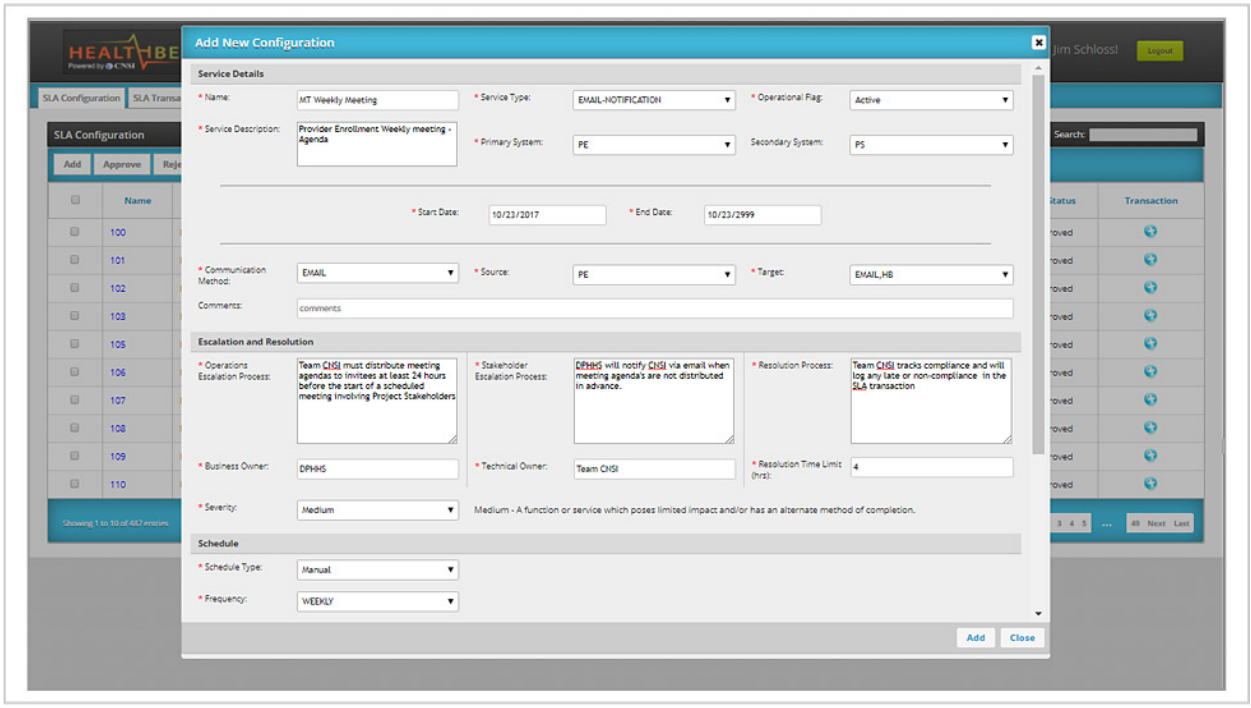
Team CNSI's SLA automation solution provides DPHHS with configurable SLA management capabilities. It is one of the tools that allow Team CNSI and DPHHS to track and ensure that SLAs are being met as defined in Attachment J - Service Level Agreements (SLA) of the Solicitation. Figure 3.10.8-1 shows the SLA automation tool architecture. Our solution uses an SLA Automation Engine which is configured to automatically or manually track various SLAs related to system and business functions, such as interfaces and report generations.

Our solution allows Team CNSI and DPHHS to have visibility of daily system and business functions and their corresponding SLAs performances. The tool is also equipped with tracking, reporting, and management capabilities using Team CNSI's HealthBeat as the front-end application. For example, the tool allows Team CNSI to measure SLAs on interface processing or ticket resolution statistics. This

allows Team CNSI the necessary visibility to monitor performance and provide SLA course correction when necessary.



The SLA Automation tool is integrated with HealthBeat, with the service configurations and transactions are accessible via HealthBeat's front-end. Each SLA Configuration is individually configured and managed, as shown below in Figure 3.10.8-2. SLA transactions are pre-populated for future records, up to 30 days. This allows Team CNSI and DPHHS the ability to see what automatic and manual SLAs are coming up to proactively respond, ensuring SLA compliance is met.

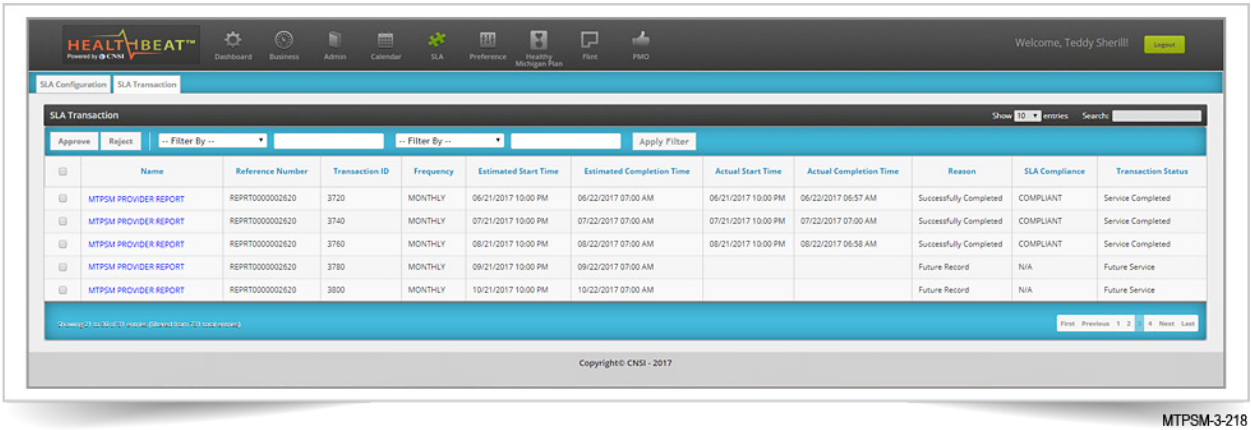


MTPSM-3-422

Figure 3.10.8-2. SLA Configuration Screen. The SLA Configuration Screen allows Team CNSI to manage service level agreements individually.

The SLA Automation engine runs on a configurable interval to generate service transactions based on the unlimited number of configured SLA's frequency schedules. The system retrieves data input from various source systems via REST or SOAP web service requests for multiple service configurations at any given time. The retrieved data – such as process start/end times and status codes – is matched to the SLA transaction based on unique criteria linked with the reference number, and automatically updated with the provided data. In the event of a non-compliant transaction, notification alert emails are generated and sent to email addresses linked to that service configuration.

Figure 3.10.8-3 shows the HealthBeat SLA history view.



MTPSM-3-218

Figure 3.10.8-3. SLA History View in HealthBeat. HealthBeat provides SLA configuration, management, and monitoring capabilities for transparency of operations.

HealthBeat comes pre-configured with most of the SLAs identified in the Solicitation that can be automated. Some SLAs by their nature are not candidates for real-time monitoring (i.e., deliverable submissions). The SLA Automation tool tracks all automatic and manually processed SLAs based on the agreement with DPHHS.

HealthBeat Reporting Dashboard

Indicative of Team CNSI's commitment to service and transparency, HealthBeat provides DPHHS with configurable, automated, and real-time visibility into business operations, SLA compliance, and system monitoring.

HealthBeat enables the setup of a hierarchy of MITA business, system, and application objectives or goals that can be linked with metrics to events and services. This will allow Team CNSI and the states using evoBrix to monitor the health of business and system processes not only in the short term but also over the long term to track historical trends. Such an approach allows Team CNSI to use real-life data in the business process configuration and ensures continuous business process improvement across all business process areas.

Currently, HealthBeat contains over 130 metrics and is continuously evolving to provide meaningful metrics to business operations users.

Proactively monitoring the health of operations enables Team CNSI to be more predictive, rather than reactive, in the provision of our services. However, it is essential that up-to-date metrics be available to provide us with the visibility needed for conducting this proactive monitoring. Team CNSI uses our HealthBeat solution as the operations dashboard to monitor business processes and system performance. Supporting performance measures that are aligned to MITA business processes, HealthBeat is in production in the states of Michigan, Utah, and Washington. In addition, the Centers for Medicare & Medicaid Services (CMS) has implemented HealthBeat to monitor operational data related to their interaction with insurers on health exchanges. HealthBeat is pre-packaged with over 130 metrics, including SLAs, available for DPHHS to select the metrics that apply.

As described in HealthBeat Reporting Dashboard, HealthBeat is central to our commitment to collaboration, transparency, and accountability. Developed by CNSI as our operations dashboard, HealthBeat provides optimized, configurable, automated, and near real-time visibility into business operations through well thought-out and presented dashboards organized by business area. HealthBeat provides aggregation, analysis, and ongoing performance monitoring data to stakeholders in the form of interactive scorecards, dashboards, and drill-down functionality. As part of our transparency strategy, we provide DPHHS access to the operational performance data that is also monitored by our staff. This approach will enable DPHHS to have near real-time visibility into SLA performance and other key metrics. HealthBeat is a web-based, mobile friendly application that will be integrated with SSO.

Traditional operations dashboards are snapshots of a point in time and focus solely on history. HealthBeat goes beyond this limitation and provides the capability to highlight trends and support forecasting, enabling Team CNSI to shift thinking from "what has happened" to "what could happen" – proactive versus reactive. Figure 3.10.8-4 provides one of the main HealthBeat views.



MTPSM-3-353

Figure 3.10.8-4. HealthBeat Dashboard. HealthBeat's interactive kiosk mode provides a display with rotating chart capabilities.

One of the features of HealthBeat is the ability to operate in a kiosk mode, which enables executives and managers to view operational performance in near-real time. MT PSM solution stakeholders will be able to monitor data trends and view early warning signals using thresholds and longer-term trends that employ historical data analysis and rule-based correlation techniques. HealthBeat is configurable and supports the addition of new metrics as needed to monitor business processes. It is pre-configured to support all MITA business processes and system operations. Team CNSI will configure HealthBeat to support the operations services required as part of our MT PSM solution.

HealthBeat provides a comprehensive application activity monitoring framework along with the capability to facilitate continuous process improvement. As the system handles each process, it collects process-related data in the data store. This data is then used to display the process dashboard and provide visibility to the process metrics and the health of the operation. The system uses workflow-based analytics to provide feedback on potential bottlenecks and application performance issues. Thresholds are configured to display performance in the traditional "red," "yellow," and "green" dashboard status. Team CNSI operations staff sets appropriate thresholds during service design. Thresholds that have DPHHS visibility will be reviewed with DPHHS to meet our commitment for transparency.

Related to system monitoring, HealthBeat reports accurate data on items such as end-user response time, CPU utilization, and hourly load averages on different servers. This allows the DPHHS and Team CNSI to see the system from a higher point of view and help make informed, strategic decisions on daily operations or future changes in policy and programs. Application management and monitoring, web services management, systems management and monitoring, network management and monitoring, performance monitoring, and event monitoring are all managed via the framework of HealthBeat.

HealthBeat also provides various reporting mechanisms, including dashboards and graphs, which can be used to report on the metrics associated with performance standards. Team CNSI uses the HealthBeat tool to collect and report on final performance measures and standards. HealthBeat uses automation to extract, analyze, and report data from various business processes and systems, and to provide a centralized reporting database. This tool provides a robust interface to the various MT PSM components for

gathering and compiling data, allowing near-real-time access to workload and system performance information.

Operational management staff regularly monitor data displayed through the dashboard and can proactively respond if performance indicators begin to decline. In this way, Team CNSI can implement corrective actions before a “red flag” situation occurs. In addition, email alerts are established to notify appropriate Team CNSI and State staff based on configured exception thresholds. Team CNSI also compiles information collected through HealthBeat and summarizes it in our regular reporting mechanisms, including statuses and required workload reports.

The tool produces visualizations of data in various formats, including dashboards and graphs that provide quick summaries for trending. Figure 3.10.8-5 shows the HealthBeat architecture that is configurable and automated.



Monitoring evoBrix

The purpose of Team CNSI's comprehensive monitoring approach during the post-implementation period is not only to perform quality control, but also to provide feedback for process improvement. Team CNSI's monitoring approach includes three tiers:

- Team CNSI NOC non-stop system monitoring on a 24x7x365 basis
- Application software engineers monitoring
- Business area monitoring

Because new data comes into the system through the eligibility and external financials systems, it is likely that there are error exceptions that need special resolutions. Additional monitoring by staff helps intervene and move the process along, saving valuable time.

In addition to monitoring system performance and processes, we also monitor application throughputs to identify areas of improvement, either from the system or process perspective. By analyzing the throughputs and backlog, we can make changes to the system when needed to remedy performance deficiencies. We are also able to make improvements to the application processes or provide feedback to providers regarding claims submission, resulting in improved performance of the system and associated business processes.

During the pre-deployment phase, Team CNSI will identify operational performance measures and the associated reports that generate or contain data relevant to system and operational performance to be monitored and reported through the evoBrix HealthBeat performance tool. Team CNSI's NOC is responsible for generating system and workload reports.

Call Center Reporting

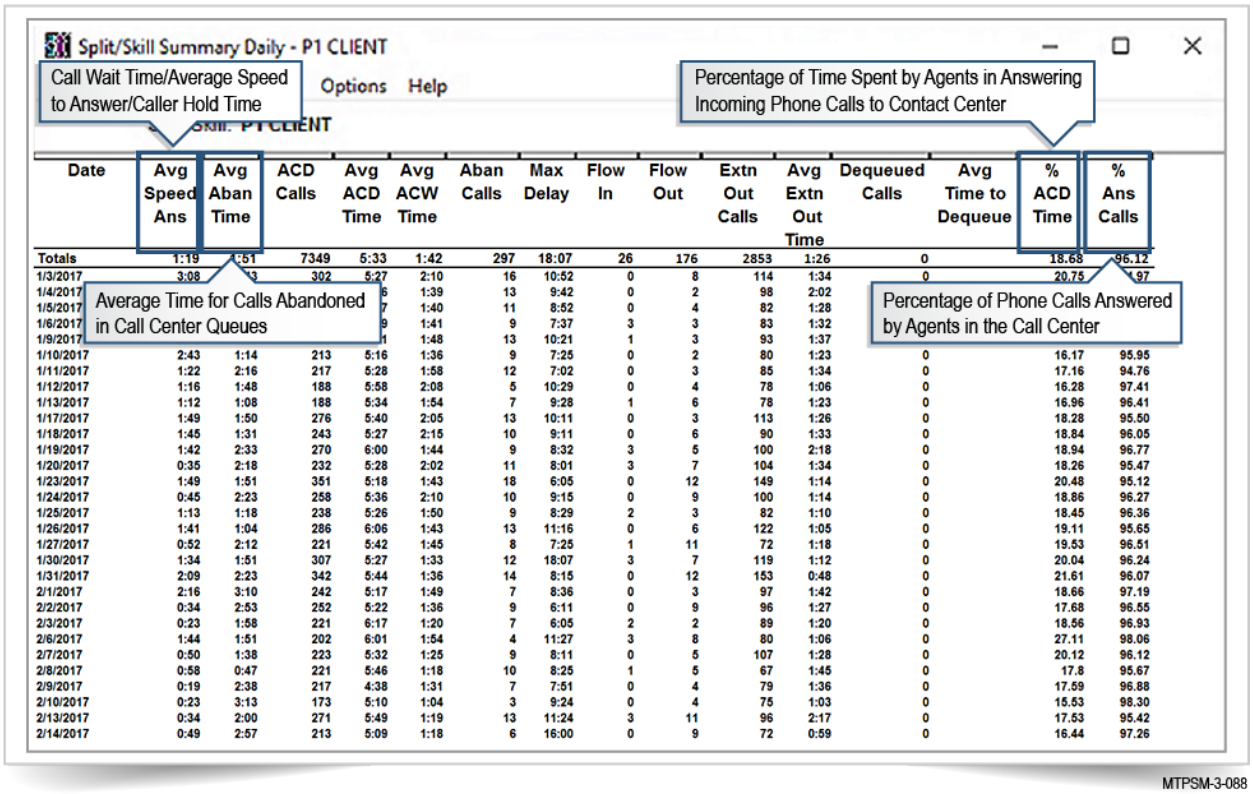
Team CNSI's Avaya solution supports interactive logging of all transactions and comprehensive ability to report call statistics. The reports available can broadly be categorized into two types, as described in Figure 3.10.8-6. The listed reports provide a 360-degree view of the Call Center performance. Additional reports can be configured as per the State's need during solutioning session.

Report Type	Description	Report Names
Avaya CMS/Call Center Reports	Provide details on the overall functioning of the call center. Avaya CMS reports can be real-time reports, historical reports or integrated (combination or real time and historical) reports. Additional reports can be configured as defined during solutioning activities.	■ Skill Status Report ■ Agent Group Report ■ Daily Summary Report ■ Agent Graphical Information Report ■ Skill Comparison Report
Avaya Aura Experience portal / IVR Reports	Provide details on all the transactions that is performed during the IVR calls and overall performance of the IVR systems. These reports can be generated on a pre-defined schedule or on demand.	■ Application Summary Report ■ Application Detail Report ■ Call Summary Report ■ Call Detail Report ■ Session Detail Report ■ Performance Report ■ Active IVR Calls Report ■ System Monitor Report

Figure 3.10.8-6. Call Center Reports. Lists various report available in Team CNSI's IVR and Call Center Solution.

CMS reports provide in depth details about the Call Center performance. These reports can be used to find the call abandonment rate, average time prior to abandonment, calls placed on hold along, with other details such as percentage of calls answered within set service levels, how many calls were handled, and summarizing activity. Reports can be obtained for a single skill or multiple skill. Reports can be also be obtained for any time frames like hourly, daily or any other time frames.

Figure 3.10.8-7 shows daily the summary report for a single skill over a 30-day period, which provides information on call abandonment rate and average time prior to abandonment, including for calls placed on hold.



Date	Avg Speed Ans	Avg Aban Time	ACD Calls	Avg ACD Time	Avg ACW Time	Aban Calls	Max Delay	Flow In	Flow Out	Extn Out Calls	Avg Extn Out Time	Dequeued Calls	Avg Time to Dequeue	% ACD Time	% Ans Calls
Totals	1:19	1:51	7349	5:33	1:42	297	18:07	26	176	2853	1:26	0		18.68	96.12
1/3/2017	3:08	[illegible]	302	5:27	2:10	16	10:52	0	8	114	1:34	0		20.75	[illegible]97
1/4/2017	[illegible]	[illegible]	[illegible]	[illegible]	1:39	13	9:42	0	2	98	2:02	[illegible]		[illegible]	[illegible]
1/5/2017	[illegible]	[illegible]	[illegible]7	[illegible]	1:40	11	8:52	0	4	82	1:28	[illegible]		[illegible]	[illegible]
1/6/2017	[illegible]	[illegible]	[illegible]9	[illegible]	1:41	9	7:37	3	3	83	1:32	[illegible]		[illegible]	[illegible]
1/9/2017	[illegible]	[illegible]	[illegible]1	[illegible]	1:48	13	10:21	1	3	93	1:37	[illegible]		[illegible]	[illegible]
1/10/2017	2:43	1:14	213	5:16	1:36	9	7:25	0	2	80	1:23	0		16.17	95.95
1/11/2017	1:22	2:16	217	5:28	1:58	12	7:02	0	3	85	1:34	0		17.16	94.76
1/12/2017	1:16	1:48	188	5:58	2:08	5	10:29	0	4	78	1:06	0		16.28	97.41
1/13/2017	1:12	1:08	188	5:34	1:54	7	9:28	1	6	78	1:23	0		16.96	96.41
1/17/2017	1:49	1:50	276	5:40	2:05	13	10:11	0	3	113	1:26	0		18.28	95.50
1/18/2017	1:45	1:31	243	5:27	2:15	10	9:11	0	6	90	1:33	0		18.84	96.05
1/19/2017	1:42	2:33	270	6:00	1:44	9	8:32	3	5	100	2:18	0		18.94	96.77
1/20/2017	0:35	2:18	232	5:28	2:02	11	8:01	3	7	104	1:34	0		18.26	95.47
1/23/2017	1:49	1:51	351	5:18	1:43	18	6:05	0	12	149	1:14	0		20.48	95.12
1/24/2017	0:45	2:23	258	5:36	2:10	10	9:15	0	9	100	1:14	0		18.86	96.27
1/25/2017	1:13	1:18	238	5:26	1:50	9	8:29	2	3	82	1:10	0		18.45	96.36
1/26/2017	1:41	1:04	286	6:06	1:43	13	11:16	0	6	122	1:05	0		19.11	95.65
1/27/2017	0:52	2:12	221	5:42	1:45	8	7:25	1	11	72	1:18	0		19.53	96.51
1/30/2017	1:34	1:51	307	5:27	1:33	12	18:07	3	7	119	1:12	0		20.04	96.24
1/31/2017	2:09	2:23	342	5:44	1:36	14	8:15	0	12	153	0:48	0		21.61	96.07
2/1/2017	2:16	3:10	242	5:17	1:49	7	8:36	0	3	97	1:42	0		18.66	97.19
2/2/2017	0:34	2:53	252	5:22	1:36	9	6:11	0	9	96	1:27	0		17.68	96.55
2/3/2017	0:23	1:58	221	6:17	1:20	7	6:05	2	2	89	1:20	0		18.56	96.93
2/6/2017	1:44	1:51	202	6:01	1:54	4	11:27	3	8	80	1:06	0		27.11	98.06
2/7/2017	0:50	1:38	223	5:32	1:25	9	8:11	0	5	107	1:28	0		20.12	96.12
2/8/2017	0:58	0:47	221	5:46	1:18	10	8:25	1	5	67	1:45	0		17.8	95.67
2/9/2017	0:19	2:38	217	4:38	1:31	7	7:51	0	4	79	1:36	0		17.59	96.88
2/10/2017	0:23	3:13	173	5:10	1:04	3	9:24	0	4	75	1:03	0		15.53	98.30
2/13/2017	0:34	2:00	271	5:49	1:19	13	11:24	3	11	96	2:17	0		17.53	95.42
2/14/2017	0:49	2:57	213	5:09	1:18	6	16:00	0	9	72	0:59	0		16.44	97.26

Figure 3.10.8-7. Daily Summary Report. Overview of a daily summary report for several days in a specific skill in Call Center.

Team CNSI's performance standards are measured throughout each phase of implementation utilizing our innovative solutions listed below and outlined in the sections below:

- Project Management
- Incident and Change Management
- System Availability
- Disaster Recovery
- Solution Architecture
- Data Management
- Provider Support

Project Management

Team CNSI's project management approach has the central theme of collaborative and transparent delivery. Engaging DPHHS and MT PSM stakeholder involvement is key to our approach. In every phase of the project, and we strive to involve stakeholders in a meaningful manner.

Team CNSI brings highly structured iVision360 software development lifecycle project management methodology to Montana, based on the PMI PMBOK and the SEI CMMI framework. This proven approach to deliverable review and management helps reduce the overall risk to the State, provides high-quality results on schedule, and ensures compliance with the requirements stated in the Montana Program for Automating and Transforming HealthCare (MPATH) Documentation Standards, in addition to compliance with service level agreements.

Team CNSI's standard Project Work Plan (PWP) contains a high-level Gantt chart showing major phase and activity start- and end-dates which will be aligned to the scope of work outlined in this RFP. Our standard PWP contains the detailed project work breakdown structure (WBS) and detailed schedule to ensure Acceptance of each Deliverable is met per the outlined due dates. Refer to Section 3.10.2.1, Project Management, for PWP details.

Team CNSI's extensive deliverable review process, using iVision360 methodology, coupled with our Quality Management Plan (QMP) ensures consistency, accuracy, and satisfies the acceptance criteria. Once the initial draft of any deliverable is produced, the following series of steps are taken prior to submission to DPHHS ensuring deliverables do not exceed two submissions to gain acceptance (steps are defined in Section 3.10.37, Project Deliverables and Documentation):

- Conduct Internal Review
- Produce Next Draft
- Technical Writing Review
- Quality Assurance Review
- Delivery to DPHHS
- DPHHS Initial Review
- Produce the Final Draft

Our Quality Management Plan includes process evaluation and improvement guidelines applicable to evaluating and improving document management processes and outputs.

The iVision360 framework includes a deliverable management process that leverages progressive review steps, as shown in Figure 3.10.8-8.

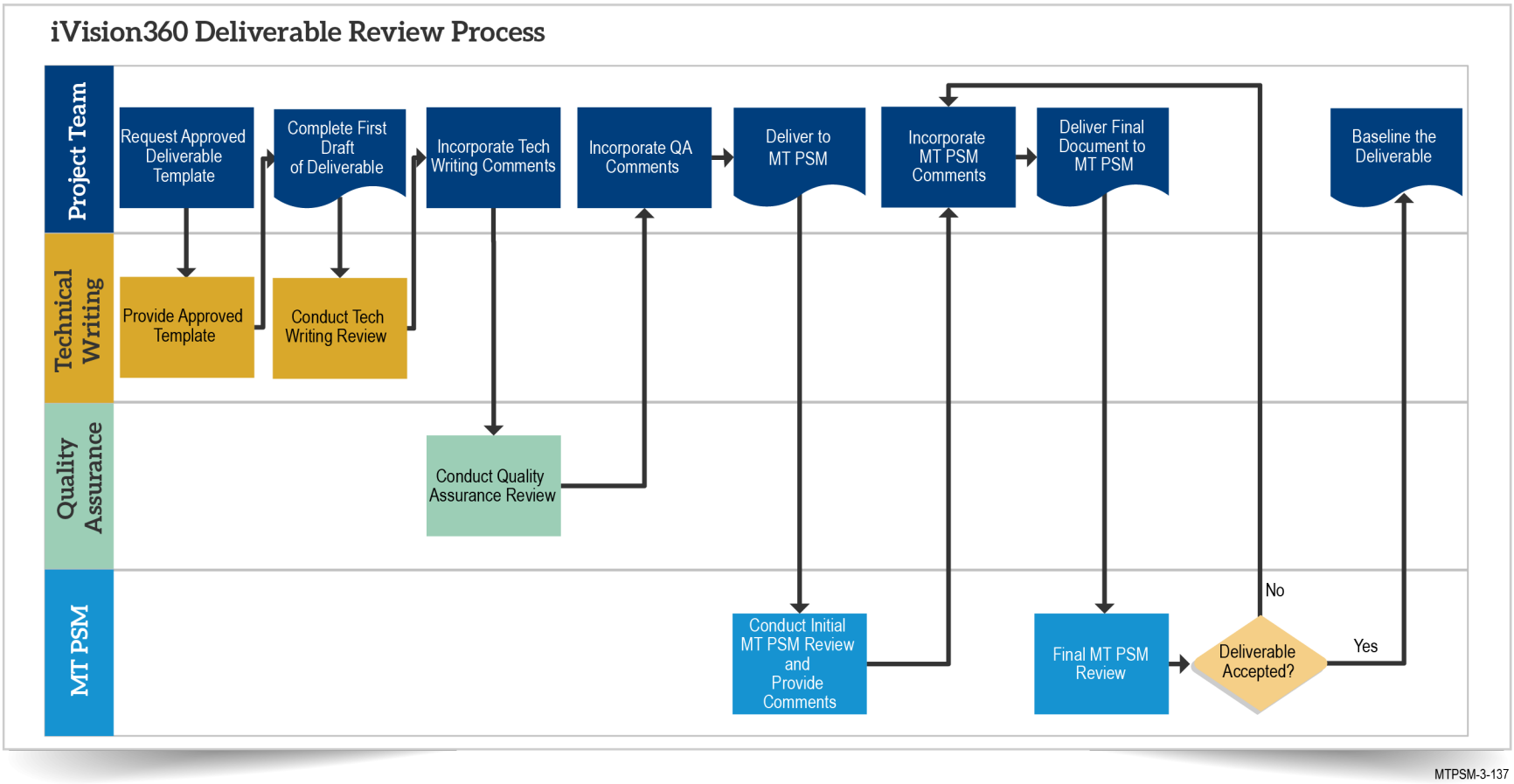


Figure 3.10.8-8. The iVision360 Deliverable Management Process. Integrating progressive review steps through the delivery process has been proven to increase the rate of initial acceptance of a deliverable.

Team CNSI's proposed PMIS solution is documented primarily in the form of Detailed Design System Design Documents (DSDD). The DSDD provides functional details on the user interface. Team CNSI will leverage this document and create the User Interface Style Guide for the MT PSM project. Any changes/updates to the functional documentation are completed within 10 days of implementing the change.

The evoBrix PMIS solution is designed to comply with state and federal policies, laws, statutes and guidelines. The system enforces these as business rules. The DSDD outlines these business rules and the functionality of the system will be in accord with the business rules. Team CNSI produces and delivers evoBrix Base DSDD. This allows the State the ability to cross-reference the regulations to the DSDD document which contains these rules for the policies and guidelines.

Team CNSI follows standardized processes to ensure that all tickets are prioritized and responded to accordingly. Team CNSI will complete and implement 100% of all critical priority tickets by the required implementation date outlined in the RFP.

Our change management process, as outlined in section 3.10.2.1, Project Management, includes methods for communicating, evaluating, and approving or rejecting changes throughout the project. This process ensures that proposed changes, submitted via Jira defect tracking system, are evaluated for impact to system, schedule, scope, cost, and resources. This facilitates informed decision-making by all parties involved in the change.

Team CNSI's follows the change management plan processes. Jira ticket priority levels are identified as shown in Figure 3.10.8-9.

Priority Level	Resolution Time Limit (RTL)
Critical	100 percent of tickets will be resolved and implemented by the defined implementation date
High	80 percent of tickets will be resolved and implemented by the defined implementation date 100 percent of tickets will be resolved and implemented by within five business days after the defined implementation date
Medium	75 percent of tickets will be resolved and implemented by the defined implementation date 100 percent of tickets will be resolved and implemented by within ten business days after the defined implementation date

Figure 3.10.8-9. Ticket Resolution and Implementation Times by Priority. Team CNSI's Help Desk process meets or exceeds SLA requirements.

Incident and Change Management

Team CNSI defines an incident/problem as any anomaly in the operational or technical environment that affects delivery of services. When a problem occurs:

- Team CNSI's operations management is notified.
- Team CNSI Help Desk is notified of the issue and impact to services. The Help Desk opens an incident ticket using OTRS.
    - The ticket describes the event and the module or operational area affected by the issue
    - The Help Desk assigns the Priority Level (i.e., Urgent, High, Normal, or Low) and enters pertinent information
    - Help Desk notifies the appropriate response team
    - Help Desk notifies account management of the issue and the assigned response team

- Team CNSI assembles the appropriate personnel to conduct an analysis of the issue and define an action plan to resolve the issue depending upon the severity level of the issue.
- Once the appropriate course of action is determined, Team CNSI opens a Jira ticket for internal tracking purposes.
- Team CNSI assigns the appropriate personnel to conduct its own detailed internal review and obtain the appropriate approvals to commence the resolution. In this meeting, a discussion of the issue, solution, and a review of the scripts, if any, is conducted. Scripts should meet the same standards set by CNSI internally to ensure continuity and reduce the chance of negative effects to the system.
- Once approved, the resolution will be implemented.
- Team CNSI Operations Management receives periodic updates throughout the incident until the resolution is completed.
- Team CNSI management notifies the appropriate DPHHS personnel.

After the incident or problem has been resolved, Team CNSI creates an Incident Report. An Incident Report compiles the following information:

- What triggered the incident
- What services are affected by the incident
- A complete timeline of events
- All actions taken to resolve the issue
- Lessons that were learned and ideas for prevention in the future
- List of each person involved at any time throughout the incident
- Summary of each communication
- Attachments, including actual emails and records of phone calls and meetings, with a summary of what was discussed

The completed Incident Report is then distributed to Team CNSI management. After review, Team CNSI management distributes the Incident Report to the appropriate DPHHS personnel. If more than one problem occurs in the same area, Team CNSI conducts a root-cause analysis to develop a thorough understanding of the issue and its causes. The Incident Reports for those problems are used as part of the tracking and understanding of the problems. A plan is derived from the analysis for either corrective or preventative actions that will reduce the risk of another occurrence to an acceptable level. The corrective or preventative actions will be documented, implemented, and shared with DPHHS. Follow up reviews of the actions are conducted to make sure they are properly alleviating the issue and determine whether there is a more efficient way of correcting or preventing the problem.

Changes are a natural part of projects and operational environments. Team CNSI proposes processes that not only anticipate changes but also addresses them on a timely and proactive basis. Team CNSI delivers high quality software to its customers through the execution of our CMMI level 3 processes for all department change requests for enhancements, which includes proposed solution and pool hours/cost within 10 days for low complexity projects, 20 days for medium complexity projects or 30 days for high complexity projects, from submission of a Department Change Request for an Enhancement.

Changes arise from new requirements leading to enhancements, process changes or software defects. Team CNSI will implement a change management process that will be used throughout the operations phase of the contract. The process and associated supporting artifacts, such as forms, templates, or reports, will be included in the Change Control Plan. The steps conducted in tracking Change Requests (CRs) are as follows:

- Create and submit the CR
- Record and review the CR information

- Assess and evaluate the CR
- Authorize the change through the CCB
- Update plans and other documents based on the impact analysis
- Implement the CR and coordinate with impact organizations
- Review and close the CR

A CR may be used to propose a change to the scope, schedule, cost, or configurable items such as hardware, software, or security permissions. A CR can originate from the State, fiscal intermediary staff, other project team members, external stakeholders, and end users that need service. CRs may also originate from the risk or issue management processes.

System Availability

Team CNSI availability architecture provides redundancy and scalability needed to support 99.5 percent availability and the goal of minimal disruption to providers, members, and other users of the solution.

Reviews business process availability requirements and aligns them with our ITIL framework. This ensures that cost-effective contingency plans are in place and tested on a regular basis to ensure that the business needs of DPHHS are met. Team CNSI's Availability Management plan includes but is not limited to the following aspects:

- Designing high-availability, redundant systems to support mission-critical applications
- Testing system availability to meet all MPATH SLAs

Monitoring and reporting high-availability to ensure that SLAs are being met.

Team CNSI's hosting platform includes hardware and software components that are built using either Traditional licensing, Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or Software as a Service (SaaS) services. Detailed list of all the proposed services and solutions are listed in Attachment L - Technology Metrics. All hardware and software components that are required to support the proposed solution and services will have the necessary licensing agreements in place for the entire duration of the contract.

Team CNSI's hosting solution includes three types of licensing models:

- Subscription based license
- Perpetual license
- Open Source

For all components that are licensed on a subscription basis or perpetual basis, upon request Team CNSI will turn over the subscription contracts and perpetual license contracts to the Department within 30 calendar days or less. For all components that are open sourced but have support contracts in place, upon request Team CNSI can turn over the necessary support contracts to the Department within 30 calendar days or less.

Team CNSI's proposed solution is built on a resilient, redundant design with best-of-breed infrastructure and a highly robust network architecture. All hardware components including servers, switches, storage appliances, backup storage appliances, and firewalls have in-built redundancy in both the primary and standby/DR data center. The primary site will host Test (System Test, User Acceptance Test, Regression Test) and Production environments, while the standby/DR site will host Stage (Performance, Parallel Test, B2B) and DR environments.

Team CNSI's evoBrix PMIS solution is modular and highly scalable supporting multiple applications in different logical environments starting from Development to Production. Detailed information about the environment topology and application topology is listed in Figure 3.10.1-66 and Figure 3.10.1-67 under ENV06 requirement in Section 3.10.1.3, Hosting and Environments.

Every environment is configured to support all applications necessary to perform the designated business functions. Detailed information about various applications that are required for a logical environment is specified in Figure 3.10.1-69 under the ENV06 requirement in Section 3.10.1.3, Hosting and Environments. Team CNSI will also ensure that all these applications running in different environments have the necessary licensing agreements required to support them.

Disaster Recovery

Team CNSI's Disaster Recovery/Business Continuity (DR/BC) Plan, as outlined in section 3.10.1.3 Hosting, ensures that Team CNSI's evoBrix PMIS solution continues with little disruption, as well as meeting and exceeding their business continuity requirements. Team CNSI's DR/BC Plan is defined based on the following examples that can lead to the declaration of a disaster:

- Extended power outage expected to exceed backup power capacity facility-wide
- Loss of a building or buildings due to fire, flood, earthquake, or a hazardous material (HAZMAT) incident
- Water or structural damage
- Regional or local damage or conditions from severe weather
- Incidents that causes the primary data center or telecommunication lines to be non-functional

To successfully restore system availability within four hours of unplanned downtime, Team CNSI's evoBrix PMIS system has a fully-equipped secondary site that is geographically separated from the primary system to prevent failure due to facility disruption from natural disasters. The secondary site is built to the same exacting security and facilities standards as the primary site. All data is replicated in real time to the secondary site so that in the event of the primary site not being available, the secondary site will fully takeover all tasks and workload. Based upon our annual testing, the secondary site becomes fully operational within four hours.

Solution Architecture

The evoBrix ISR core architecture leverages ESB features within the SOA framework to integrate disparate systems effectively. This architecture provides an integration backbone that connects core applications and services without directly accessing underlying systems. The evoBrix architecture is based on leveraging a series of COTS products that use a services-based integration platform.

evoBrix relies on open standards and standard application program interfaces (API), such as the Java Business Integration (JBI) standard, for plug-ability of third-party communities. The evoBrix architecture uses an enterprise class service bus (Oracle Fusion SOA) as the core orchestration tool of business processes across the different applications that support Medicaid operations. evoBrix supports robust authorization, authentication and validation features using Oracle Service Bus. The proposed solution is capable of handling common industry standard service requests such as SOAP and REST. Also, evoBrix has the ability to change the various attributes of the service without impacting existing clients. The ESB infrastructure allows Core MMIS to avoid point-to-point communication between different system components to streamline flow of all information throughout the MT PSM implementation. This ensures the maximum amount of time between the receipts of a transaction, by the Enterprise Service Bus (ESB) through the response sent to the appropriate receiving system, will not exceed two seconds.

Data Management

As part of the MT PSM conversion effort, Team CNSI's conversion team will ensure that 99% of all data converted is correctly mapped and usable by the scheduled completion date. Team CNSI would like to emphasize the fact that the successful outcome of the conversion effort is tied to the quality of the conversion business rules to be provided by MT DPHHS jointly working with Team CNSI, so it is critical to ensure that the conversion mapping exercise is validated by the relevant stakeholders to ensure a quality outcome. We will also convert all required and supporting source data to ensure that the business and usage requirements are met right from the go live in the new MT PSM solution. The conversion process will take the following into account:

- Conversion of all operationally relevant and required source data for day-to-day operations
- Sufficient historical data to ensure all audit and legal requirements are addressed
- All required source data is accurately mapped in the conversion mapping documents
- Varying time periods for different functional areas which are required for reporting, analytics, and business operation
- The conversion process is completed as per the project timelines and requirements

The evoBrix solution for MT PSM is designed on an integrated data model to handle transactional and operational data. The data model not only determines the structure and flow of data throughout the solution, but more importantly ensures the data that gets into the system is consistent in terms of business relevancy, data format, and other data semantics. The data model is normalized and minimizes data inconsistencies by enforcing data integrity via a combination of database constraints such as primary key, foreign/referential integrity keys, check and unique integrity constraints, and validates for the presence of mandatory values in conjunction with application enforced business rules. With the enforcement of data integrity, the MT PSM solution has the checks and balances in place to ensure that anomalous data is not introduced to begin with ensuring that the overall data integrity error rate for any data updates or batch updates stays less than .001%. The same philosophy applies to any data updates in MT PSM that are triggered by batch/real-time feeds coming from external systems and the MT PSM solution will ensure that the transactional processing/routing errors stay less than .001% and proper notifications are generated to communicate the errors.

All web service traffic to MT PSM solution will be routed via Oracle OSB managed by ISR framework. Team CNSI's evoBrix integration solution, which has been proven in CNSI's current implementation with other states (Michigan, Illinois, and Utah), enables MT PSM's real-time transactions to receive data from real-time Interfaces to be accessible in the Module within three seconds at least 99% of the time; excluding batch interface updates. The audit capability of the solution provides the ability to monitor request time, response time, requesting user, requested service, request message and response message. This enables MT PSM users to measure the performance of real time transactions, as outlined in section 3.10.1.6, Interfaces.

Team CNSI has extensive experience in implementing X12 version 5010 and interacting with providers, clearing houses and third-party vendors using the following HIPAA transactions as required by 45 CFR Parts 160 and 162, to adhere to applicable specifications of all EDI transactions.

- 270 – Eligibility, Coverage, or Benefit Inquiry
- 271 – Eligibility, Coverage, or Benefit Information
- 276 – Electronic Claim Submission System Request
- 277 – Electronic Claim Submission System Response
- 277RQ - Health Care Claims Request for Additional Information
- 277CA - Health Care Claim Acknowledgement Report

- 835 – Healthcare Claim Payment Advice
- 837D – Healthcare Claim – Dental
- 837I – Healthcare Claim – Institutional
- 837P – Healthcare Claim – Professional
- 999 – Functional Acknowledgment
- TA1 – Interchange Acknowledgment
- 278 – Prior Authorization Request
- 278 – Prior Authorization Response

Team CNSI follows a 'design first' approach when developing its REST APIs for target audiences who are the external customers and trading partners. Since 'design first' approach advocates for designing the API's contract first before writing any code, we use Swagger Specification to publish the API description. The clients consuming these services will have a rich User Interface (UI) that serves as a playground for interactive testing of the REST API. The approach is transparent to the clients, speeding up the integration process with parallel development.

Team CNSI's evoBrix solution can support DPHHS need to move towards real-time web services. There are several instances of enabling near real-time web services that supported in our production environments that can be leveraged for meeting DPHHS needs. The following are the different scenarios of near real-time web services usage that are available in the evoBrix solution.

The key interoperability capabilities of the proposed solution are as follows:

- SOA/Standards-based integration approaches using protocols including REST, SOAP, and COTS APIs.
- Support for standard content formats such as documents, XML, JSON, EDI for user, and machine-readable and understandable content.
- REST APIs leveraging Swagger specifications for producing, consuming, and visualizing APIs. Used to support service inquiries.
- SOAP APIs leveraging WSDL specifications for data exchange with business partners for post services. Versioning through the Mediation layer allows for rapid adoption of change. Web-services-based information exchange for real-time integration capabilities.
- COTS APIs expose COTS functionality as internal and external interfaces through standard APIs. Examples include Document Management API, Workflow API, Correspondence API, and SIEBEL API.
- Supports for standards-based information exchange for EDI transactions (e.g., HIPAA ANSI X12 standards). Support for secure FTP gateway. Compliance with CORE rules.
- File-based information exchange for standard and non-standard file based integration.
- Secure information exchange using API keys, web service security 1.0 standards, and other security protocols for securing data during transit.

Provider Support

Team CNSI's operations strategy provides DPHHS the staff to support the provider enrollment Call Center toll-free phone lines. Our Call Center is available from 8:00 a.m. to 5:00 p.m., Mountain Time, on all State business days, Monday through Friday (excluding State holidays) to respond to provider inquiries. Team CNSI's solution integrates with HealthBeat, our reporting dashboard, to report on Call Center metric data, including the time and date stamp phone lines were open and when phone lines were turned off.

Team CNSI's Customer Relationship Management (CRM) Siebel system Open UI delivers rich user experience and helps the Customer Service Representative (CSR) agent to better understand and address the needs of the customers in an effective and efficient manner to deliver a researched response, or an accurate resolution to the inquiry within two business days. Our solution offers a multi-channel environment where providers can connect with a CSR in the manner most suitable, such as assisted chat, email, and voice. The CRM solution ensures responses have a 97% or higher accuracy resolution rate, within the 25% threshold of inquiries that are unable to be resolved during first contact. Section 3.10.14.3, Customer Relationship Management, provides additional details on how Team CNSI accomplishes this requirement.

The CRM application is tightly integrated with the multi-channel contact center solution, and provides the mechanism to track all communications and document the resolution and outcome. Team CNSI's solution tracks Call Center data and reports daily on our interactive reporting dashboard, HealthBeat to track request date against the response date for DPHHS to monitor.

Team CNSI uses our innovative mobile application, SiteVisitPro (SVP) to conduct and maintain site visits. SVP is designed for use with tablets to enable our business operations staff to provide site visit updates on a real-time basis to support the enrollment process. Eliminating the need to transfer data from paper forms greatly improves the accuracy and efficiency of our provider enrollment processes. This application uses real-time provider information directly from our PMIS module, eliminating redundant data entry.

Team CNSI's SiteVisitProcesses utilize two primary solutions modules, PMIS and SiteVisitPro, used by our staff to manage and conduct provider enrollment and related site visits. The PMIS module provides the central provider enrollment and management capability supported by an attribute-rich data store. Key provider information such as demographics, locations, ownership, taxonomy, and risk category are shared with SVP for providers selected for site visits. SVP is used to manage all aspects of the site visit from scheduling to documenting the results to ensure the onsite screening checklist will be completed and keyed into the applicable provider profile within the solution with 97% accuracy. The site visit results are posted to PMIS for reporting and record keeping. SiteVisitProcess steps and activities are logged for monitoring using Team CNSI's HealthBeat.

3.10.9 Subcontractors

The highest scoring Offeror will be the Prime Contractor if a contract is awarded and shall be responsible, in total, including for all work of any subcontractors. Nothing contained within this document or any contract documents created as a result of any contract awards derived from this RFP shall create any contractual relationships between any subcontractor and the State. The Offeror must describe their approach to meet the Subcontractor requirements defined in Attachment F, Requirements Matrix.

For the PSM effort, CNSI immediately reached out to its longtime partner, Noridian Healthcare Solutions, LLC (Noridian), to bring its impressive history in health care and claims processing to the team. Noridian originated in 1966. Its initial purpose was to provide government-funded health care administration as a Medicare carrier and fiscal intermediary to CMS. Throughout the next 40 years, Noridian grew consistently larger, establishing itself as a fully capable provider of administrative services and setting the groundwork to take on Medicaid and commercial lines of business in addition to Medicare.

The partnership between CNSI and Noridian spans nearly 10 years, because CNSI values Noridian's expertise and excellent reputation in the industry. Currently, Noridian is a subcontractor on CNSI's contract with the state of Michigan and is responsible for performing predictive analytic medical reviews. Specifically, Noridian's review nurses support the business operations of the ClaimsSure solution, CNSI's product to detect improper billing – a solution that, according to the state of Michigan's publicly-

shared metrics, has saved the State approximately $30 million since go-live in 2013. This success has only strengthened the working relationship and collaboration between CNSI and Noridian.

The following sections provide CNSI's responses to the RFP requirements specific to Subcontractors.

SUB01

The Contractor may use subcontractors for no more than forty percent (40%) of the scope of work included in the contract.

On the PSM initiative, Noridian will be providing expertise and operations support services pertaining to our contract offerings under Option B, Provider Services, as defined in the Statement of Work and detailed in response to Requirement SUB04 below. As is evidenced from the detailed breakout of their responsibilities, Noridian's work share is within the mandated 40% threshold of the scope of work that can be subcontracted under this contract.

CNSI's government services organization unit is appraised at Capability Maturity Model Integration (CMMI) Maturity Level 3, which includes subcontractor management. CNSI's partner/vendor management team at the corporate level is responsible for partner participation, collaboration, and success. We establish relationships with all strategic partners and vendors, all the way up to the executive team. This is critical for escalating and resolving issues quickly. We also set clear expectations for all partners, and provide for a clear, concise, and executable subcontractor management plan. Part of this process is the clear definition and assignment of work to the various entities participating on our team, and ensure agreement with, and understanding of, what each is responsible for.

SUB02

If the Contractor transfers resources required to fulfill the contract to a third party, the third party is considered a sub-contractor and the transfer will be subject to the 40% subcontractor limitation.

CNSI intends to use Noridian as our sole subcontractor. As the owner of the evoBrix PMIS solution that Team CNSI is proposing to meet the MT PSM requirements, CNSI does not anticipate transferring resources to fulfill the contract to a third party. Utilizing our analysis and assessment of the RFP requirements, CNSI is sure that we will require the services of only Noridian on this contract. However, we do understand and acknowledge that if we transfer resources required to fulfill the contract to any additional "third party", then that entity will be considered a subcontractor, and the transfer will be subject to the 40 percent subcontractor limitation. In such a scenario, we will immediately inform the DPHHS of the addition to our team and ensure that work assignment to the third party will still conform within the overall subcontracting limit under this contract.

SUB03

The Contractor shall list all subcontractors, if any, in the proposal.

As mentioned earlier, the only subcontractor CNSI has on this project is Noridian.

SUB04

The Contractor shall provide a detailed description of all work to be subcontracted to third parties.

As CNSI's subcontractor, Noridian will support the following areas under the Option B scope of work:

- Conduct Provider Site Visits
- Include Reference Documentation
- Customer Relationship Management (CRM)
- Provider Call Center
- Integrated Voice Response (IVR)
- Staffing
- Collect and Enter State Auditor's Office Financial Information
- Performance Requirements

Noridian possesses the technology, business processes, and experience with the provider community for the multi-state cooperative members supported through the NASPO ValuePoint initiative. They support Medicare providers in the states of Montana, Wyoming, South Dakota, North Dakota, and Oregon. Noridian also brings experience in federal and state health care services, including direct support of providers participating in these programs.

The core aspect Team CNSI's Option B solution is based on our evoBrix Provider Management Information System (PMIS), which provides a repository to enable our business operations staff to manage the full life cycle of provider services. A rich set of provider management capabilities also enables self-service, provider enrollment, pre- and post-enrollment screening, license renewal, and address validation/standardization. Additional details pertaining to Noridian's Option B Provider services support are addressed in Section 3.10.14 of our proposal.

SUB05

The Contractor must submit to the Department annually, a Subcontractor Usage Report on the use of subcontractors and certify that all subcontractors are in compliance with the employment practices mandated by federal and State statutes and regulations.

CNSI agrees to submit a Subcontractor Usage Report to DPHHS, and will certify that our subcontractor is in compliance with the employment practices mandated by federal and State statutes and regulations. CNSI has submitted similar reports on other contracts, such as those with the states of Maryland and Washington. Additionally, CNSI and Noridian have teamed on similar engagements before, and are very familiar with each other's contractual, operational, and regulatory practices and obligations.

SUB06

The subcontractor will be required to enter into a signed Business Associate Agreement (BAA) as a part of the contract, that is in compliance with the Privacy and Security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) prior to start of work. The BAA is included in the contract template found in the Procurement Library.

Following contract award and prior to the start of contract work, CNSI will require Noridian to provide a signed Business Associate Agreement (BAA) to become part of our contract to show that they will be in compliance with the Privacy and Security provisions of HIPAA. As part of their standard practice, Noridian has signed similar agreements and, therefore, accepts to sign the BAA, as required by the Department.

SUB07

The Contractor shall allow Department personnel direct access to all subcontractor or third-party personnel serving in critical roles on the project and shall not act as an intermediary between the Department and such parties for questions about the proposed solution or operation of the proposed solution. The Department reserves the right to discuss design, configuration, implementation, operation, routine maintenance, and enhancement of the proposed solution(s) directly with any subcontractors or third parties involved in performing work for the Department.

CNSI will provide DPHHS full transparency to Noridian, providing access to, and enforcement of, the same security policies. This creates a "badgeless" team, with each individual working with one "face" and "voice" for the customer, regardless of which company employs the team member. Project resources are unified and the fact that they are employed by different employers is not a barrier to communication or project commitment and completion.

To validate this approach, Team CNSI provides DPHHS with a single point of contact – our Project Manager, Diana Grogan – to streamline communication and bolster responsiveness. However, we agree to allow DPHHS personnel direct access to all Noridian personnel serving in critical roles on the project. CNSI will not act as an intermediary between the DPHHS and our subcontractor for questions about the proposed solution or operation of the proposed solution. We understand and accept that the Department reserves the right to discuss design, configuration, implementation, operation, routine maintenance, and enhancement of the proposed solution(s) directly with any of our subcontractors (in this case, Noridian) who are involved in performing work for the DPHHS.

SUB08

The Department shall have the right to review and approve any subcontracts through the Contractor.

CNSI acknowledges and accepts that DPHHS will have the right to review and approve any subcontracts through CNSI.

3.10.10 Enrollment

This section addresses provider enrollment requirements. The Provider Services module will support a web-based tool for providers to electronically enroll with Montana Healthcare Programs which includes an automated tool for screening activities that must be completed in accordance with State and federal statutes, policy, mandates as well as industry standards required for the Contractor's Scope of work. The Offeror must describe their approach to meet each of the Provider Enrollment requirements defined in Attachment F, Requirements Matrix.

evoBrix PMIS provides a rich set of Medicaid Information Technology Architecture (MITA)-aligned features for provider enrollment, provider information management, and provider support functions that will serve to address the State's requirements. The solution combines a full-featured, secure, self-service provider portal with a comprehensive administrative framework to manage enrollment, disenrollment, inquiry, provider information maintenance, and provider support. The solution provides State staff and providers with a full range of online, real-time inquiry and update functions through web-based data entry screens. The solution maximizes the opportunity to collect valid and complete information throughout the provider's association with Montana Department of Public Health and Human Services (DPHHS). The solution provides a browser-based and interactive system supporting the day-to-day business needs of the providers and DPHHS user communities. evoBrix PMIS, including Provider Enrollment, Provider Credentialing Service (PCS), and SiteVisitPro (SVP) modules, is the only true web-centric automated provider enrollment solution with comprehensive provider credentialing service in the State Medicaid market that is in production and running successfully.

The Team CNSI Advantage

Team CNSI's certified implementations in the states of Michigan and Washington will bring the State a proven and mature Provider Management Information System (PMIS).

- evoBrix PMIS is a modern, web-centric provider enrollment and management solution, based on the fully CMS-certified solution in Michigan
- evoBrix PMIS supports both NPI and non-NPI compliant providers
- Rich enrollment options include online enrollment through secure self-service provider portal and offline enrollments through email, traditional mail, telephone or fax to facilitate higher process maturities and provider adoption rate
- Business process wizards powered by rules engine facilitate step-by-step provider enrollment and maintenance process with built-in validation
- One-stop credentialing platform provides improved automation and reduced manual intervention
- Mobile enabled application streamlines site visit processing using a real-time system, eliminating paper

MTPSM-3-021

Figure 3.10.10-1 shows provider enrollment statistics of CNSI's previous implementations of the Provider Enrollment system.

	Michigan	Illinois	Washington	Utah
Enrolled Provider Volume	165,000	255,000	198,000	25,000

Figure 3.10.10-1. Enrolled Provider Volume from CNSI's Previous Implementations. Provider volume ranges from 25,000 to 250,000 across the four states.

evoBrix PMIS supports the processes identified in the MITA's Provider Management business process area and comes with the built-in capabilities listed below:

- Online web capabilities for all users including providers. The solution offers the unique Provider portal that allows providers to access many services 24 hours a day, 7 days a week (24x7x365). The portal enables providers to enter new enrollment applications and maintain their provider data.
- User-friendly, rules-based structure to support provider enrollment and reenrollment policies.
- Proven audit trail features identifying who initiated the change, what changed, when the change was requested, who approved or denied the change, and when.
- Outstanding filtering and inquiry capabilities allowing authorized users to search for and retrieve provider information based on user-supplied search criteria.
- Compliance with and use of the National Provider Identifier (NPI) for provider enrollment and automatic assignment of atypical provider IDs for providers who are not eligible for NPIs.
- Fully service-oriented platform with a seamless integration of industry leading commercial off-the-shelf (COTS) products for letter generation, content management, reporting, and enterprise service bus to support the file exchange process.

Overall, evoBrix PMIS module benefits DPHHS by modernizing and streamlining the ability to respond to provider requests and improve customer service. Figure 3.10.10-2 shows the overall evoBrix PMIS business architecture. This figure depicts a summary of the functions available to providers and business operations staff, as well as the various enrollment types supported in the solution. This figure also shows the integration with external systems, evoBrix application security, and COTS products. The evoBrix PMIS module interacts with external systems through an automated communication channel using real-time web-services and file exchange process.

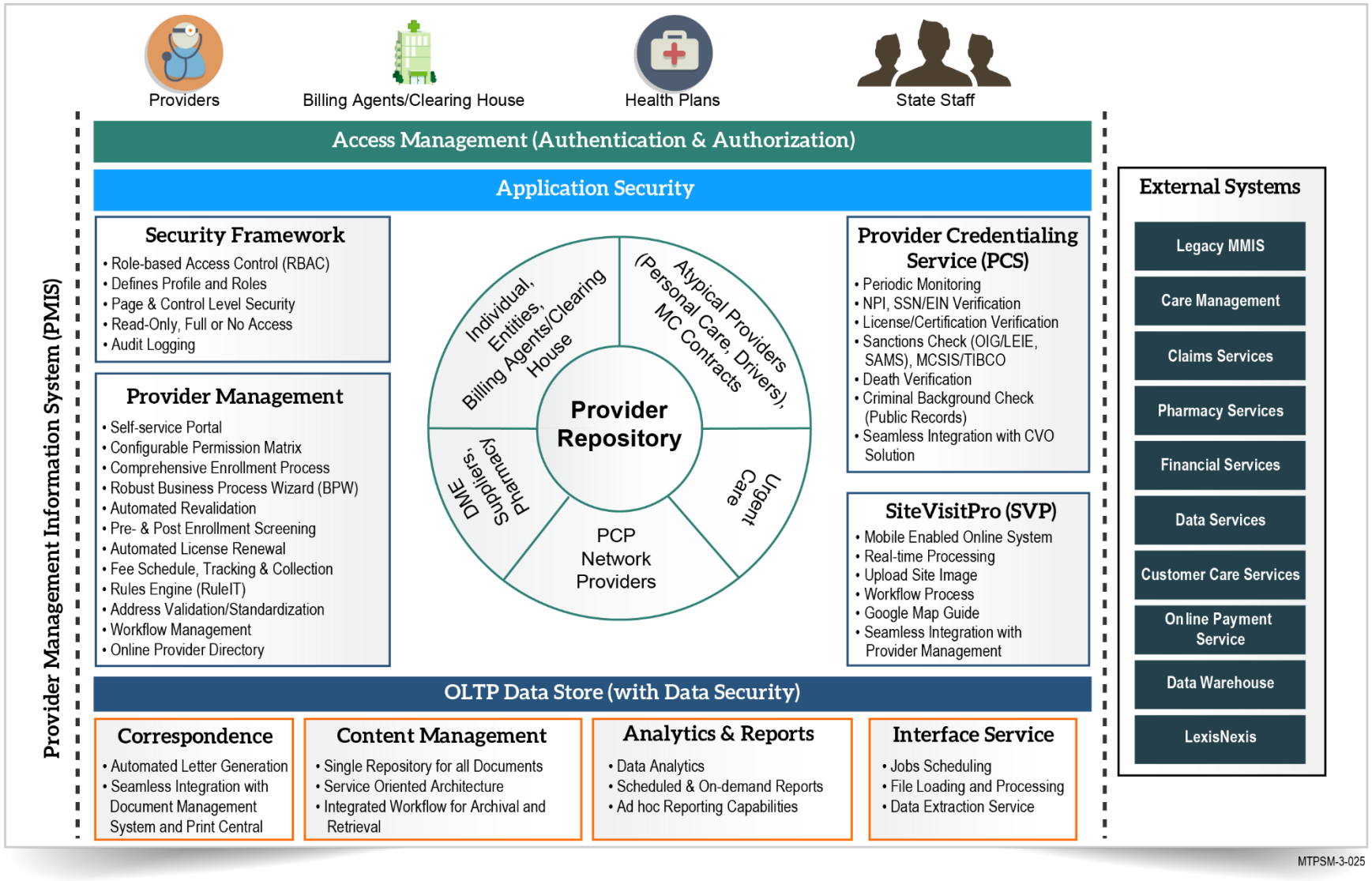


Figure 3.10.10-2. evoBrix PMIS Business Architecture. This figure depicts a summary of the functions available to providers and business operations staff.

evoBrix PMIS has built-in functionality to allow new user registrations for both providers and State-authorized users, a workflow feature to route new user registrations to authorized State staff for their review, a feature to enforce a password reset policy, functionality to actively monitor user accounts for prolonged period of inactivity for automated locking of those accounts, and functionality to maintain demographic information of all users. The evoBrix PMIS solution provides functionality that allows State staff to request for security profiles based on their job duties.

evoBrix PMIS offers a configurable Security Framework that provides a secure environment for information management and protects against unwanted loss or disclosure of data. Authenticated access and role-based access control (RBAC) enforces security in the evoBrix PMIS module. The security framework maintains extensive user audit logging for the audit trail in support of HIPAA Security and Privacy. The Security Framework supports role-based security and limits access to users by domain and user ID. evoBrix maintains three independent, secure access methods for the provider enrollment business area. The method of access depends on the status and type of user as outlined below.

- The first type is a provider who has no previous relationship with DPHHS and is applying for the first time.
- The second type of user is a provider who has a prior active relationship with the DPHHS and who wants to initiate a new enrollment.
- The third type of user is a business operations worker. Business operations workers may have responsibility for processing enrollment applications submitted online, reviewing submitted applications and rendering an approval or denial decision, or providing support to enrolling providers.

Provider enrollment process is supported by a Business Process Wizard (BPW) that guides the provider through the process. Business rules are housed in the decision management framework called RuleIT, which governs the sequence of the enrollment steps and the content collected. The business rules prevent submission of the enrollment application until the information content has been verified for completeness and validity. The system communicates the process deficiencies and missing information in online screens in real time before allowing the provider to move to the next step in the enrollment process.

The evoBrix PMIS solution supports both new enrollments and enrollment modifications. The new enrollment application, once submitted by the provider, will be reviewed and approved by the provider enrollment unit. The solution also provides the ability for providers to perform updates to the enrollment information using the web portal, which will be forwarded to the provider unit for review and approval. The BPW uses DPHHS-specific rules configured using the RuleIT rules engine to designate steps as required or optional, dynamically depending on data entered by the provider for a given enrollment type. The wizard validation rules are based on the enrollment type and include validation of data, such as NPI.

The evoBrix PMIS solution highlights are listed below:

- Configure enrollment process workflow per state-defined criteria
- Accept electronic forms, supporting documents/attachments
- Perform enrollment process electronically
- Define industry standard provider types, specialties and sub specialties; associate standard and non-standard taxonomies through a comprehensive Permission Matrix
- View/Upload attachments for uploading the supporting documentation such as copy of license, copy of any certifications with the enrollment application
- Enroll/Dis-enroll/Activate/Deactivate providers per state-provided criteria
- Collect enrollment fee for the institutional providers via online payment service
- Track fingerprinting based on the provider risk category

- Support submission and processing of provider appeals and grievances including service requests tracking

The evoBrix PMIS provides a decision management framework for administration that allows authorized users to configure, define, and maintain the business rules required for provider enrollment, disenrollment, re-enrollment, and maintenance activities as required by State policy. The decision management framework includes features that allow authorized users to perform the following activities:

- Define State-specific provider type and specialty/subspecialty combinations
- Configure mandatory, optional, and conditionally mandatory enrollment and re-enrollment data requirements by provider enrollment type and specialty
- Define and configure credentialing and re-credentialing rules for each unique provider type and specialty combination

In evoBrix PMIS, business rules for provider management use the following tools to cover three broad areas:

- Permissions Matrix – To define the specialties the State supports under different administrations/programs
- Credentialing Matrix – To define specific credentials, such as licensing, required by the successful applicant for each defined enrollment type/specialty combination
- RuleIT – To define the enrollment steps needed for each category of enrollment

The evoBrix PMIS uses the flexible and comprehensive RuleIT Rule Composer to allow users to define the enrollment rules for each enrollment type and specialty. Authorized users will use the Rules Composer to define each step of the enrollment process and the data elements that are required in determining a particular step to be complete under a given enrollment type.

The provider enrollment BPW uses these State-specific rules in the RuleIT rules engine functions to designate steps as required or optional dynamically depending on data entered by the provider for a given enrollment type based upon the configurable Permission Matrix and Credentialing Matrix. The wizard also displays validation error messages throughout the data entry process. These interactive messages alert the provider to conditions that need to be corrected so that validated and complete data is captured prior to submission.

Affordable Care Act (ACA) – Provider Screening Mandate

One of the ACA provisions mandated new screening procedures for Medicare, Medicaid, and Children's Health Insurance Program (CHIP) providers. The key goal of these screenings is to ensure that the provider is actively functioning and servicing patients at the reported location, and subsequently reduce the chance of fraud, waste, or abuse. The screening applies to:

- New providers enrolling for the first time
- Providers reenrolling due to a change of ownership
- Existing providers revalidating their enrollment

All providers are assigned to one of the risk categories: High, Moderate, and Limited. Prior to completing enrollment processing, providers are subject to screening tasks based on their risk category. The screening requirement includes:

- Validation of disclosed individuals with the Office of Inspector General (OIG) Excluded Individuals database, the Excluded Parties List System (EPLS) and the Social Security Death Master List.

- In-state and out-of-state professional license verification.
- Clinical Laboratory Improvement Amendments (CLIA) and Drug Enforcement Administration (DEA) Certification verification.
- Proof of Medicare enrollment, if Medicare-enrolled.
- Validation of the NPI with the National Plan and Provider Enumeration System (NPPES).
- All providers classified as "High" and "Moderate" are subject to unscheduled and unannounced site visits. Periodic site visits are also required when existing providers re-validate their information with the timing based on the risk categorization.

Provider Credentialing Service (PCS)

CNSI's PCS platform, in partnership with LexisNexis, will provide full compliance with the ACA Provider Enrollment Screening requirements. The PCS solution is comprised of pre- and post-enrollment screening processes that integrate the system with a real-time credentialing service. This one-stop solution provides improved automation and reduced manual intervention. Pre-enrollment screening results are available in real time within PCS web pages for the provider enrollment specialist to review and make appropriate decisions regarding whether to approve or deny the enrollment application.

The solution is flexible for the provider enrollment specialist to perform the screening process on an on-demand basis using online PCS web pages anytime during enrollment application or modification review. The solution performs periodic screening of providers using LexisNexis credentialing service and applies the business rules defined by the State Medicaid program. The PCS solution provides ability to track screening results to meet audit requirements for the following screening criteria:

- State/Federal Death Verification
- Sanctions
- OIG Sanctions
- General Services Administration (GSA) Exclusion list (EPLS/SAM)
- License Board Sanctions
- NPI Verification
- SSN, EIN/TIN Verification
- National Council for Prescription Drug Programs (NCPDP) Verification
- License/Certification Verification
- In/Out-of-state professional license
- DEA, CLIA, Board Certification Verification with American Board of Medical Specialties
- Criminal History and Sex Offense check

The PCS common features are as follows:

- Integrates with LexisNexis credentialing service
- Integrates with other State-specific data sources provided by DPHHS
- Ability to view screening results in real time
- Real-time, on-demand screening capabilities anytime during enrollment application review or modification review
- Supports audit capabilities
- Screening of individual practitioners, hospitals/entities, disclosed entities (such as board of directors, office managers, corporate, agents), etc.

Figure 3.10.10-3 shows the various components in the PCS architecture. CNSI's PCS has a web interface that provides a user-friendly Graphical User Interface (GUI) for viewing screening results in a tabular layout. Any screening that requires attention is flagged for users so they can check for more details before deciding.

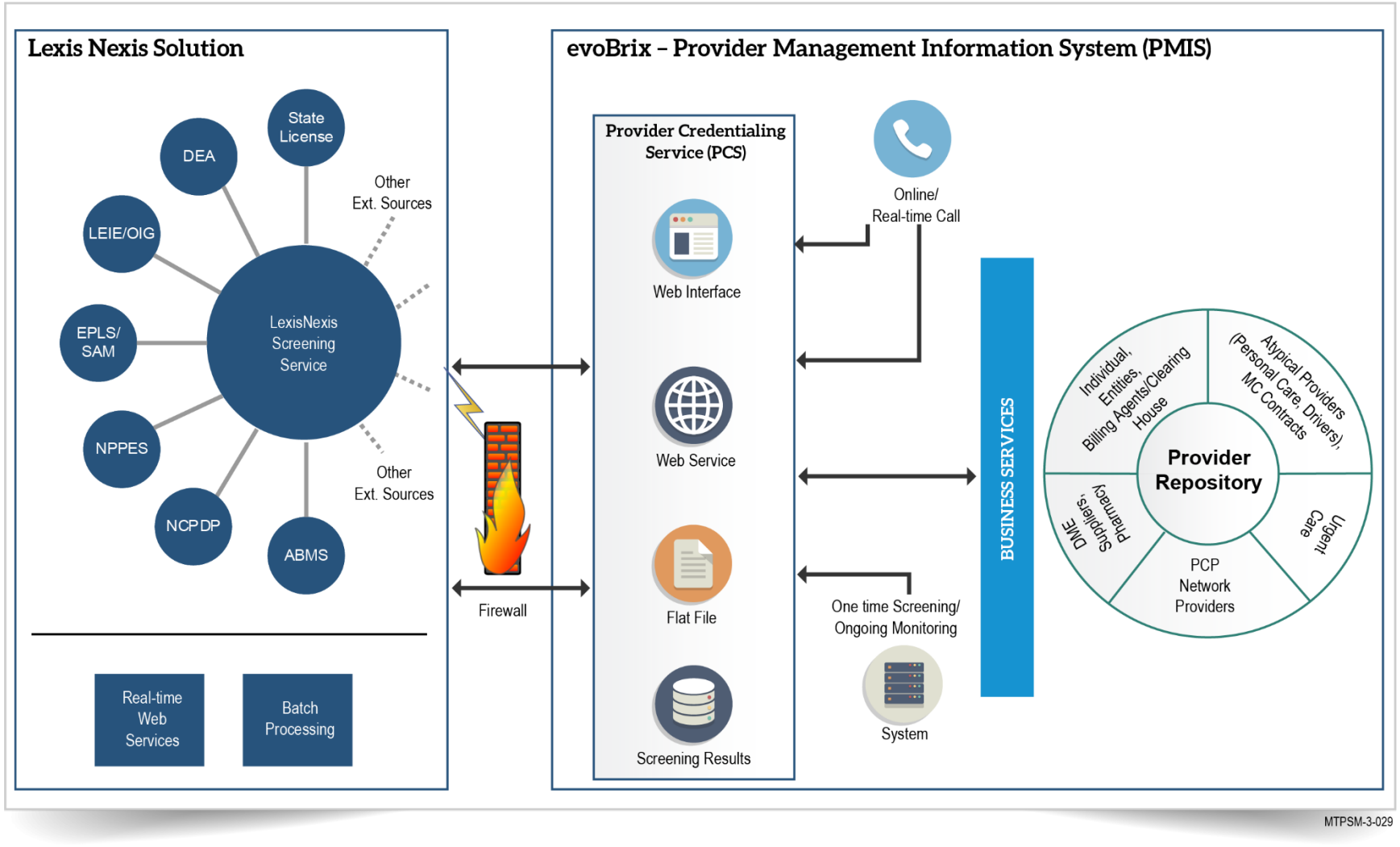


Figure 3.10.10-3. Provider Credentialing Service Solution Overview. evoBrix PMIS integrates with LexisNexis through the PCS solution.

Provider Enrollment through Web Portal

For providers who have never had a relationship with the State Medicaid program, an enrollment is initiated through the evoBrix PMIS web portal. The evoBrix PMIS pages are designed to give a nearly identical GUI experience to providers and State staff. Because the pages are identical in most cases, it is easier for the State staff to provide support to providers. This also simplifies help desk processes.

At the first step of the enrollment process, evoBrix PMIS issues a unique enrollment application number to the provider. Using this number and an alternate unique identifier, such as the provider's NPI or federal TIN, the provider may continue to access and update their in-process application until it has been submitted for review and approval/denial decision.

Enrollment Type Selection

The evoBrix PMIS supports enrollment of all types of providers, including

- Traditional medical providers who use an NPI to conduct business, e.g. physician, nurse practitioner, physician group, clinic or hospital
- Atypical providers who are not eligible for NPIs, e.g. taxi/transportation company, home help
- Other organizational entities supporting delivery of care, such as MCOs, billing agent/clearinghouses

Figure 3.10.10-4 shows the list of enrollment types that the user can choose to initiate the enrollment. The options available in the screen enable the provider to decide what enrollment type he/she belongs to before continuing with the enrollment process.

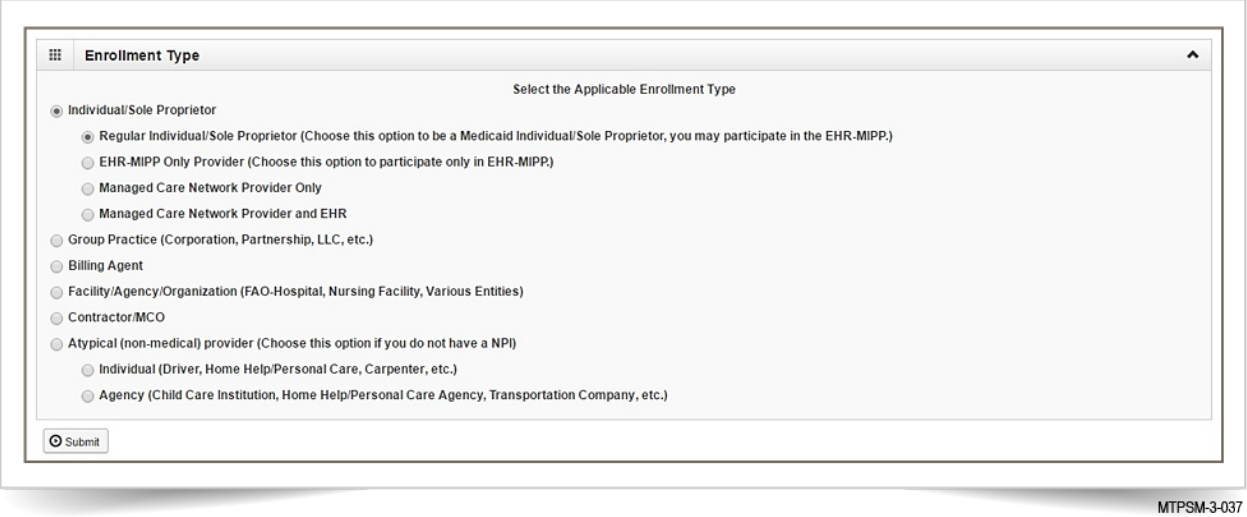


Figure 3.10.10-4. evoBrix PMIS Enrollment Type Selection for New Enrollment. The evoBrix PMIS enrollment wizard validation rules are based on the enrollment type.

Application Tracking

During the new enrollment process, evoBrix PMIS generates a unique 14-digit application number after collecting basic information from the provider, as shown in Figure 3.10.10-5. The providers use the number as reference which allows them to track and resume working on an incomplete application. The application number also allows providers to check on the status of their submitted application. evoBrix PMIS provides the ability for the providers to view and print a copy of enrollment application data for their records, prior to and after submission.

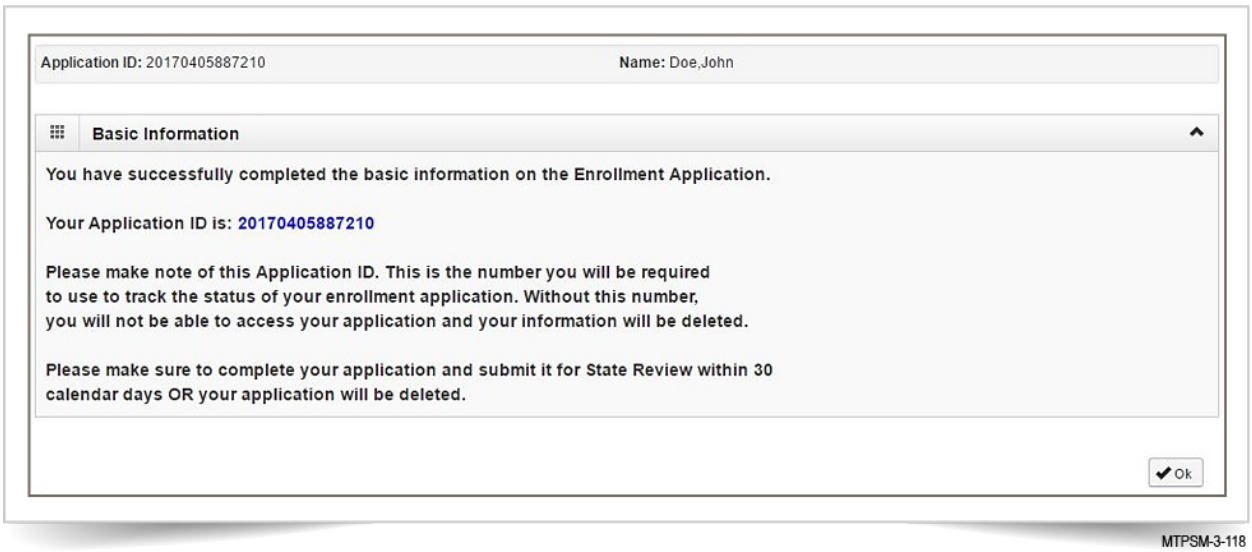
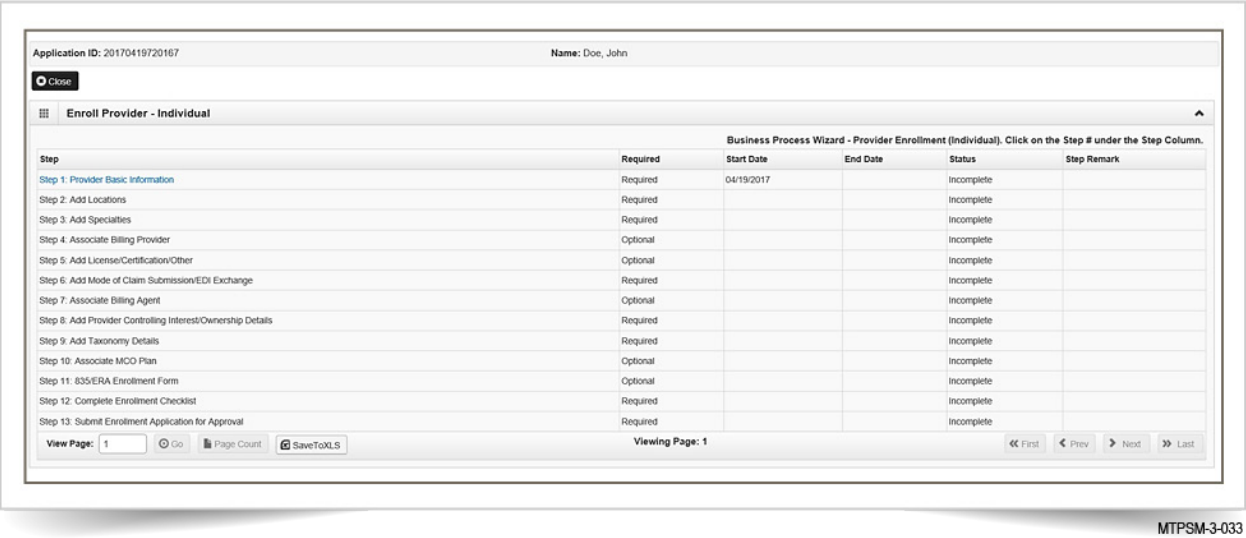


Figure 3.10.10-5. Application ID Generation. After basic information is successfully completed, the system generates an Application ID for tracking the application by providers.

Enrollment Business Process Wizard

The evoBrix PMIS supports interactive online enrollment application that provides structured, online screens with a BPW for provider enrollment. The wizard guides the provider step-by-step through the enrollment process. It maintains the state of the application thus allowing providers to resume an incomplete application exactly where they have interrupted during the enrollment process. The wizards are configured to the State's standards and fully support State-specific credentialing rules. As the provider proceeds through the application, the wizard marks each step as required or optional, and shows which steps have been completed. It allows the providers to navigate, view, validate, and modify any information in the application up to final submission for review and approval. Providers can access help materials online within the evoBrix PMIS portal and the help desk number is also listed for them to call in case they need any assistance.

The evoBrix PMIS provider enrollment BPW is configurable for different enrollment types. After the basic information is saved, the system generates the application number and displays the BPW to the user. Figure 3.10.10-6 shows an example of the wizard for a newly initiated Individual enrollment type.



MTPSM-3-033

Figure 3.10.10-6. The evoBrix PMIS Individual Enrollment Business Process Wizard. The evoBrix PMIS wizard guides the enrolling provider through all steps of the enrollment process.

The enrollment process captures many details about the provider. All details are captured through the data entry pages and dialogs that are triggered from each enrollment step in the wizard. The provider's information captured includes:

- Enrollment Type such as Regular Individual, Rendering/Servicing Only Provider, Group Practice, Facility/Agency/Organization/Institution, Billing Agent, Atypical Individual, Atypical Facility/Agency/Organization/Institution
- Depending on the Enrollment type and Applicant Type, Enrollment Steps in the Business Process Wizard changes as per the State business requirements, such as for "Individual Sole Proprietor Only" Providers, BPW adds a Location step details but in case of "Individual Rendering/Servicing Only" providers this step does not exist
- Provider NPI for all traditional medical providers
- Provider name, gender, and date of birth, or alternately organization name and organization business name
- Multiple provider addresses and contact details, including office locations, pay to location, and mailing addresses, and Managed Care Organization Location (for MCOs)
- Taxonomies associated with the NPI at NPPES registry
- Credentials such as State Professional license, DEA, CLIA, and certifications such as ABMS and NCPDP
- Claim submission methods such as EDI exchange or Paper or Direct Data Entry
- Provider associations with other entities, such as MCO Networks, billing agents, and billing/servicing providers

The BPW allows users to create new enrollment, bundling all the necessary information in the following steps:

- Provider Basic Information – The evoBrix PMIS collects the provider's demographic information in the Basic Information screen which is the first step of the enrollment process wizard. For individuals, an SSN, date of birth, first name, middle initial, last name, email, and home address are required as part of this step. NPI is not required for Atypical Individuals. For organizations, Entity Business Name must be provided with the provider's EIN/TIN number. The NPI is mandatory for all

traditional medical providers. The evoBrix PMIS supports different classifications of individual providers such Sole Proprietor or Rendering/Servicing Only.

- Locations – After successful entry of basic information, evoBrix PMIS collects the location information for each billing provider. A profiled billing provider in evoBrix has one Base Location (primary practice location) and can have as many as 99 additional service locations. Location Name, contact information including communication preference, and accepting new patient flag are collected at each location.
- Specialties – Provider types/specialties are captured at the provider Base Location. Providers can select a combination of provider type, specialty, and subspecialty available for selection through this step. Provider Type/Specialty and Sub-specialty is a matrix which can be configured based on the enrollment type.
- Billing Provider Association – The evoBrix PMIS gives providers the ability to associate to Billing providers who are pre-existing in the system. This is achieved through the Associate Billing Provider step, which becomes mandatory or optional based on the Applicant Type and Enrollment Type selection. The system gives the option to search and confirm the Billing Provider based on NPI or Provider ID type search. Providers will be able to associate to one or more Billing providers based on the Business Status of the Billing Provider.
- License/Certification/Other – The evoBrix PMIS allows the State to maintain specific policies on the credentials each provider must present to be enrolled and to be able to serve State Medicaid members. The Credentialing Matrix includes a complete list of all possible credentials and allows authorized users to define which of these credentials must be provided for each enrollment or re-enrollment activity.
- Mode of Claims Submission/EDI Exchange – Providers will be able to select their preferred method of claims submission in the Mode of Claims Submission step. This step allows providers to select submission method through EDI exchange or other methods like Paper or Direct Data Entry (DDE).
- Billing Agent Association – If the provider selects the option to submit claims through a Billing Agent, this step becomes required and the provider will need to enter at least one Billing Agent to continue with the enrollment.
- Provider Controlling Interest/Ownership Details – The evoBrix PMIS provides the ability for the provider to enter ownership details as part of the enrollment process. An owner is any individual or entity who is associated with the provider as Board of Director, Partnership, managing employee, or an entity which holds a stake in the organization. This information is sent to the screening process, as required by ACA. In addition to entering the owners into the system, the provider must also enter the relationship details between the owners, which gives the complete picture of the owners and their role in the provider enrollment.
- Taxonomy Details – Provider can enter up to 15 taxonomies into the system through this step. The taxonomy codes entered by the user are validated against the database of taxonomy. The provider taxonomies are screened against the taxonomies registered at NPPES database.
- MCO Plan Association – The evoBrix PMIS allows a network provider to associate with an MCO plan during new enrollment or modification of a provider enrollment. The provider can search and select from the list of available of network plans in the system to establish this relationship.
- 835/ERA Enrollment Form – The 835 ERA step is required for all providers who have chosen to accept 835 at the location level. By submitting this form, the user is authorizing to the setup of 835/ERA account for the enrollment EIN.
- Complete Enrollment Checklist – Additional information is collected from the providers through a set of checklist questions. Some questions pertain to whether the provider has ever submitted any false claims or ever been convicted of any criminal offenses. Based on the responses, system might require additional information from the provider
- Submit Enrollment Application for Approval – Once the provider has completed all above steps, they will be able to submit the enrollment. In this final step, the provider must accept the terms and

conditions and submit the enrollment, after which an Application ID is generated for tracking purposes.

Validate Applications

evoBrix PMIS provides real-time field level edits on each webpage that greatly reduce keying errors. Besides field level validations, the BPW provides easy to use, step-by-step processes with built-in validation and feedback to ensure complete and accurate information before submission. The wizard also displays validation error messages throughout the data entry process to account for data presence, field formatting, inter-field relationships, and completeness. evoBrix PMIS validates and ensures all enrollment steps required in the wizard are completed; providers are prohibited from submitting their application until they have passed all online validity and completeness checks for the enrollment type. These interactive messages alert the provider to conditions that need to be corrected so that validated and complete data is captured prior to submission.

Process Enrollment Applications

The evoBrix PMIS displays the business status of the provider and application status of the enrollment application in the web portal. The evoBrix PMIS tracks the application status throughout the enrollment process. Initially, enrollment application status is set as “In Process.” After the provider successfully submits the enrollment, the application will have “In Review” status and be ready to be reviewed by the enrollment staff. The provider can track the application status but cannot make modification to the enrollment data until it’s approved. If an application is denied, enrollment application status is set as “Denied” and cannot be modified further by the provider.

During the enrollment review process, the enrollment specialists can push the application back into the “In-Process” state, requesting additional supporting documentation from the providers. The system allows the providers to attach optional documentation to their enrollment application and re-submit.

Provider Enrollment Review

Provider enrollment specialists who have responsibility for processing enrollment applications submitted online, reviewing submitted applications, and rendering an approval or denial decision, or providing support to enrolling providers, use the evoBrix PMIS secure portal that provides access to the authorized operation users. Built-in security features allow evoBrix PMIS authorized users to view in-process provider applications and modifications, and to render approval and denial decisions. This allows business operations staff to track and report on the provider enrollment activities from receipt of application to final disposition.

evoBrix PMIS gives comprehensive abilities for the business user to review enrollment data for Approval/Denial or put the Application back into “In-Process” for the providers for resubmission. As shown in Figure 3.10.10-7, business users with relevant profiles can look at the list of applications that are “In-Review.”

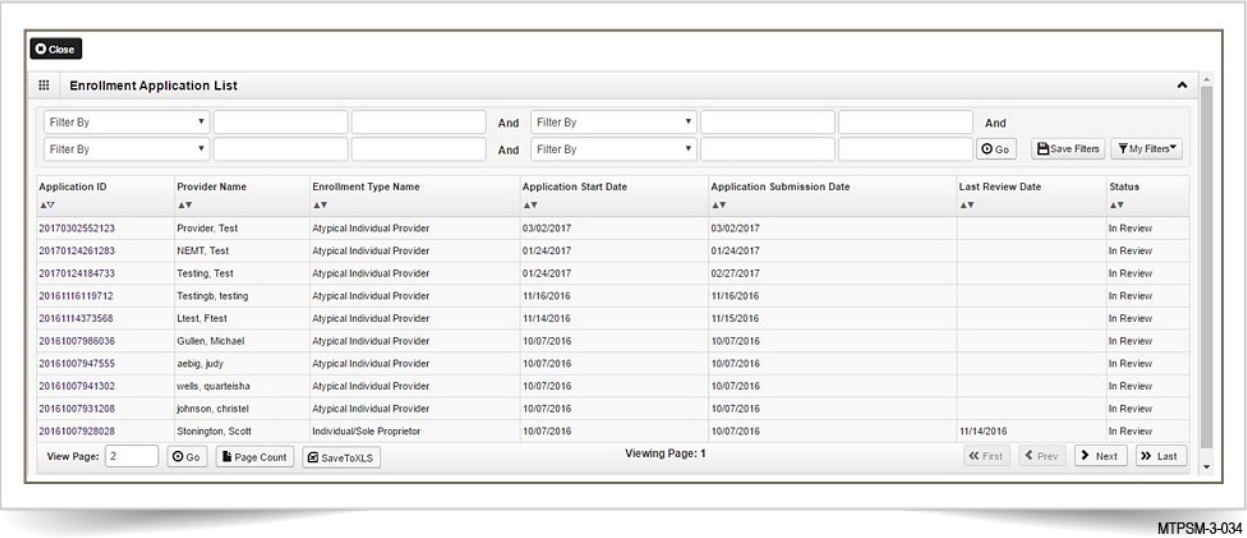


Figure 3.10.10-7. Enrollment Application List. After the enrollment is submitted the provider enrollment specialist can look at the list of applications in this screen.

Figure 3.10.10-8 shows the Enrollment Review page for a provider unit enrollment specialist to review the enrollment data and decide on application approval or denial.

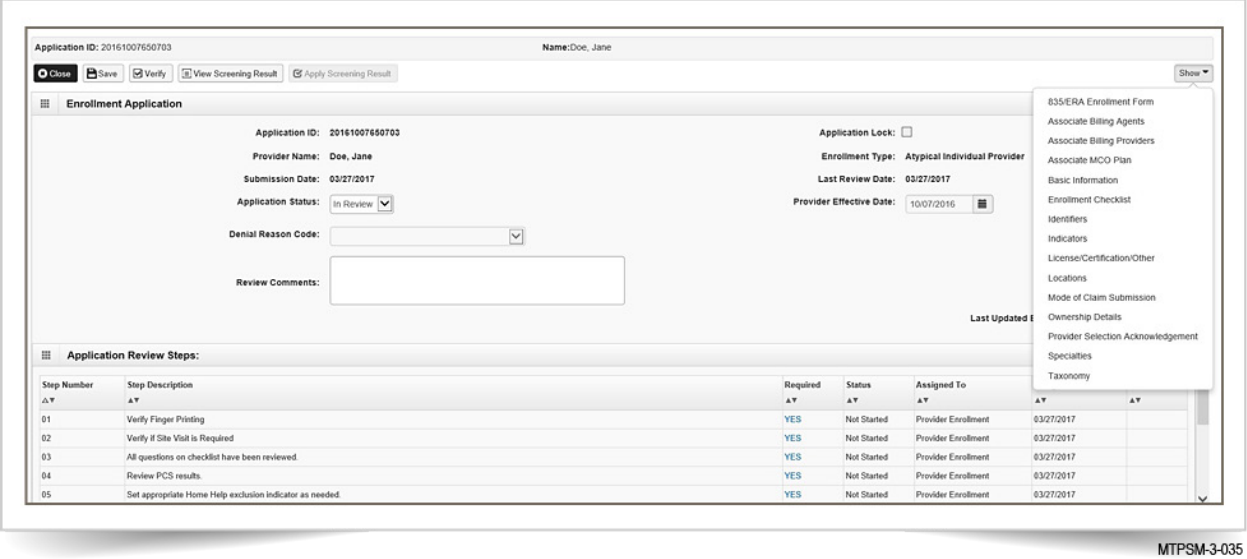


Figure 3.10.10-8. Provider Enrollment Review Page. This page allows a provider enrollment specialist to review the enrollment data and make an appropriate decision.

After a decision is made on the enrollment application, evoBrix PMIS sends an Approval or Denial letter automatically to the provider. If the provider is approved, evoBrix PMIS assigns a 7-digit Provider ID as shown in Figure 3.10.10-9 and sends a welcome letter helpful information orienting the providers to the program requirements, next steps, providing links to provider support resources. The welcome template can be configured to include additional information, such as service limitation and restriction, and relevant rules and regulations specific to the provider's provider type. If an application is denied, evoBrix PMIS will send a denial letter to the provider with the denial reason. The system can be configured to send notification to relevant Departments and programs based on State-specified rules. After the enrollment approval, the data is moved to the Manage area for further maintenance.

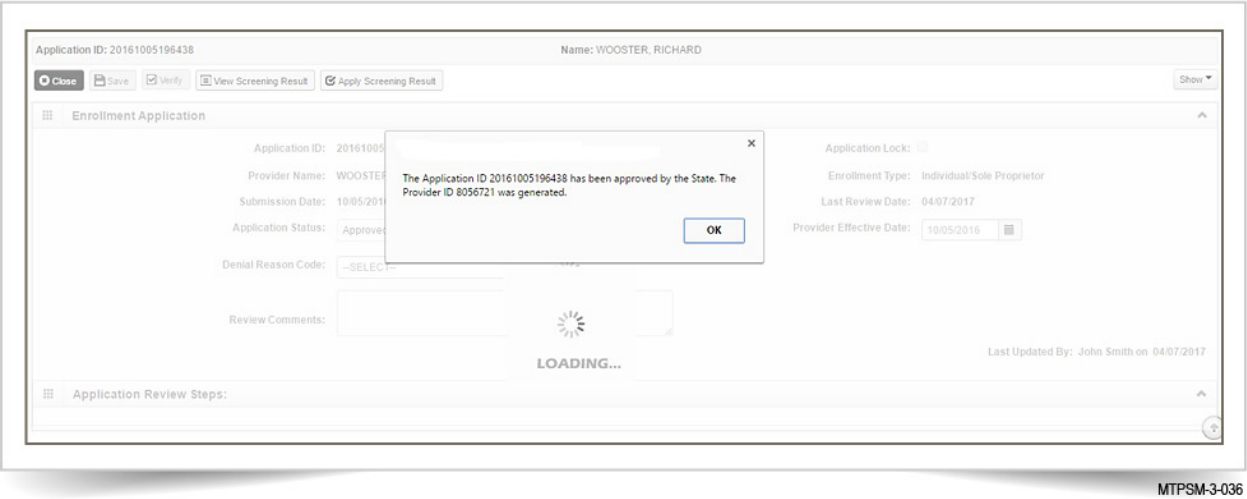


Figure 3.10.10-9. Enrollment Approval and Provider ID Generation. After the enrollment is approved, the system generates a 7-digit Provider ID for the enrollment.

Provider Screening

Team CNSI's PCS solution, in partnership with LexisNexis, provides full compliance with the ACA Provider Enrollment Screening requirements. LexisNexis provides a comprehensive solution that assists with provider enrollment and program integrity efforts enabling agencies to:

- Verify and validate the credentials of providers
- Implement robust, up-front enrollment screening for verification and risk assessment
- Screen all currently enrolled fee-for-service providers
- Monitor provider files for risk indicators between enrollment periods

Team CNSI's PCS has a web interface that provides a user-friendly GUI for viewing screening results in a tabular layout. Any screening that requires attention is flagged for provider enrollment staff so they can check for more details before taking a decision.

The Provider Information tab displays Name, SSN, NPI, EIN/TIN, Address, State, and Federal Death file records. The precision scale shows the data quality of the response received as part of the screening. Figure 3.10.10-10 displays the PCS screening results from the Provider Information tab.

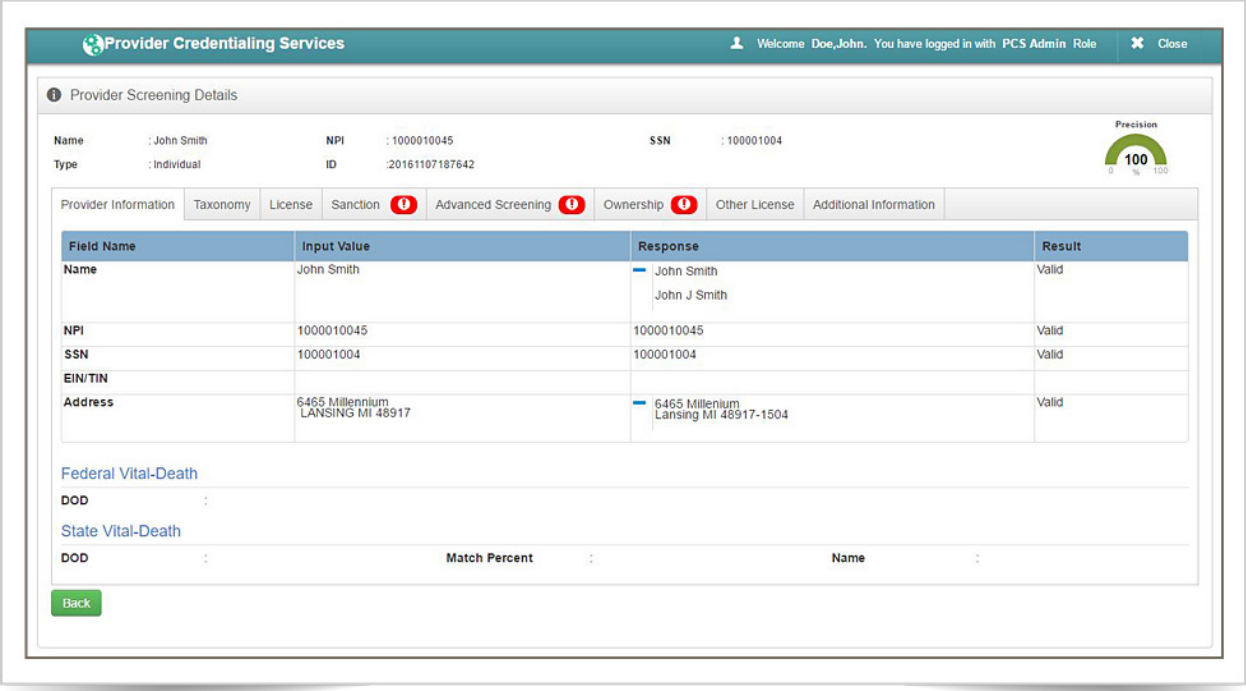


Figure 3.10.10-10. Provider Screening Details Screen. This screen shows the provider information, as part of the screening results.

As part of license screening, state professional licenses (in-state and out-of-state), DEA, CLIA, Board, and NCPDP Board certificates disclosed by the provider are screened and the results are displayed in the License tab. When the user navigates to the License tab, they can look for any invalid, expired, or suspended licenses from the screening, and use the information to make an appropriate business decision. Figure 3.10.10-11 displays PCS screening results for Licenses.

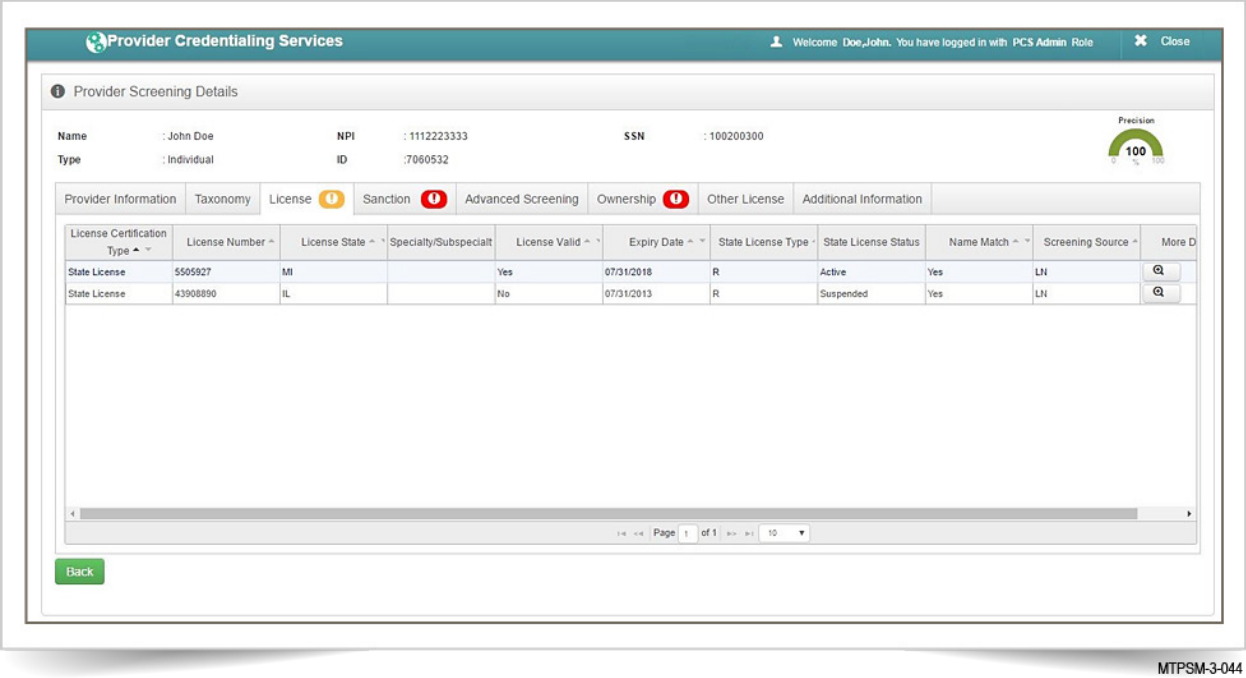
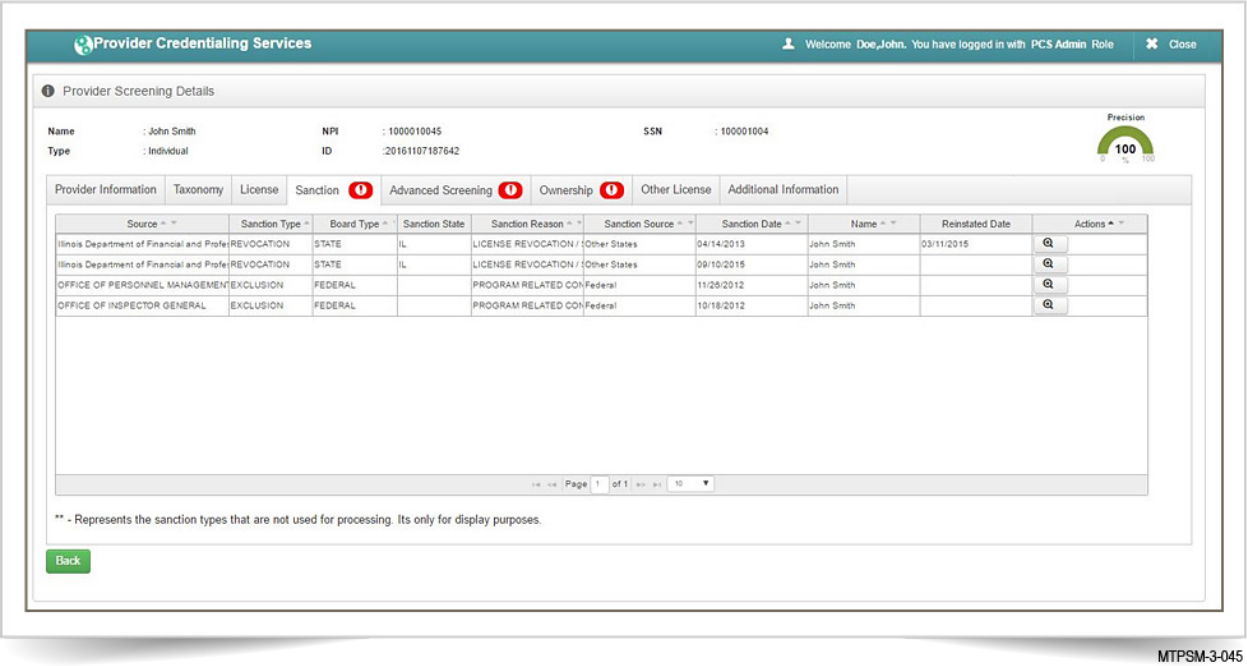


Figure 3.10.10-11. Provider Screening Details Screen - License Tab. This screen shows the provider license information, as part of the screening results.

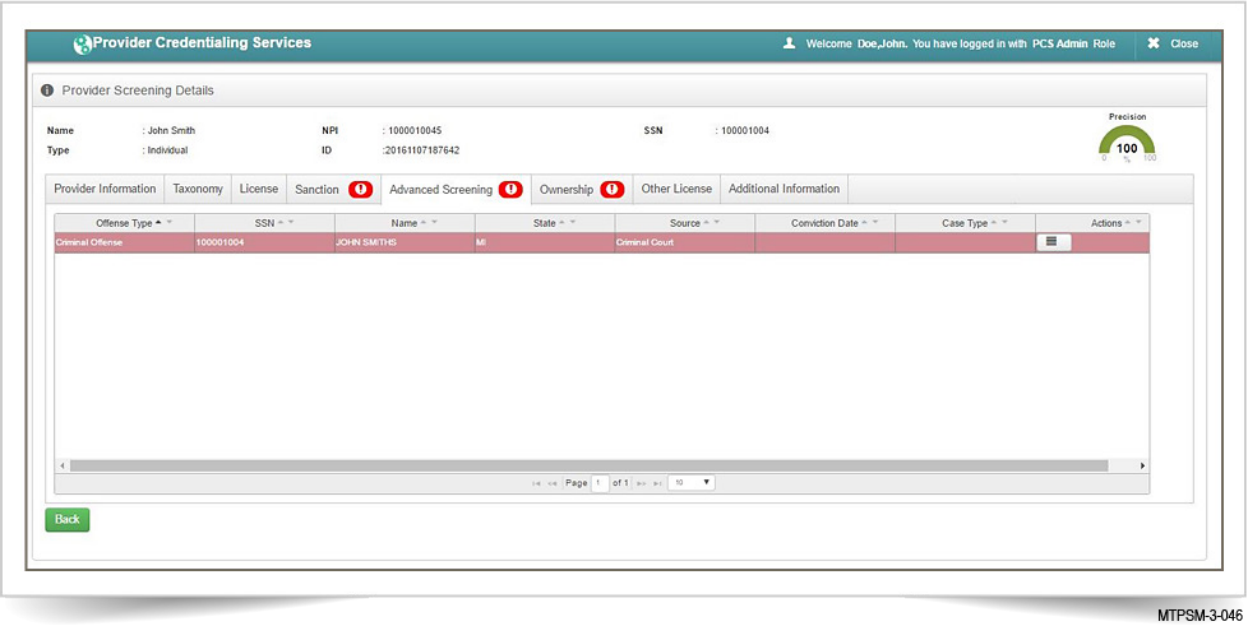
As part of CMS guidelines for State Medicaid Agencies, under ACA 42 CFR part 455.436, State Medicaid Boards are required to screen providers against the Federal Databases such as OIG (for LEIE), SAM (EPLS) and other State agencies for any exclusions at these sources. The PCS solution, in partnership with LexisNexis, screens providers against Federal databases. Additional data sources can also be plugged into the system (for example MCSIS, CMS-MED sanction files). The PCS solution also includes monthly batch screening of providers against these databases. This comprehensive screening of providers meets pre-enrollment and post-enrollment screening criteria per the CMS guidelines. Figure 3.10.10-12 displays the PCS screening results of providers against sanction databases.



MTPSM-3-045

Figure 3.10.10-12. Provider Screening Details Screen - Sanction Tab. This screen shows the sanctions on the provider, as part of the screening results.

The Advanced Screening tab displays the results of background screening for any criminal and sex offenses. This meets the 42 CFR Part 455.434 requirement to perform criminal background checks for providers against Department of Corrections, County Courts, and arrest logs for various states in the country. This information can be used by the State to perform additional checks on the providers and make appropriate decisions. Figure 3.10.10-13 shows the provider Advanced Screening information.



MTPSM-3-046

Figure 3.10.10-13. Provider Screening Details Screen - Advanced Screening Tab. This screen shows the advanced screening information for the provider.

Ownership Screening is part of the enrollment screening in PCS. Owners are also screened, along with providers, against sanction databases, state/federal death records, and criminal background records. Figure 3.10.10-14 shows the Ownership Screening information for owners.

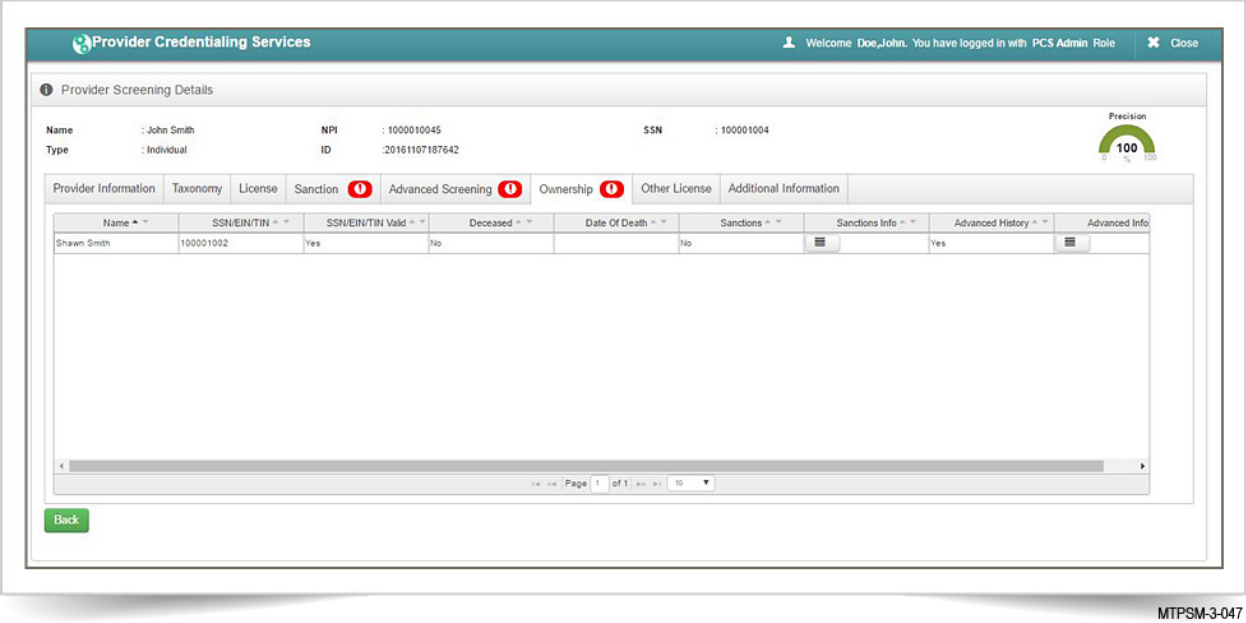


Figure 3.10.10-14. Provider Screening Details Screen - Ownership Tab. This screen displays the screening information for the owner(s).

The Other Licenses tab displays any licenses the provider has, but not disclosed as part of the enrollment. This allows the State staff to be informed of provider's other licenses, perform an inquiry and check if there were any revoked or suspended licenses in other states, and make appropriate business decisions. Figure 3.10.10-15 shows the Other Licenses of the provider.

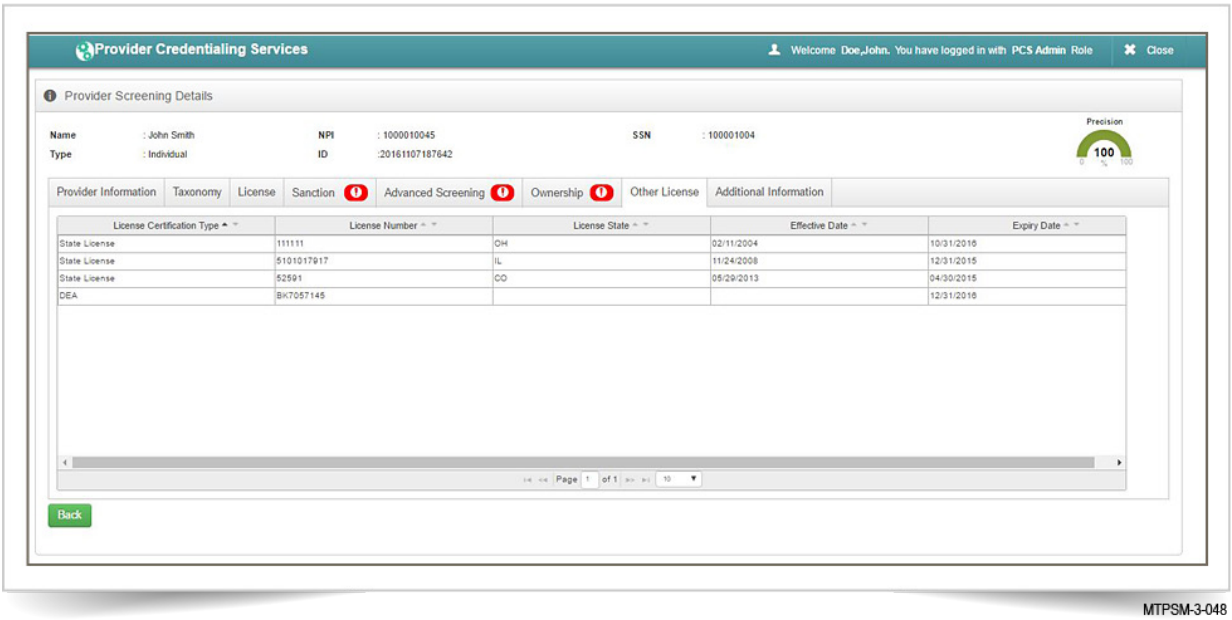


Figure 3.10.10-15. Provider Screening Details Screen - Other License Tab. This screen displays any additional licenses a provider may hold but has not disclosed during the enrollment process.

The Additional Information tab gives more information on the provider pertaining to medical schools, group affiliations, hospital affiliations, and specialties a provider may have. Figure 3.10.10-16 shows the Additional Information tab.

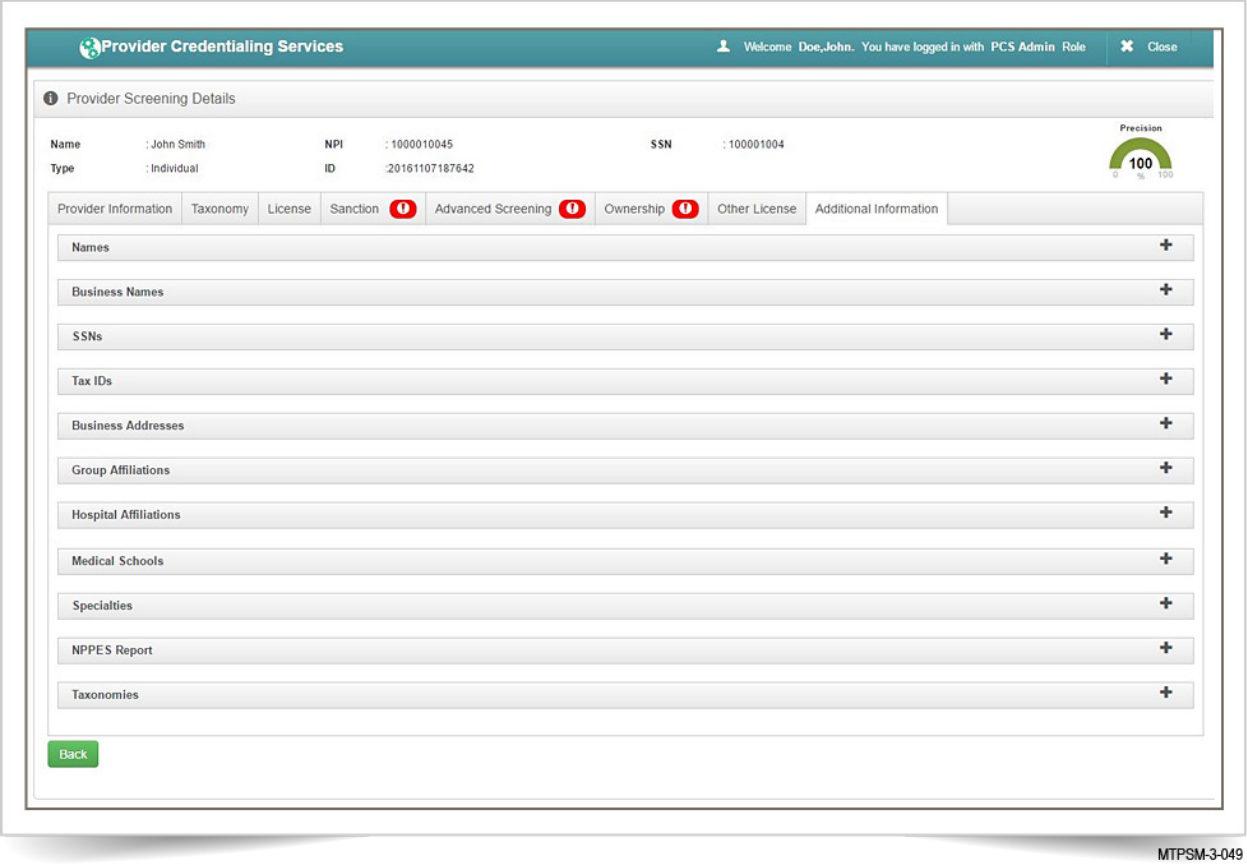
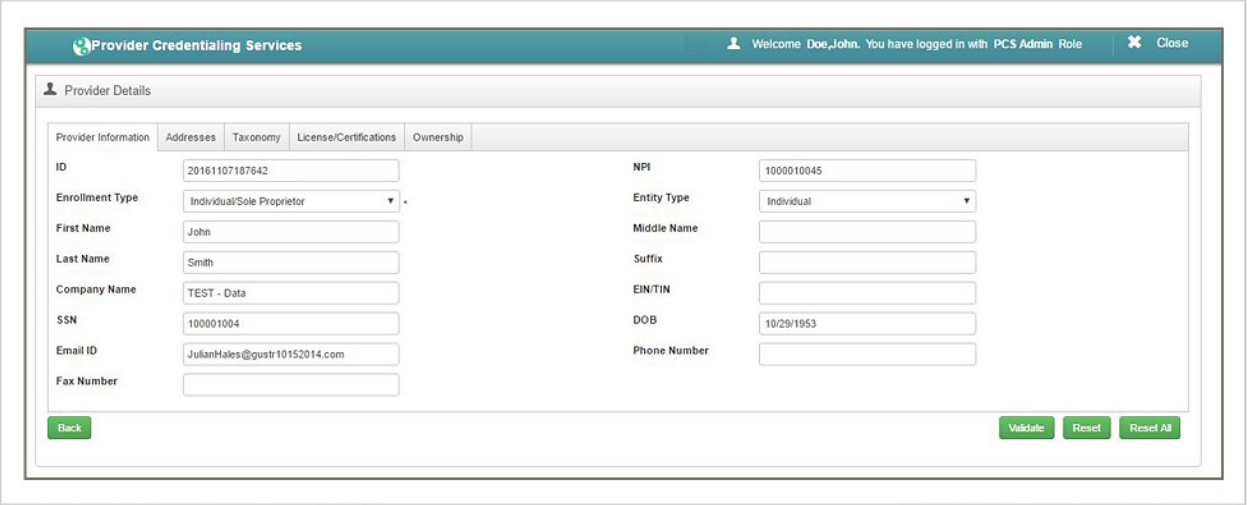


Figure 3.10.10-16. Provider Screening Details Screen - Additional Information Tab. This screen displays medical schools, group affiliations, hospital affiliations, and specialties a provider may have.

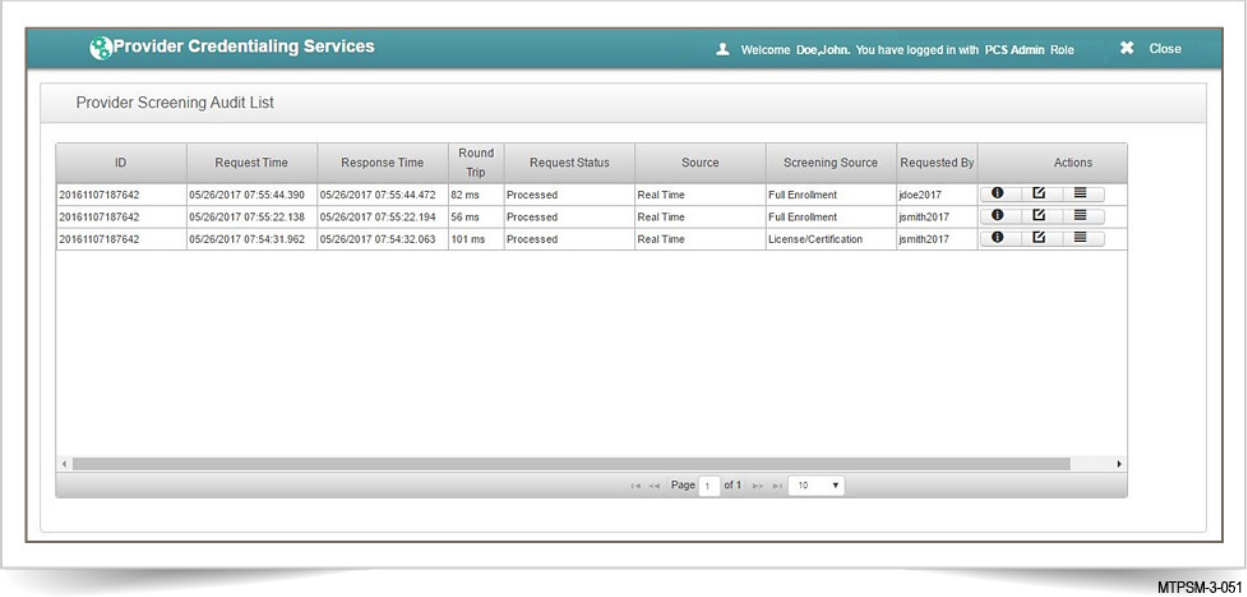
Though PCS is integrated within the evoBrix PMIS to allow real-time screening, it can also be used to perform a quick real-time check by manually entering provider and owner information. This is called On-Demand screening and State staff with appropriate privileges will be able to perform this screening. Figure 3.10.10-17 shows the On-Demand screening feature of PCS.



MTPSM-3-050

Figure 3.10.10-17. PCS On-Demand Screening Screen. This screen allows the user to perform a real-time screening of a provider by entering the provider and owner information.

Any screenings that were performed are displayed in the Audit Trail List screen. Figure 3.10.10-18 shows the audit trail screen with the history of screening done on the provider.



MTPSM-3-051

Figure 3.10.10-18. PCS Audit Trail Screen. This screen displays the history of past screenings performed on a provider.

SiteVisitPro (SVP)

Team CNSI's SVP is a portable application designed for use with tablets. The SVP application allows business operations staff to perform unannounced site visits and capture the results in real-time, eliminating the need to transfer data from paper forms. This application supports organizations in performing site visits using real-time provider information directly from the Medicaid Provider Enrollment system, eliminating redundant data entry. SVP assists in the identification of fraudulent

providers by capturing specific information about the provider's practice. SVP can be accessed from anywhere with a wireless connection.

The site visit mobile application provides a user-friendly GUI for administering, scheduling, and collecting site visit information. When a site visit admin logs into the system, the user will be presented with options to search, review site visit results, or view the site via Google Maps.

As a part of scheduling a site visit, the admin user can search for a specific provider using provider NPI, specialties, location, tax ID, or risk level, and after a successful search, the user can assign it to a processor. Figure 3.10.10-19 shows the provider search screen available to the admin.

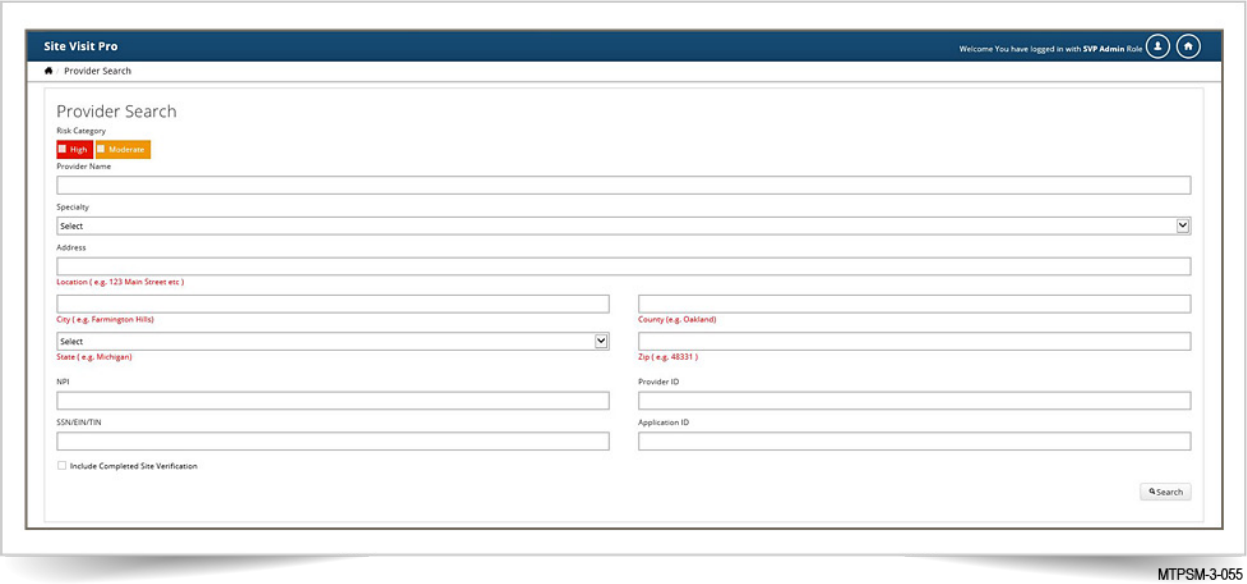


Figure 3.10.10-19. SiteVisitPro - Provider Search Screen for the Admin User. Admin users can search for providers by provider NPI, specialties, location, tax ID, or risk level.

The other major functionality for the admin is to search for scheduled site visits. The admin can also reassign a previously assigned site visit to a different processor to balance work load among multiple processors. Figure 3.10.10-20 shows the admin capability to reassign the site visit to a different processor.

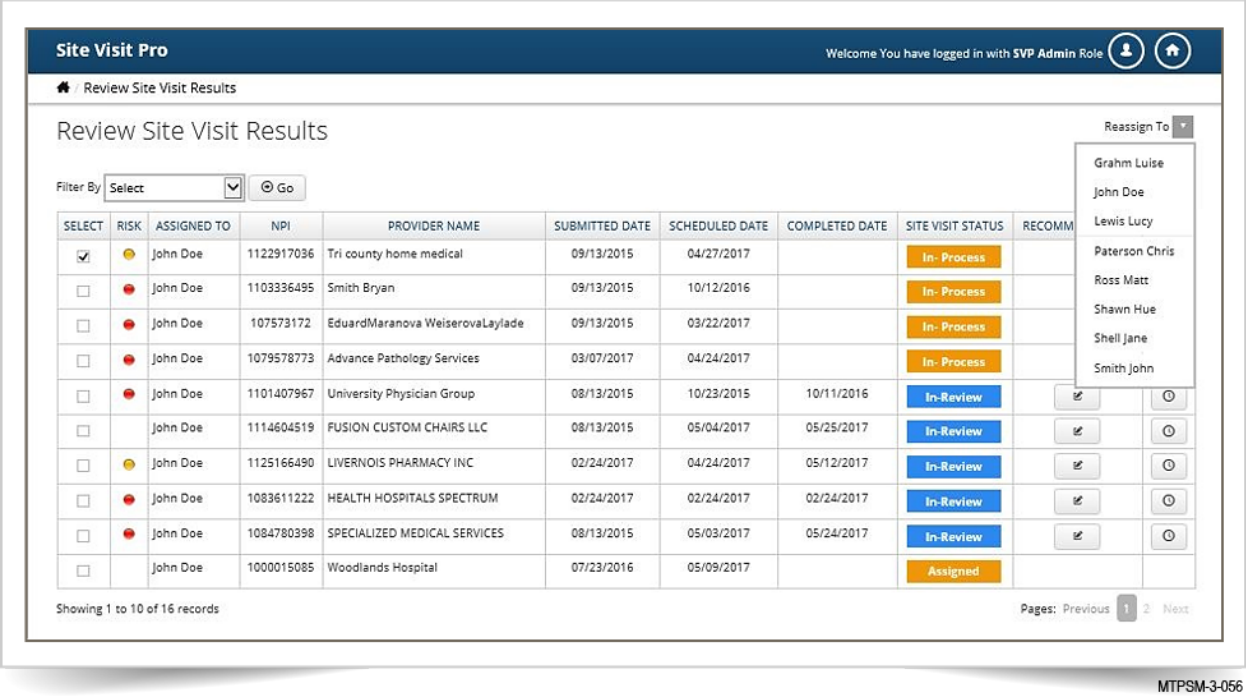


Figure 3.10.10-20. Review Site Visit Results Page. Admin can search for scheduled site visits and, once presented with the results through this screen, can reassign a scheduled site visit to a different processor.

The admin can view the site visit details of a provider including basic information, site visit details, and additional information. All this information is used by the admin to determine the outcome of the site visit, as shown in Figure 3.10.10-21.

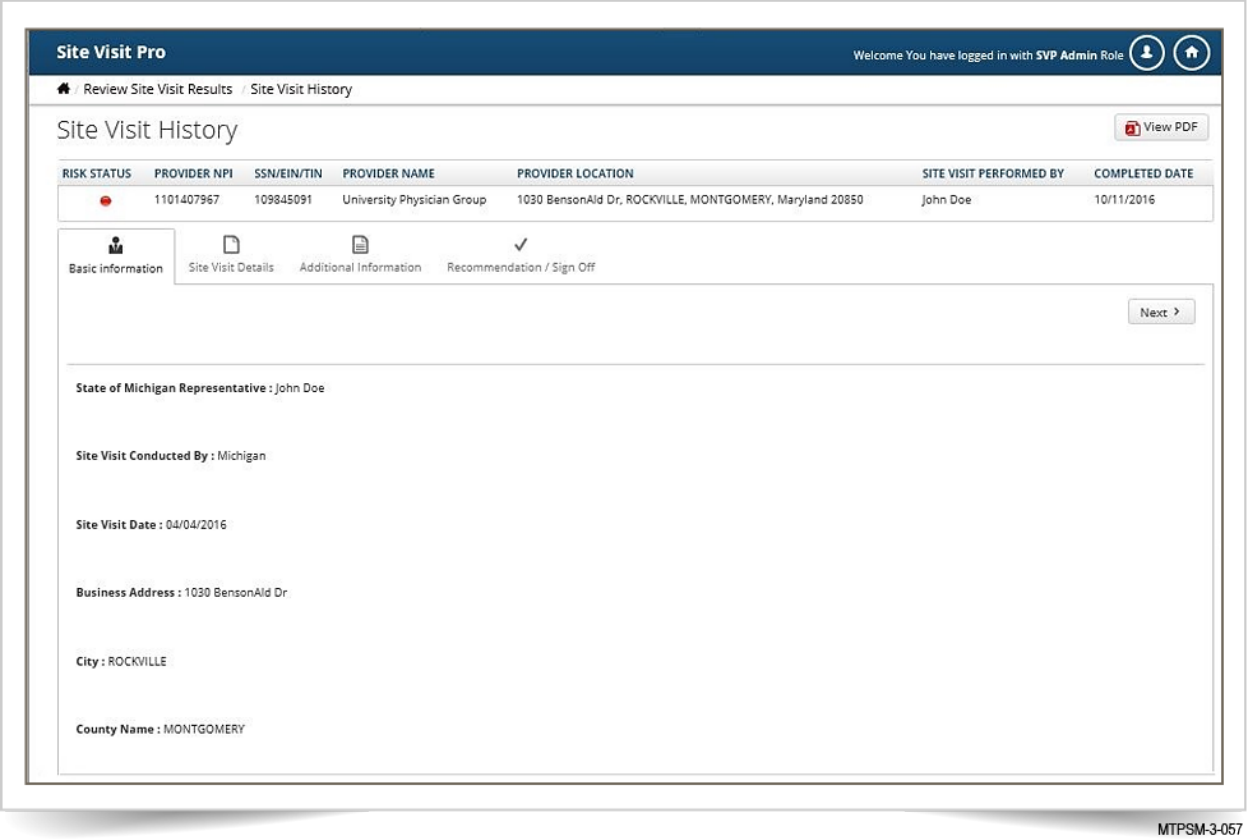
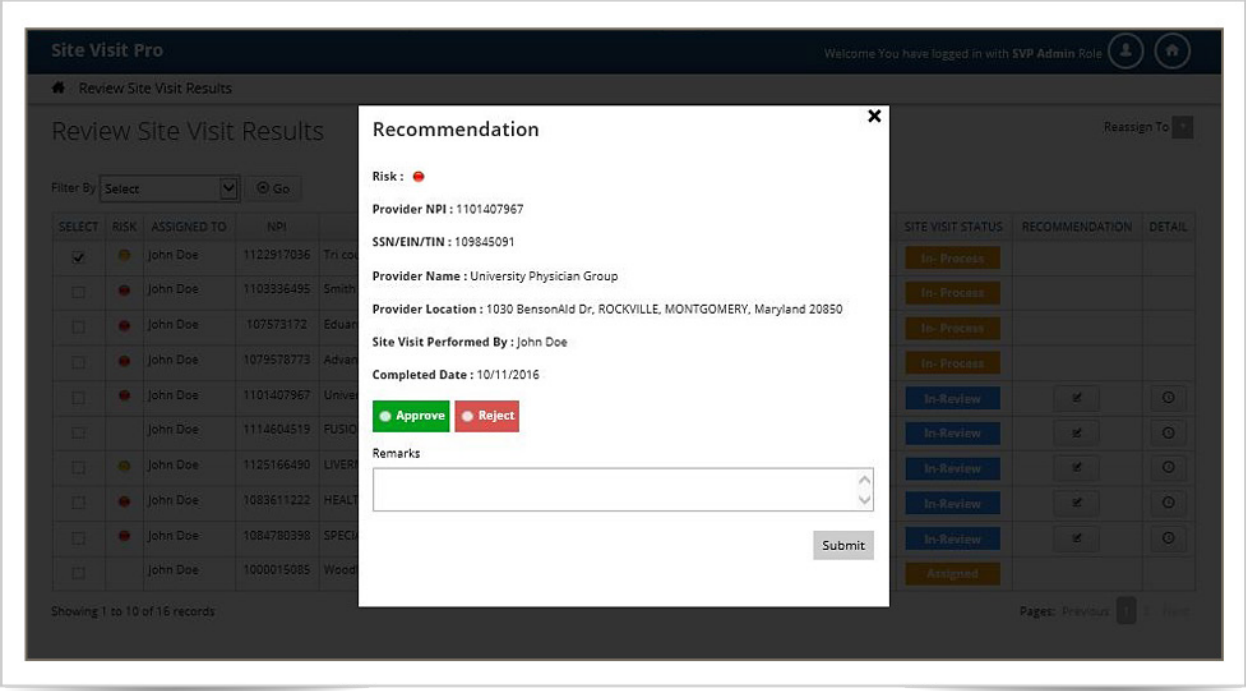


Figure 3.10.10-21. Site Visit History Page. Allows an admin to view the details of a specific site visit.

After reviewing all the details, the admin can now either approve or reject the site visit of the provider, as shown in Figure 3.10.10-22.



MTPSM-3-058

Figure 3.10.10-22. Site Visit Recommendation Page. After reviewing the details of a specific site visit, the admin can then either approve or reject the same.

The other major profile for the site visit application is the SiteVisitProcessor who conducts the site visit at the location. The application has an embedded calendar which the processor can use to look for all the site visits scheduled for a month. Figure 3.10.10-23 shows the calendar for the processor for all the scheduled site visits.

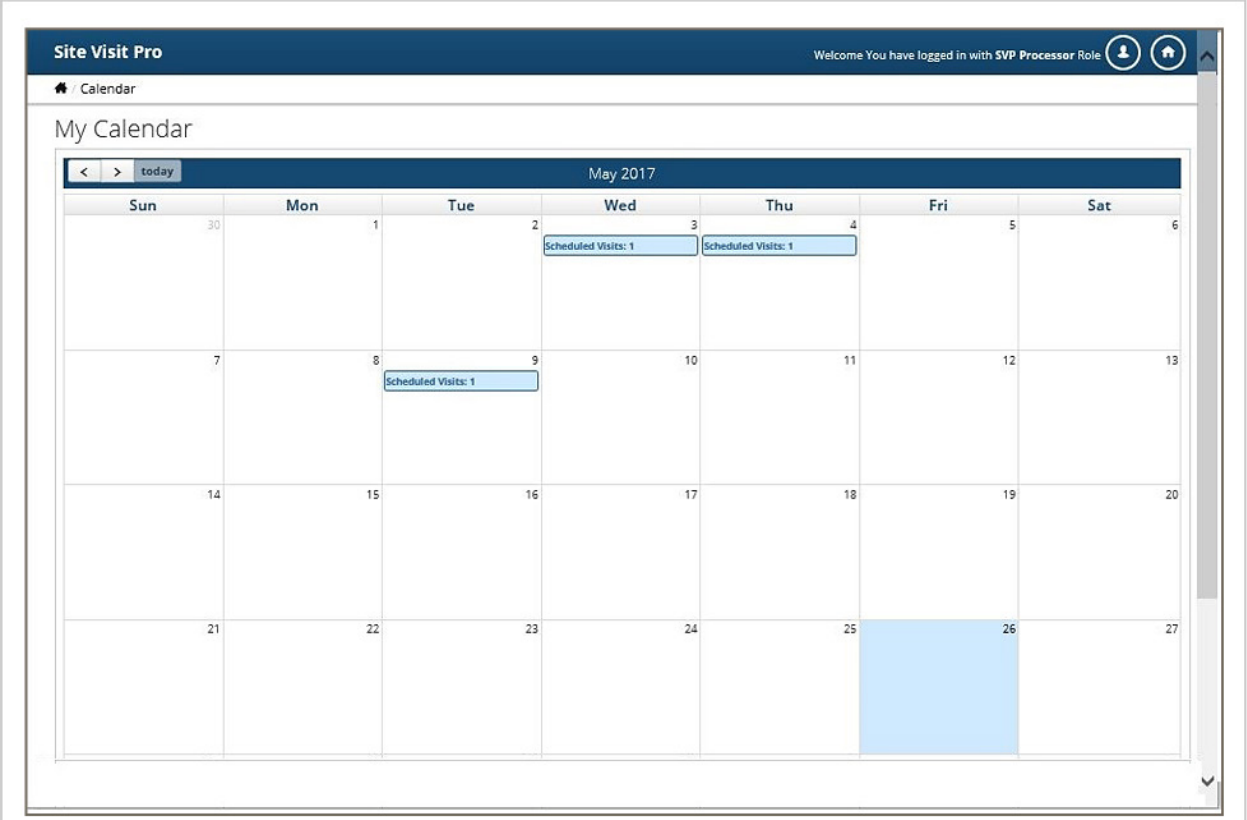


Figure 3.10.10-23. Site Visit Calendar Page, for Processors. This page displays the calendar of site visits for the logged in processor.

The processor can look at the site visit screenings that are assigned to him/her and plan accordingly. This screen provides the processor the capability to add additional site visits to the calendar, complete any in-process site visit or use the maps for directions to the destination. Figure 3.10.10-24 displays the site visit screenings of the processor and their statuses.

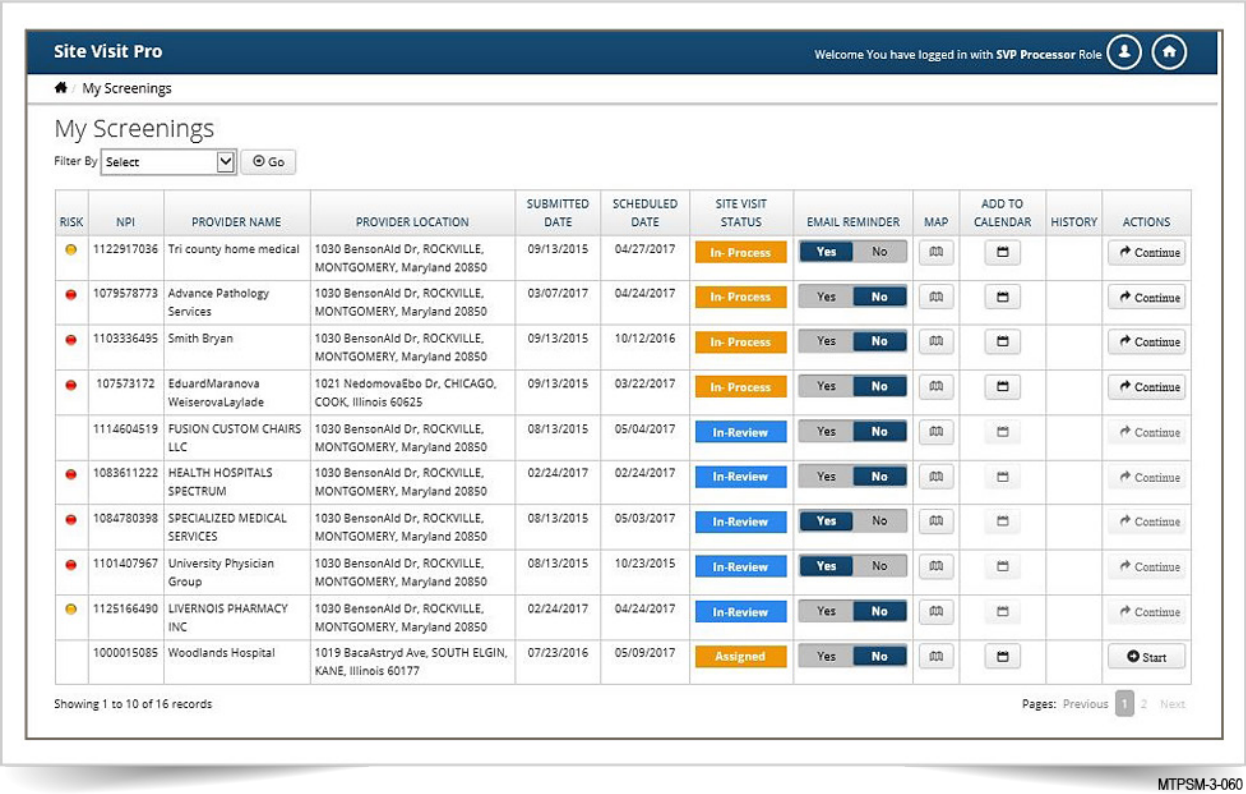


Figure 3.10.10-24. Site Visit Screenings Page, for Processors. This page displays the screenings scheduled for the logged-in processor.

As part of the site visit at the location, the processor collects basic information of the provider such as name, address, and whether a site visit was conducted by other State or PECOS already, as shown Figure 3.10.10-25.

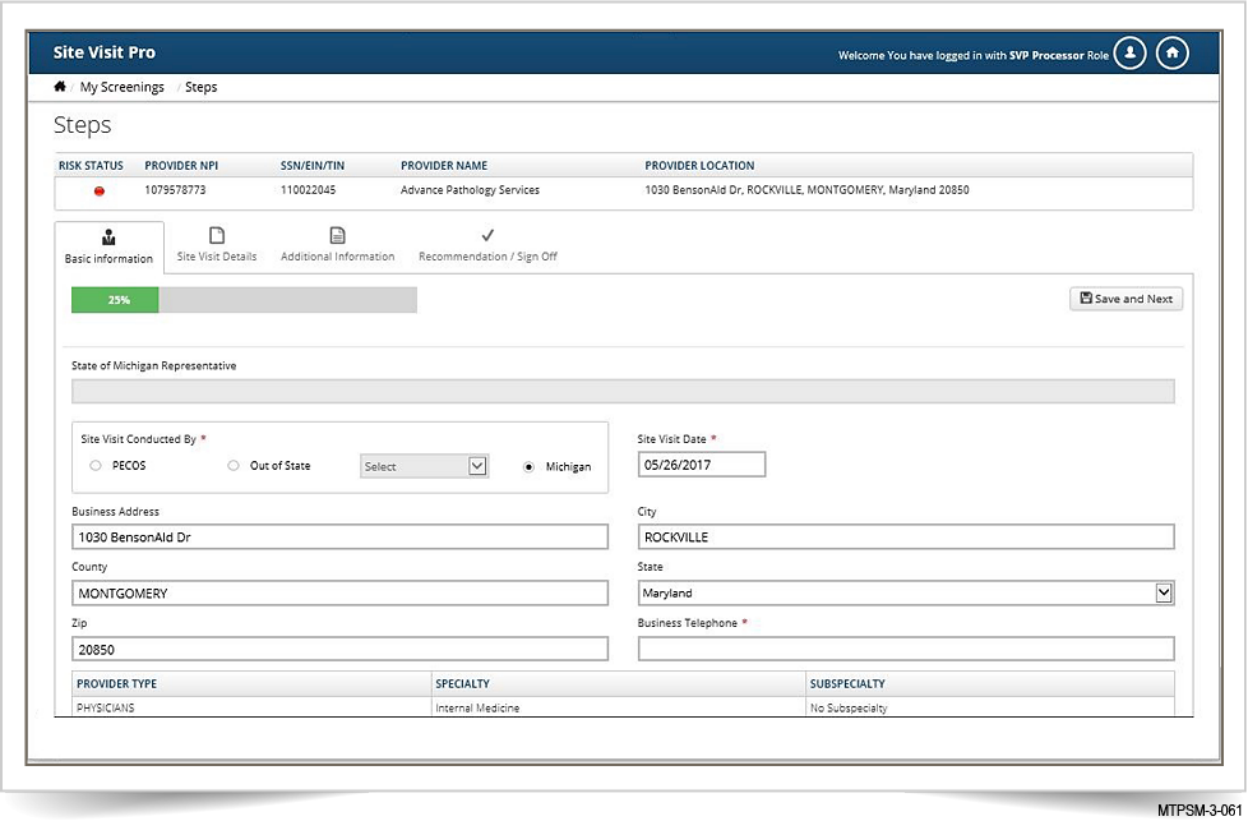


Figure 3.10.10-25. Site Visit - Basic Information Screen. This page allows the processor to capture basic information about the provider during the site visit.

The processor collects site visit details, recording the contact details, date and time of the site visit, and other additional questions pertaining to the site visit, as shown in Figure 3.10.10-26.

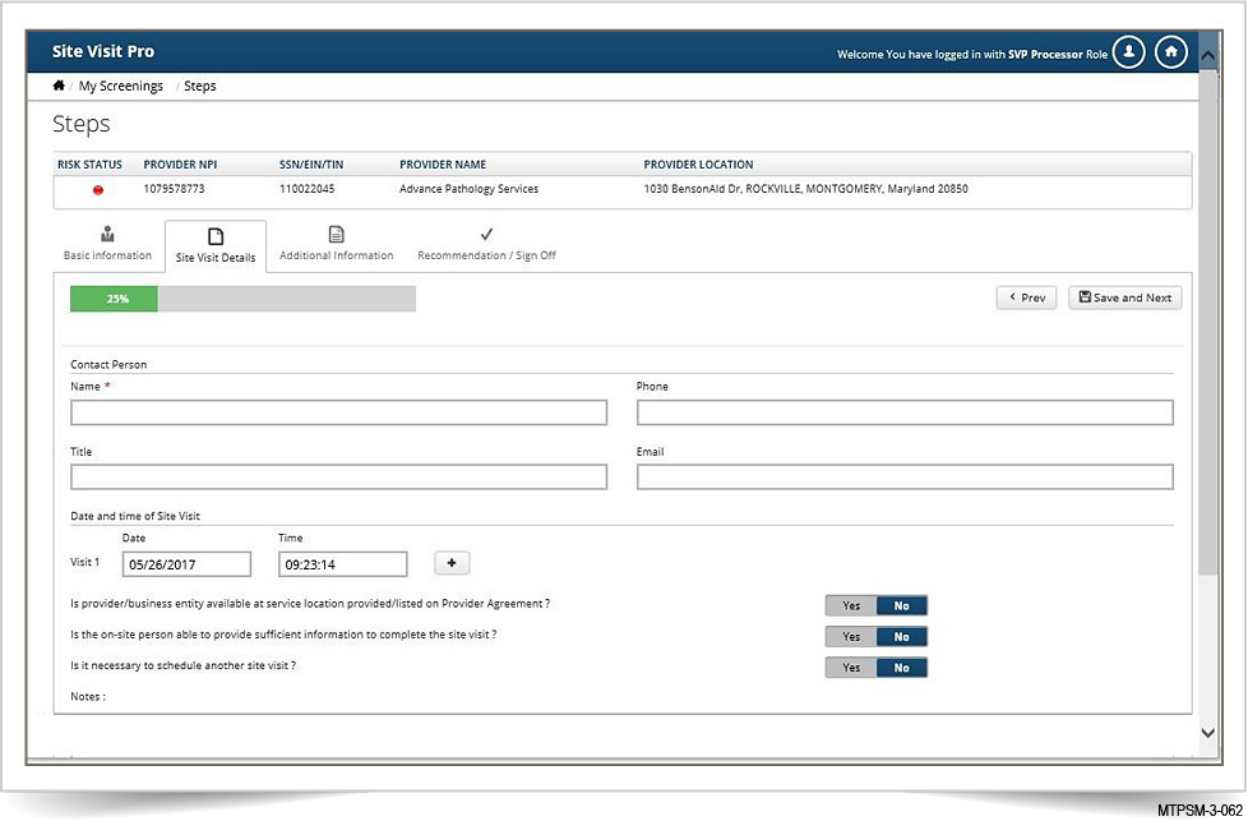


Figure 3.10.10-26. Site Visit Details Screen. This page allows the processor to record the date and time of the site visit, along with contact details.

Then the processor collects additional information and offers his/her recommendation, which is sent to the admin for approval, as shown in Figure 3.10.10-27.

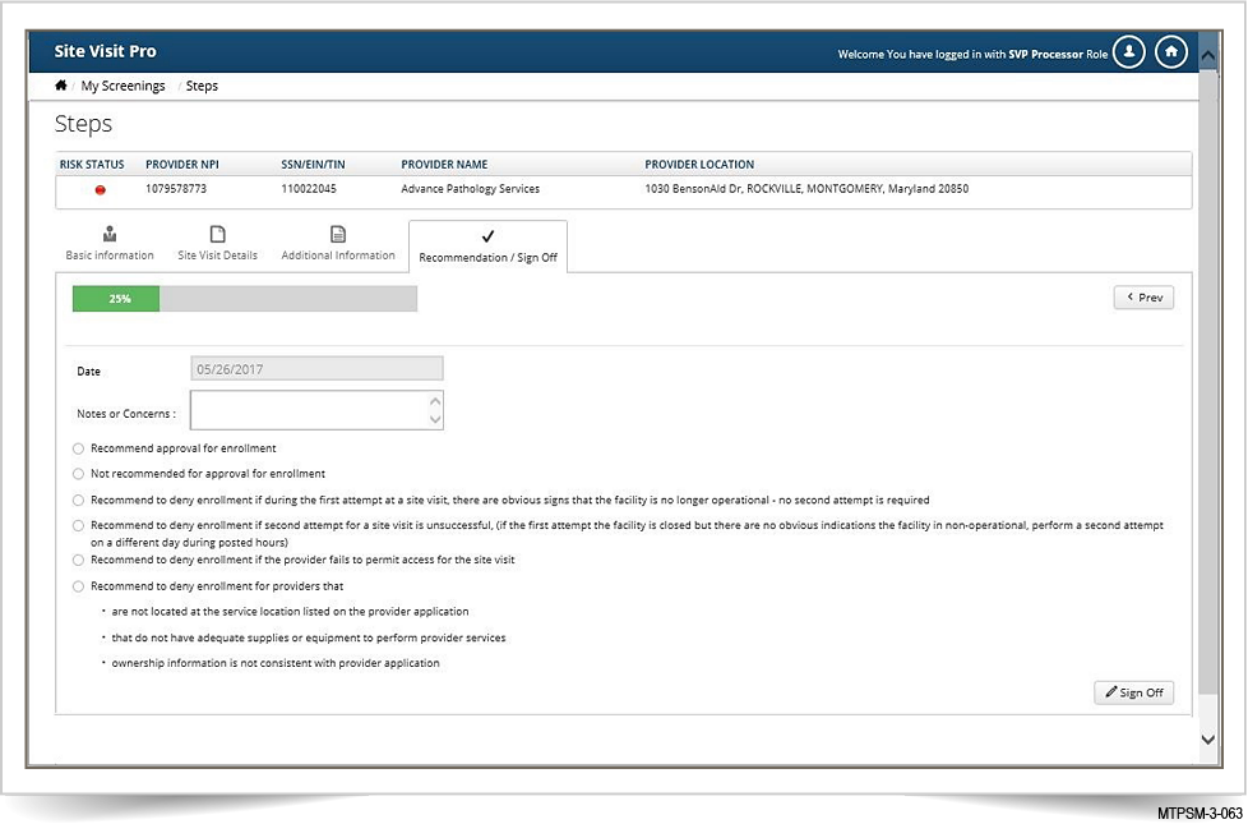


Figure 3.10.10-27. Site Visit Recommendation Screen. This page allows the processor to record their recommendation following the site visit.

ENR01

The Contractor's solution shall provide a unique submitter number for each billing service or submitter that transmits HIPAA X12 transactions with the State for single or multiple providers.

The evoBrix PMIS allows users to establish trading partners in conformance with HIPAA standards. All submitters of EDI transactions will be given a unique Trading Partner Identifier (TP ID). Prior to allowing electronic claim submission capability, providers must submit test claims in accordance with HIPAA and State guidelines using their TP ID in the EDI test environment. Once the testing is completed and compliant with State implementation guidelines, the transaction mode of submission for that submitter will be marked for production submission.

ENR02

The Contractor's solution shall receive provider applications through a web based provider self-service tool and on paper. The solution shall allow for the enrollment, re-enrollment, termination, recertification, or revalidation of providers and provide real-time notification to the providers of the receipt of the enrollment application.

Team CNSI's evoBrix PMIS includes a full-featured, self-service Provider Portal that supports the provider enrollment function to process submissions by prospective and current providers for DPHHS

enrollments and revalidations. evoBrix PMIS offers full support for provider enrollment, re-enrollment, termination, revalidation, and screening functions. The evoBrix PMIS solution allows authorized State users to manually enter the enrollment information received through paper.

Provider screening processes are supported by Team CNSI's PCS solution, in partnership with LexisNexis, which provides full compliance with the ACA Provider Enrollment Screening requirements. To ensure that only qualified providers and suppliers remain in the Medicaid program and meet ACA compliance, the evoBrix PMIS performs a monthly screening to determine if providers and suppliers remain in compliance with State licensure requirements. The ability to remain enrolled in the system is linked to the renewal of each provider's license. If the provider does not respond within the pre-configured timeframe, the provider's eligibility is end-dated in the system with the expiration date of the license and will not be renewed until the provider has renewed his/her license.

The evoBrix PMIS solution offers a streamlined, configurable process for automated provider revalidation according to State requirements. evoBrix PMIS sends automated revalidation notices based configurable business rules to begin the revalidation process for each provider. The providers will have at least 30 days (configurable option) from the date of their revalidation letter to complete the revalidation process. The providers are required to revalidate all the steps in the enrollment by completing each step that are listed in the BPW screen.

The evoBrix PMIS also sends automated revalidation reminder notices for each provider 15 days prior to the due date. evoBrix PMIS terminates enrollments automatically and sends termination notices for the providers who do not complete revalidation within 30 days. The 30-day revalidation period and 15-day reminder notice period are configurable based on DPHHS policy. evoBrix PMIS provides ability to configure a five-year revalidation interval by Risk Category (High, Moderate, and Low) or by Provider Type/Specialty.

ENR03

The Contractor's solution shall use automated screening and monitoring processes and tools to verify provider enrollment and eligibility based on Federal requirements contained in 42 CFR 455.436 (e.g., CMS data matching for provider screening and monitoring, Social Security Administration's Death Master File, the National Plan and Provider Enumeration System (NPPES), the List of Excluded Individuals/Entities (LEIE), the Excluded Parties List System (EPLS)).

Team CNSI's PCS solution is comprised of pre- and post-enrollment screening processes using LexisNexis credentialing service. The key goal of these screenings is to ensure that the provider is actively functioning and servicing patients at the reported location, and, in turn, reduce the chance of fraud, waste, or abuse. The screening applies to:

- New providers enrolling for the first time
- Providers reenrolling due to a change of ownership
- Existing providers revalidating their enrollment

All providers are assigned to one of the risk categories: High, Moderate, or Limited. Prior to completing enrollment processing, providers are subject to screening tasks based on their risk category. Depending on the provider's type and specialty, the screening requirements include:

- Validation of disclosed individuals with the OIG Excluded Individuals database, the Excluded Parties List System (EPLS) and the Social Security Death Master List.

- In-state and out-of-state professional license verification.
- Clinical Laboratory Improvement Amendments (CLIA) and Drug Enforcement Administration (DEA) Certification verification.
- Proof of Medicare enrollment, if Medicare-enrolled.
- Validation of the NPI with the National Plan and Provider Enumeration System (NPPES).
- All providers classified as "High" and "Moderate" are subject to unscheduled and unannounced site visits. Periodic site visits are also required when existing providers re-validate their information with the timing based on the risk categorization.

Pre-enrollment screening results are available in real time for the provider enrollment specialist to review and make appropriate decisions regarding whether to approve or deny the enrollment application.

ENR04

The Contractor's solution shall allow entities enrolling as trading partners with the State's healthcare programs to select the HIPAA X12 transactions they choose to submit and receive.

The evoBrix PMIS allows users to establish trading partners in conformance with HIPAA standards. All submitters of EDI transactions including electronic claims will need to enroll as a Trading Partner and can select the HIPAA X12 transactions they choose to submit and receive.

Providers will be able to select their preferred method of claims submission in the Mode of Claims Submission step during the enrollment process as shown in Figure 3.10.10-28. This enrollment step allows providers to select the submission method through EDI exchange or other methods like Paper or Direct Data Entry (DDE).

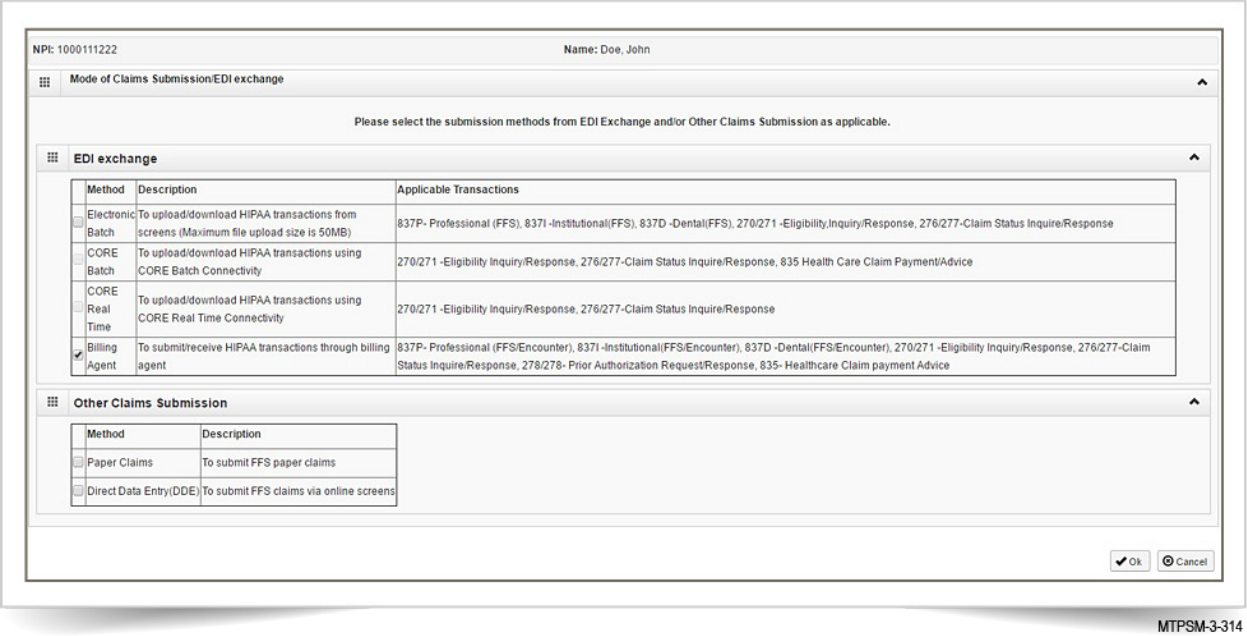


Figure 3.10.10-28. Mode of Claim Submission. Providers can select one more methods of claims submission in the system.

ENR05

The Contractor's solution shall assign a unique provider ID for all providers including atypical providers, for use in transactions with the enterprise.

The evoBrix PMIS has a built-in feature for automatic assignment of Provider ID for all enrollments. The Provider ID will be used as Atypical Provider Identifier (API) for providers who are not eligible for NPIs.

ENR06

The Contractor's solution shall prompt users in the event of data entry errors, missing data or inconsistencies in the provider enrollment, maintenance, or revalidation process.

The evoBrix PMIS provides real-time field level edits on each webpage that greatly reduce keying errors. Besides field level validations, the BPW provides easy to use, step-by-step processes with built-in validation and feedback to ensure complete and accurate information before submission of new enrollments or enrollment modifications. The wizard also displays validation error messages throughout the data entry process to account for data presence, field formatting, inter-field relationships, and completeness. The evoBrix PMIS validates and ensures all enrollment steps required in the wizard are completed; providers are prohibited from submitting their application until they have passed all online validity and completeness checks for the enrollment type. These interactive messages alert the provider to conditions that need to be corrected so that validated and complete data is captured prior to submission.

ENR07

The Contractor's solution shall allow enrolling providers to enroll in one or more program types (e.g., Care Management, waiver, CHIP, Standard Medicaid) using a single enrollment event.

As part of the enrollment process, providers may enroll to serve specific State programs as long as they meet the appropriate credentialing criteria. The evoBrix PMIS solutions provides ability for enrolling providers to associate with one or more programs in a single enrollment.

ENR08

The Contractor's solution shall have configurable business rules to suspend or restrict the enrollment of providers, trading partners or clinics affiliated with individuals debarred by State or Federal agencies, listed in Registries (e.g., Child Abuse, Elder/Adult Abuse, Sex Offender), or do not meet requirements specified by the State.

As part of CMS guidelines for State Medicaid Agencies, under ACA 42 CFR part 455.436, State Medicaid Boards are required to screen providers against the Federal Databases such as OIG (for LEIE), SAM (EPLS) and other State agencies for any exclusions at these sources. The PCS solution, in partnership with LexisNexis, screens providers against Federal databases. Additional data sources can also be plugged into the system (for example MCSIS, CMS-MED sanction files).

PCS also comes with the capability to perform background screening for any criminal and sex offenses. This meets the 42 CFR Part 455.434 requirement to perform criminal background checks for providers

against Department of Corrections, County Courts, and arrest logs for various states in the country. This information can be used by the State to perform additional checks on the providers and make appropriate decisions.

The evoBrix PMIS solution has built-in configurable rules, that are driven by the PCS screening outcome, to either suspend or restrict the enrollment of providers, trading partners or clinics.

ENR09

For enrolling and actively enrolled providers electing to participate in specific programs, the Contractor's solution shall collect and maintain the supporting data (e.g., geographic locations, number of preferred assigned members, and capacity to accept additional members), present the program agreement/contract for review, and acceptance (i.e., digital signature).

The evoBrix PMIS BPW uses State-specific rules to designate enrollment steps as required or optional dynamically depending on data entered by the provider for a given enrollment type based upon the configurable Permission Matrix and Credentialing Matrix. This feature can be leveraged to collect program specific supporting data and to present program specific agreement/contract for review and acceptance during the final enrollment submission step.

The evoBrix PMIS collects and maintains various supporting data from providers including their geographic locations, number of preferred assigned members, and capacity to accept additional members as shown in Figure 3.10.10-29.

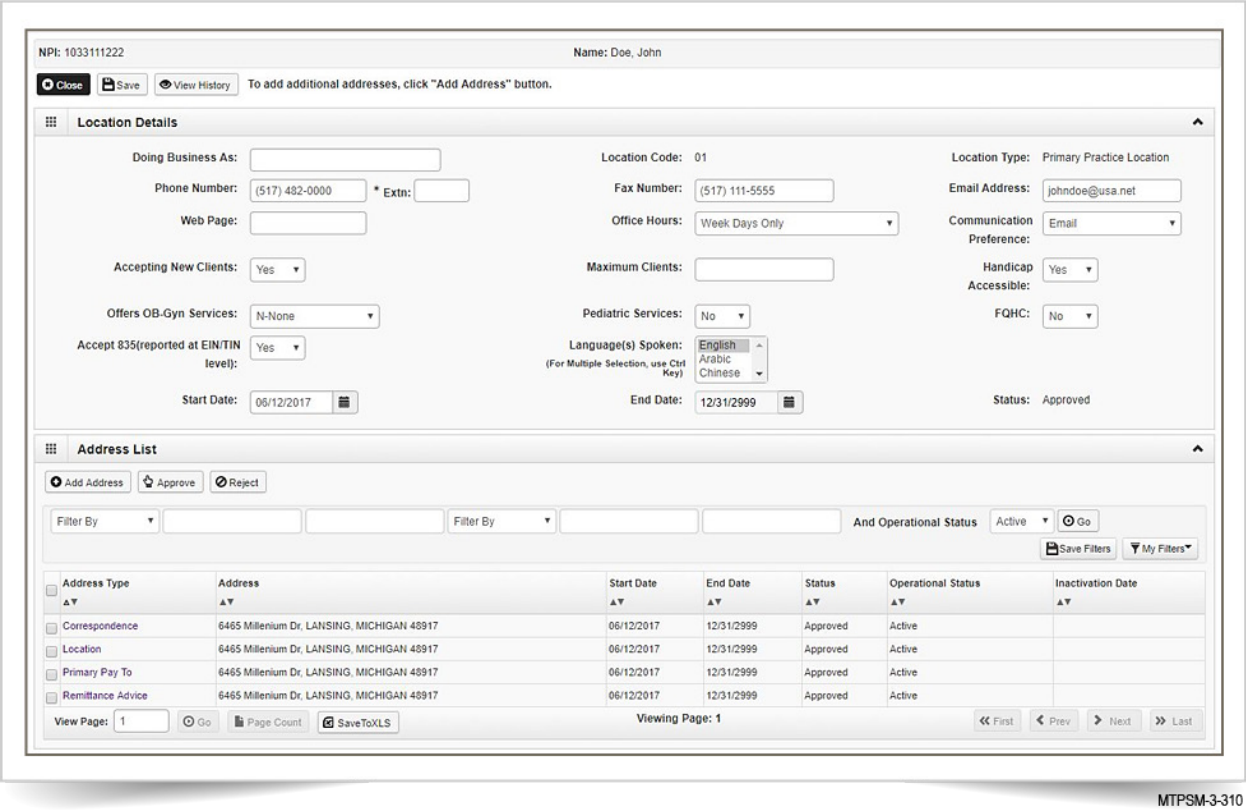


Figure 3.10.10-29. Location Details Screen. Providers enter their location details, whether they are accepting new clients and their capacity through this screen.

ENR10

The Contractor's solution shall be configurable to allow or prevent provider enrollment based on provider characteristics.

The evoBrix PMIS solution is configurable to allow or prevent provider enrollment based on provider characteristics such as provider type, provider specialty, or a finding during the initial screening process (e.g., when the enrolling provider is discovered on a federal or state exclusion list). The evoBrix PCS solution sets the indicators on a provider based on the screening results, which will prevent that provider from getting successfully enrolled in the system.

ENR11

The Contractor's solution shall prevent the creation of duplicate records during enrollment application submission.

The evoBrix PMIS centralized database eliminates duplicate enrollments using a single master record to contain all relationships the provider may have with the State. Even if a provider has multiple provider types, evoBrix PMIS retains the information under a single enrollment that is permanently linked to the provider's unique NPI and Taxpayer Identification Number (TIN) combination.

The evoBrix PMIS editing functionality performs the following validations to ensure data integrity before the provider basic information can be accepted and saved.

- NPI Validation. evoBrix PMIS verifies against NPPES database to make sure the NPI, provider name, and provider entity type entered match to the data registered with NPPES.
- Duplicate Check. evoBrix PMIS verifies the entered data against the enrolled providers in the system to ensure that the NPI is not already associated with a previously enrolled provider.

ENR12

The Contractor's solution shall allow a provider to use a single enrollment application for multiple programs, specialties or service types.

The evoBrix PMIS allows a provider to choose multiple programs, specialties, or service types in a single enrollment as shown in Figure 3.10.10-30, Figure 3.10.10-31, and Figure 3.10.10-32 below.

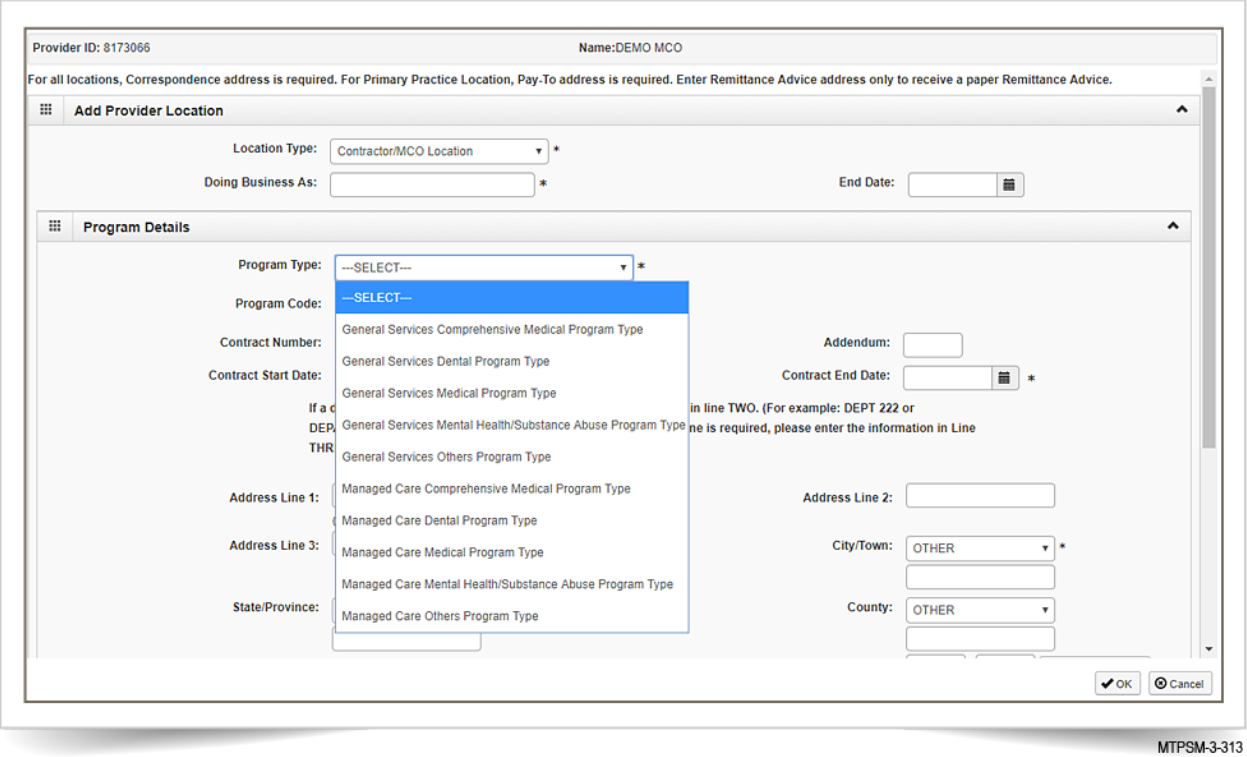


Figure 3.10.10-30. Program Details Screen. Providers can enter multiple programs during enrollment as shown.

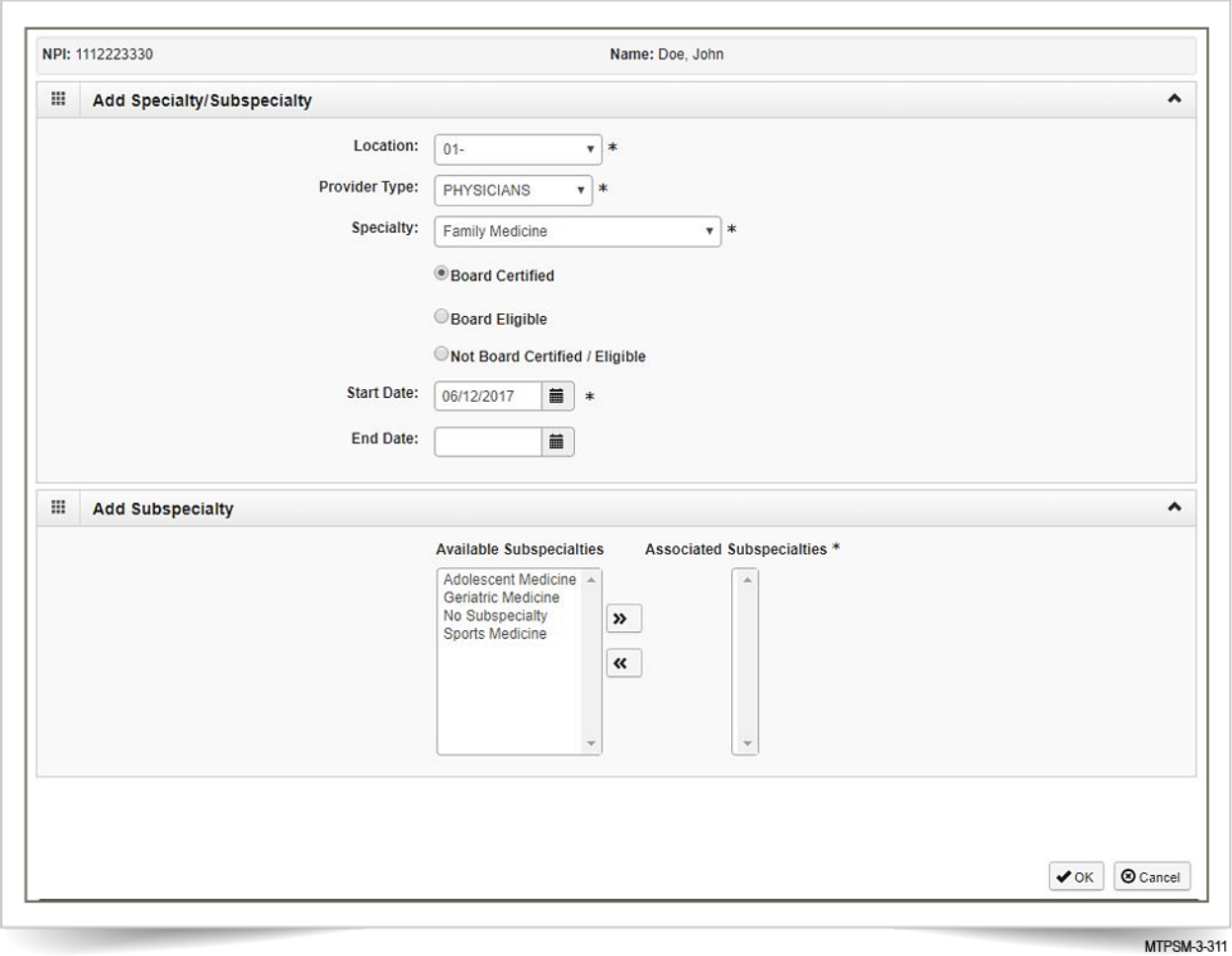


Figure 3.10.10-31. Add Specialty/Subspecialty Screen. Providers can enter multiple specialties during enrollment as shown.

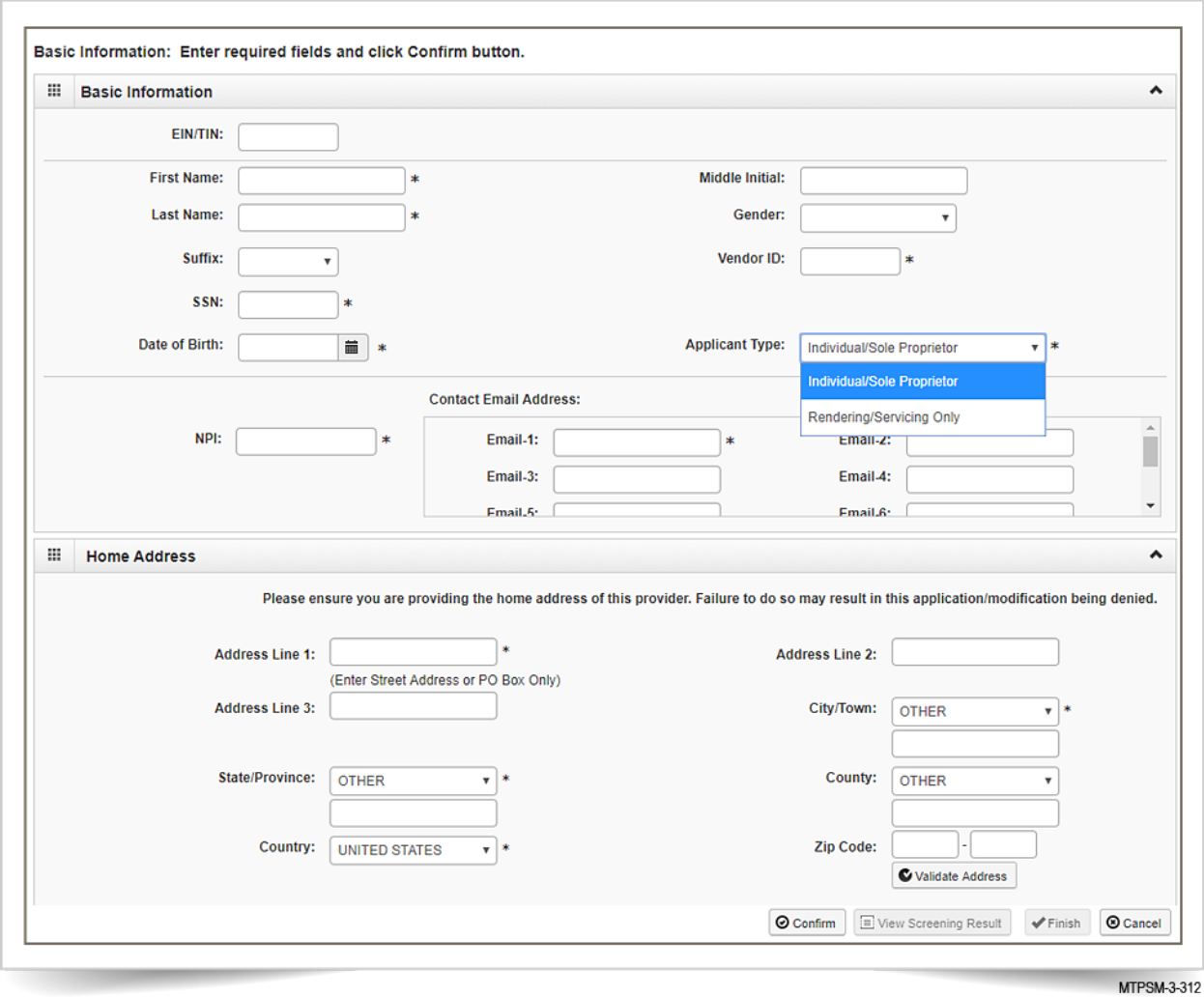
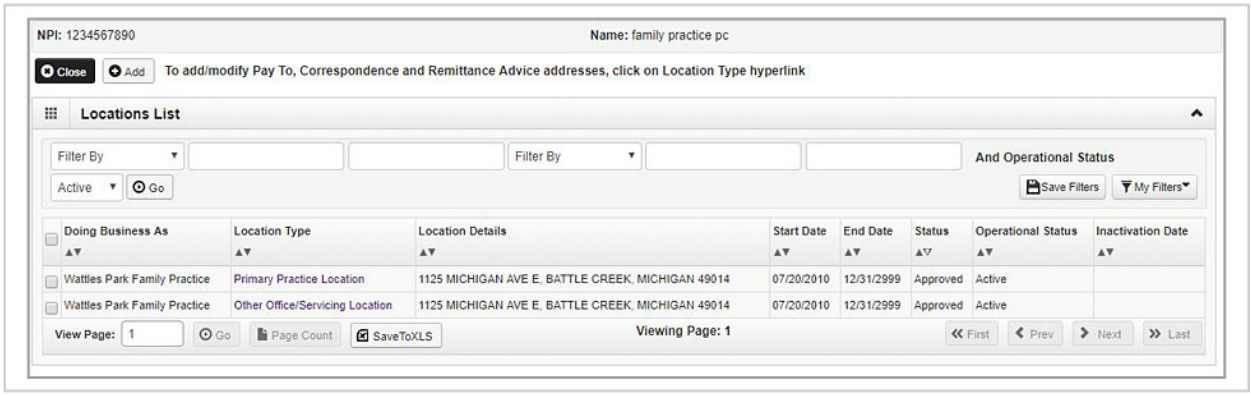


Figure 3.10.10-32. Basic Information Screen - Enter Servicing Type. Providers can enter the servicing type during the first step of the enrollment process.

ENR13

The Contractor's solution shall allow a single provider to enroll multiple service locations.

The evoBrix PMIS allows a provider to choose multiple service locations while enrolling. The provider will need to designate one of the service locations as the primary as shown in Figure 3.10.10-33.



MTPSM-3-394

Figure 3.10.10-33. Locations List Screen. Providers can enter multiple service locations while enrolling but must designate one of those as primary.

ENR14

The Contractor's solution shall collect and maintain all information needed to complete provider enrollment in compliance with all State and federal policies and regulations.

The evoBrix PMIS collects several data elements from Providers, including basic information like name, enrollment type, contact information, NPI/API, provider location information, provider specializations/taxonomies, provider ownership details, licenses and certification information, billing provider details, servicing provider information, and provider affiliation information as part of the Provider Enrollment process, in compliance with State and Federal policies and regulations.

ENR15

The Contractor's solution shall determine provider eligibility in accordance with State and Federal policies and regulations.

Within evoBrix PMIS, providers' eligibility can be updated by one of the following methods:

- By the system as part of the system initiated batch processes (such as license updates, monthly batch monitoring)
- By the system as part of the PCS screening process
- By authorized State Staff as requested by provider or DPHHS (based on provider sanction information received by State)

Provider eligibility maps to Active or Inactive/Closed or Deceased status, and providers cannot update their eligibility status directly.

ENR16

The Contractor's solution shall provide the ability to accept and track provider enrollment fee information.

The evoBrix PMIS provides the ability to collect, maintain, and track the enrollment application fee for all institutional providers. Institutional providers are identified based on provider type and specialty. The fee collection solution is an interactive, online solution that integrates with the provider enrollment solution and seamlessly integrates with the third-party payment gateway for collecting enrollment application fees. The fee collection screen is integrated into provider enrollment process as one of the steps within the BPW. The system allows the institutional providers to pay the enrollment fee during the new application enrollment and revalidation process. The solution also integrates with the State treasury system for reporting and reconciliation of the provider payments. evoBrix PMIS provides the ability for the enrollment specialist to configure fee collection parameters (e.g., fee amount, effective state date, and effective end date) for each provider type and specialty combination through the Fee Schedule maintenance screen.

ENR17

The Contractor's solution shall allow providers to view status of their enrollment online.

During the new enrollment process, evoBrix PMIS generates a unique 14-digit application number after collecting basic information from the provider, and sends an email notification to the provider. The providers use the number as a reference which allows them to track and resume an incomplete application. The application number also allows providers to check on the status of their submitted application. Once the online application is completed and submitted, a message is displayed acknowledging the submission of the application.

ENR18

The Contractor's solution shall support real-time edits allowing providers to submit corrections to applications as needed.

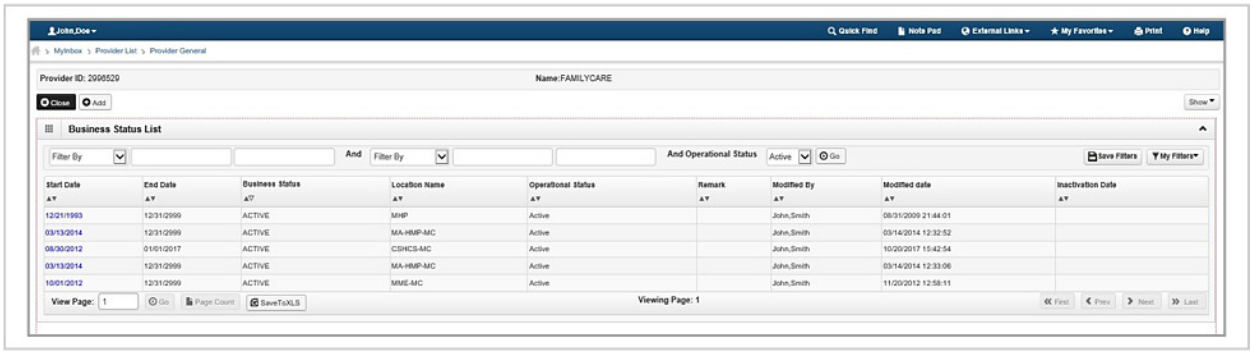
The evoBrix PMIS provides real-time field level edits on each webpage that greatly reduce keying errors. All data entry is performed through data entry screens on the provider portal, thus reducing the volume of issues and delays resulting from loss of forms in mail, and the amount of time needed to process new applications and maintenance requests.

Enrolled active providers can make modifications to their provider enrollment data through the portal's self-service maintenance.

ENR19

The Contractor's solution shall be capable of suspending provider participation in specific programs while maintaining participation in other programs and initiate notification(s) to the provider, agency staff, and modules.

The evoBrix PMIS has the capability to suspend provider participation in programs while maintaining participation in other programs. In the event of such an occurrence, system will initiative notification(s) to the provider, and the State staff. Figure 3.10.10-34 shows the list of programs in which a specific provider is enrolled in and the resp. eligibility status for each.



MTPSM-3-395

Figure 3.10.10-34. Business Status List Screen. Providers can enroll in multiple programs and their eligibility is maintained by program.

ENR20

The Contractor's solution shall use automated screening and monitoring processes and tools to verify provider enrollment eligibility based on State regulations and policies (e.g., State licensing agencies, State exclusion lists, Provider Enrollment Chain and Ownership System (PECOS)).

Team CNSI's PCS solution, in partnership with LexisNexis, provides full compliance with the ACA Provider Enrollment Screening requirements. The PCS solution is comprised of pre- and post-enrollment screening processes that integrate as a real-time credentialing service. This one-stop solution provides improved automation and reduced manual intervention. Pre-enrollment screening results are available in real time for the provider enrollment specialist to review and make appropriate decisions regarding whether to approve or deny the enrollment application. The screening solution performs periodic screening of providers and applies the business rules defined by the State Medicaid program.

The provider screening checks will be conducted in real-time, which includes the following screening criteria:

- State/Federal Death Verification
- Sanctions
- OIG Sanctions
- General Services Administration (GSA) Exclusion list (EPLS/SAM)
- License Board Sanctions
- NPI Verification
- SSN, EIN/TIN Verification
- National Council for Prescription Drug Programs (NCPDP) Verification
- License/Certification Verification
- In/Out-of-state professional license
- DEA, CLIA, Board Certification Verification with American Board of Medical Specialties
- Criminal History and Sex Offense check
- Provider Enrollment Chain and Ownership System (PECOS) – Upon availability of the data source from CMS

The screening solution provides the ability to meet the new ACA provider enrollment and screening requirements for database checks by streamlining LexisNexis screening service and retrieving the information in an automated manner. evoBrix PMIS automatically dis-enrolls/end-dates the eligibility of

the enrollment upon Sanctions, License Expiry/Lapsed/Suspended, and Deceased during the periodic monitoring and revalidation process.

ENR21

The system will be able to link to training modules within the enrollment process (e.g., contractors authorizing member and provider services).

The evoBrix PMIS self-service portal has a configurable External Links feature that will store the links to the external applications that State staff or providers will need to access from the application. The external links are configurable separately for both State staff and providers to access external content such as In-State License, Taxonomy Codes, State Plan, Program Policy information, and Medicaid Information Bulletins and to provide links to external programs such as low-income service and programs, health plans, vital stats, waiver programs, and aging services.

Team CNSI will configure the Training Module link to the External Links for the authorized State and provider users to access via the self-service portal within the enrollment process, as discussed in response to requirements TRN17 in Section 3.10.14.4, Provider Call Center.

ENR22

The Contractor's solution shall support at a minimum, the following enrollment status designations or their equivalent: denied, terminated, suspended, provisionally accepted, accepted, in progress, pending, voluntarily terminated.

The evoBrix PMIS supports enrollment status designations: denied, terminated, suspended, accepted, in progress, pending through a combination of enrollment status and business status data elements.

ENR23

The Contractor's solution shall allow users to enroll retroactively in compliance with State policy, ACA and CMS standards.

The evoBrix PMIS allows users to enroll retroactively, in compliance with State policy, ACA and CMS standards. This is accomplished using a checklist question that asks the provider if they need to enroll retroactively. If the provider responds in the affirmative, they must specify the retro-enrollment date.

ENR24

The Contractor's solution shall maintain the provider's effective date to begin administering services as of the date the provider screening process is complete as the standard effective date unless otherwise overridden and specified by the State.

The evoBrix PMIS sets the provider's effective date in the system as the date when the provider enrollment application gets submitted, which is also the date when the provider screening process completes.

ENR25

The Contractor's enrollment process shall be configurable to include trading partner enrollment within the overall provider enrollment business process.

The evoBrix PMIS supports enrollment of trading partners within the overall provider enrollment business process.

ENR26

The Contractor's solution shall present conditionally required resource materials and training required in order to complete the enrollment business process.

The evoBrix PMIS self-service portal has a configurable External Links feature that will store the links to the external applications that State staff or providers will need to access from the application. The external links are configurable separately for both State staff and providers to access external content such as In-State License, Taxonomy Codes, State Plan, Program Policy information, and Medicaid Information Bulletins and to provide links to external programs such as low-income service and programs, health plans, vital stats, waiver programs, and aging services.

Team CNSI will configure conditionally required resources and training materials to the External Links for the authorized State and provider users to access via self-service portal within the enrollment process, as discussed in response to requirements TRN17 in Section 3.10.14.4, Provider Call Center.

3.10.11 Maintenance

This section addresses provider maintenance requirements. The Provider Services module must support provider maintenance activities for external and internal users that are founded on business process driven workflow automation principles. Maintenance activities include the collection, storage, maintenance of information. It also requires ongoing automated provider monitoring necessary to support Montana Healthcare Programs business objectives and must be compliant with federal and state statues, policies and mandates. The Offeror must describe their approach to meet each of the Provider Maintenance requirements defined in Attachment F, Requirements Matrix.

The evoBrix Provider Management Information System (PMIS) features a secure, web-based provider portal that delivers functionality for provider access through a rich set of self-service functions. Providers must have a system-issued domain name and profile to access the evoBrix PMIS provider portal.

After successful enrollment, providers can use the provider portal to do the following:

- Initiate enrollment for another provider
- Update enrolled provider information

The Team CNSI Advantage

Team CNSI's certified implementations in the states of Michigan and Washington will bring the State a proven and mature Provider Management Information System (PMIS).

- The evoBrix PMIS is a modern, web-centric provider enrollment and management solution, based on the fully CMS-certified solution in Michigan
- The evoBrix PMIS combines a full-featured, self-service provider portal with a comprehensive administrative framework to manage enrollment, disenrollment, inquiry, provider information maintenance, and provider support
- The solution gives the ability to assign multiple specialty/subspecialty classification for providers based on the permission matrix configuration
- It provides capability for automated provider revalidation and generates correspondence upon specific events such as revalidations and license renewals

MTPSM-3-325

- Retrieve correspondence
- Self-administer provider domain access

The provider portal provides multiple time-saving features. It offloads the data entry workload from enrollment specialists to the provider. evoBrix PMIS business process wizards (BPWs) and online, real-time edits greatly reduce keying errors. All data entry is performed through data entry screens on the provider portal, thus reducing the volume of issues and delays resulting from loss of forms in the mail, as well as the amount of time needed to process new applications and maintenance requests.

Provider Administration

Using evoBrix PMIS secure portal, provider enrollment specialists can review enrollment application and approve or deny based on the decision made during review. Built-in security features allow evoBrix PMIS authorized users to view in-process provider applications and modifications, and to render approval and denial decisions. This allows business operations staff to track and report on the provider enrollment activities from receipt of application to final disposition.

evoBrix PMIS pages are designed to give a nearly identical graphical user interface (GUI) experience to providers and enrollment specialist staff. Because the pages are identical in most cases, it is easier for business operations staff to provide support to providers. This also simplifies help desk processes. All of the features described above are available through the evoBrix PMIS interface used by enrollment specialists, with the exception of self-administration of provider users.

The Provider Services business area displays menu options specifically for provider administration and enrollment staff. These are controlled through the security profile. The Provider Services business area allows enrollment unit staff the ability to perform many different functions. As shown in Figure 3.10.11-1, the three main menu selections are: 1) Provider Enrollment; 2) Manage Provider; and 3) Administer.

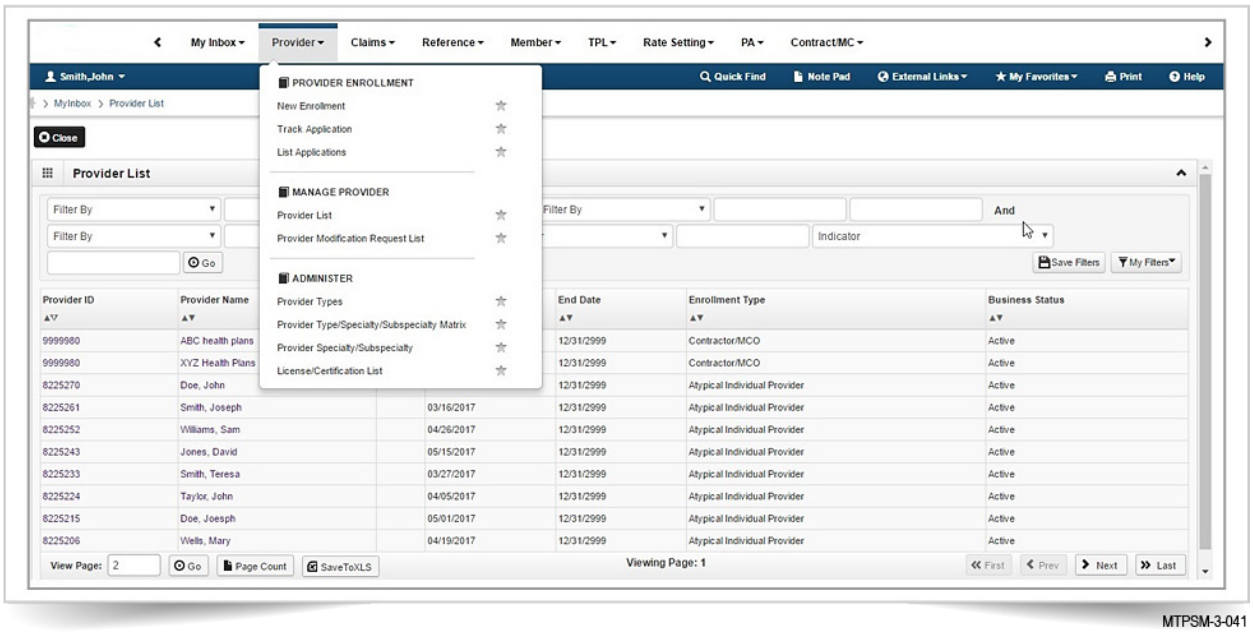


Figure 3.10.11-1. evoBrix PMIS Online Portal. The enrollment specialists can administer providers, manage provider data, and review enrollment applications and modification requests.

Provider Enrollment

Under the Provider Enrollment menu, enrollment specialists access functions to begin a new enrollment application or view applications entered by providers, applications under review for acceptance or rejection, and applications that have been accepted or rejected, as shown in Figure 3.10.11-. The enrollment specialist uses a tracking number to view a specific application, search through the entire list, or make inquiries based on user-defined parameters. This menu option enables authorized enrollment unit users to access the User Maintenance function that is used to authorize provider enrollment staff for specific enrollment and maintenance review queues.

Manage Provider

The Manage Provider menu allows authorized enrollment specialists access to requested modifications initiated by providers on the provider portal. Figure 3.10.11-2 shows the Modification Request Task list where the enrollment specialist can locate the modification request initiated by the provider and manage the routing process using workflow management functionality.

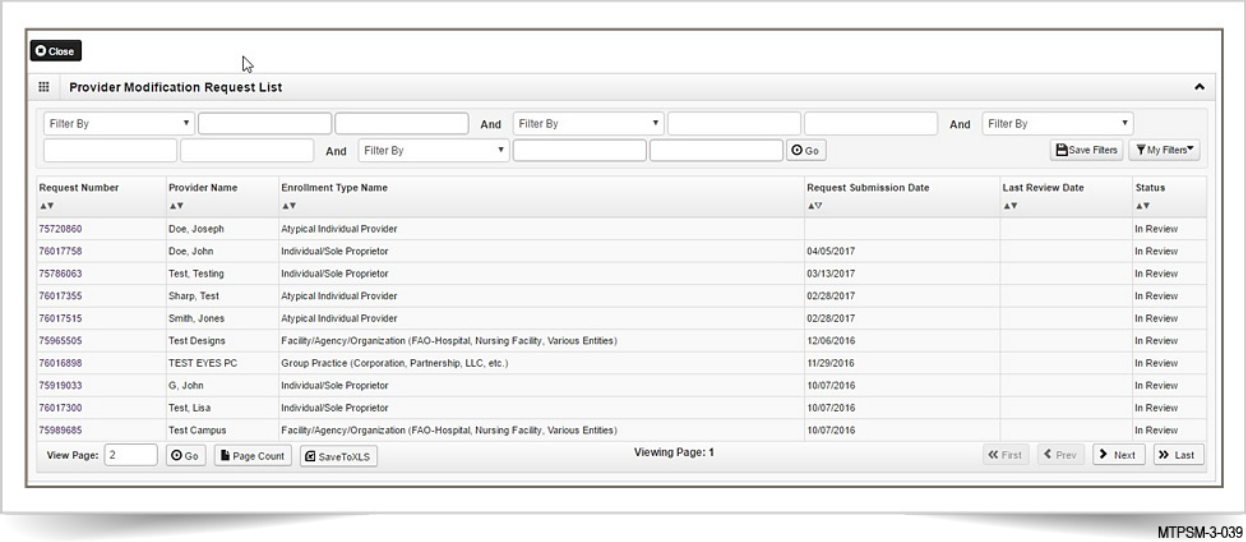
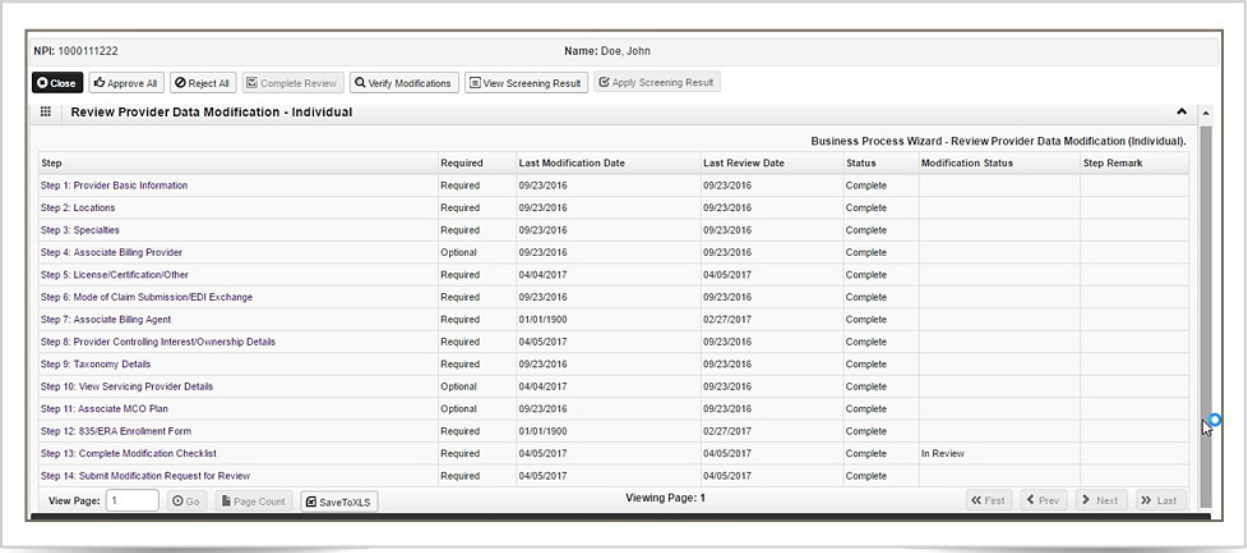


Figure 3.10.11-2. Modification Request Task List. The enrollment specialists access the review wizard to review the data that have been updated by the providers and make appropriate decisions.

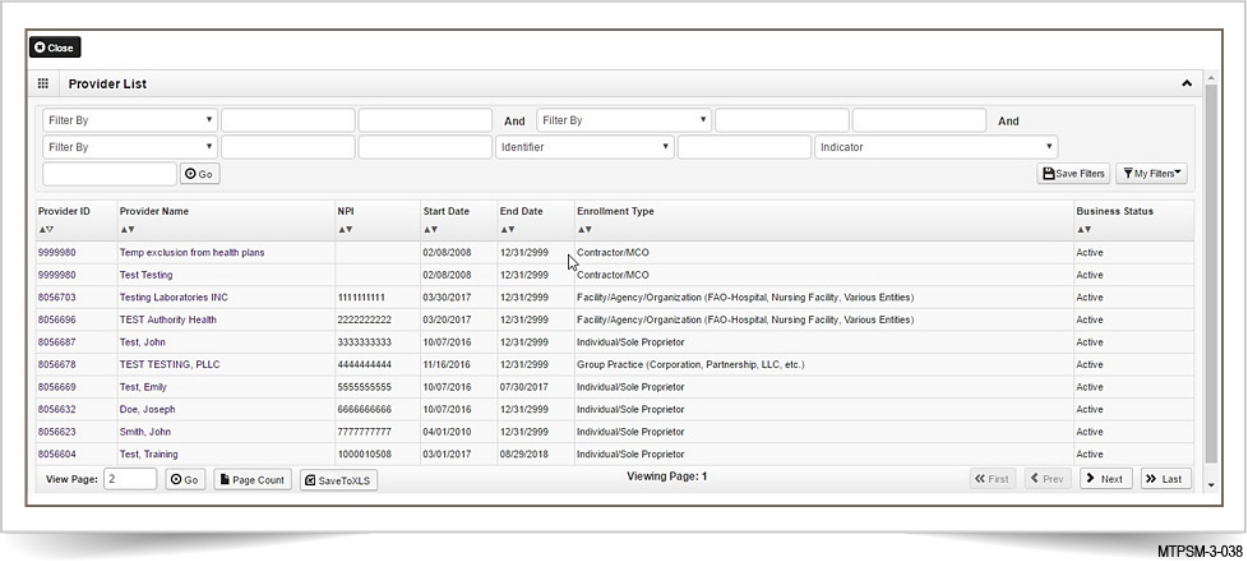
The evoBrix PMIS routes maintenance requests based on the requesting provider's enrollment type and taxonomy. As with the enrollment workflow, the maintenance request routing can be configured according to business need. The enrollment specialists access the review wizard to review the data that have been updated by the provider user and make decisions. Figure 3.10.11-3 shows the Individual Provider Modification BPW, which is similar to the provider enrollment wizard.



MTPSM-3-040

Figure 3.10.11-3. Individual Provider Modification Business Process Wizard. Users can view and update the provider data through this screen.

Also, under the Manage Provider menu, authorized users can access the robust Provider List feature, an extremely powerful function within the Provider Services business area. Provider List allows the user to search on multiple provider attributes to locate a specific enrolled provider (e.g., NPI) or group of providers sharing a common set of attributes (e.g., zip code and specialty). As shown in Figure 3.10.11-4, the Provider List page has three primary filters and two secondary filters. The secondary filters are Identifier and Indicator. The user has the ability to save favorite search criteria by selecting the Save Filters button. Saved filters are retrieved under the My Filters dropdown. The list retrieved may be exported to Excel for additional analysis using the Save to XLS button. The sorting functionality on the list page can allow the user to display the data in reverse chronological order.



MTPSM-3-038

Figure 3.10.11-4. Provider List Page Showing Filter Capability. This screen highlights the three major filters, the secondary filters, the Save Filters and My Filter retrievals, and Save to XLS features.

Administer

Under the Administer menu, authorized enrollment unit staff access evoBrix PMIS provider functions to perform mass updates to providers and define new provider type and specialty/subspecialty combinations. The Mass Update feature allows the user to add newly-defined specialty/subspecialty to all providers of a specific type and the end-date for the discontinued specialty/subspecialty. This makes it easy for authorized enrollment unit staff to quickly apply changes affecting multiple providers. Also, this screen provides the ability for the authorized staff to define license/certification requirements for each provider type and specialty/subspecialty combinations.

PMNT01

The Contractor's solution shall have the capability to terminate inactive providers based on criteria determined by the department for either automatic termination or initiate a workflow for manual termination.

The evoBrix PMIS solution has built-in feature to check for provider eligibility and take actions to terminate any inactive/ineligible providers. The termination can be performed either through automated process or through manual workflow process based on State requirements.

The automated process reduces manual intervention and saves time for the staff by periodically monitoring providers, assessing their eligibility based on predefined criteria and terminating providers who fail to meet the eligibility criteria defined by State. Once the batch process completes, system is geared to generate a report that lists out the terminated providers after each run.

Alternately, the automatic process can also be configured to flag providers for additional review by State staff, leaving the final decision to them, to determine whether a provider needs to be terminated within the system if they fail to meet the criteria.

The evoBrix PMIS solution also comes with a comprehensive workflow process for routing the provider data to multiple department personnel, through a workflow queue to arrive at a decision based on collective comments and feedback of the personnel involved. evoBrix PMIS allows authorized enrollment staff to suspend or terminate the enrollment eligibility based on the State-defined policy. Once a provider is terminated, the business status of his record is changed to "Inactive/Closed" and the information is retained in the system for seven years from the date of termination.

PMNT02

The Contractor's solution shall collect and retain electronically all provider documentation (e.g., original application and copies of correspondence) for actively participating providers. For terminated providers, records shall be retained electronically according to record retention requirements (i.e.,7 years).

evoBrix PMIS seamlessly integrates with the FileNet content management solution by IBM, which is Team CNSI's Document Management System (DMS). FileNet provides advanced document management features and technology frameworks that meet DPHHS requirements and will serve as the repository for all system documents and provider support materials including original enrollment application, copies of all correspondence, all system generated letters, and provider supporting documents. The archived documents can then be accessed through the evoBrix PMIS portal or printed on demand.

Team CNSI brings a data retention framework that is configurable to meet the data retention needs for audit and history. evoBrix PMIS tables to be included or excluded for the Data Retention policy, the "data selection criteria" (date-based or other custom criteria) that determines which aspect of the historical data needs to be purged and what needs to be retained, and the scheduling and execution of the end-to-end process are configured and fully automated. The configuration details for data retention will be used by a backend process to orchestrate the data purge.

evoBrix PMIS will be configured to maintain provider data for a minimum of seven years for terminated providers. Any terminated provider data that falls outside the defined data retention period of seven years would be considered as operationally non-relevant historical data and the data retention framework will physically delete the applicable data record in evoBrix PMIS solution. Team CNSI's business operations team will validate the potential transactions to be deleted/purged before the actual historical data gets deleted from the system. Team CNSI follows a rigorous and time-tested approach of ensuring that the stakeholders/data stewards are kept informed via summary reports capturing the timespan along with the high-level metrics of the data to be deleted before implementing the data purge policies in the Production environment.

PMNT03

The Contractor's solution shall require, capture and maintain the 10-digit National Provider Identifier (NPI) for all healthcare providers required to have an NPI and interface with NPPES to verify the NPI is valid.

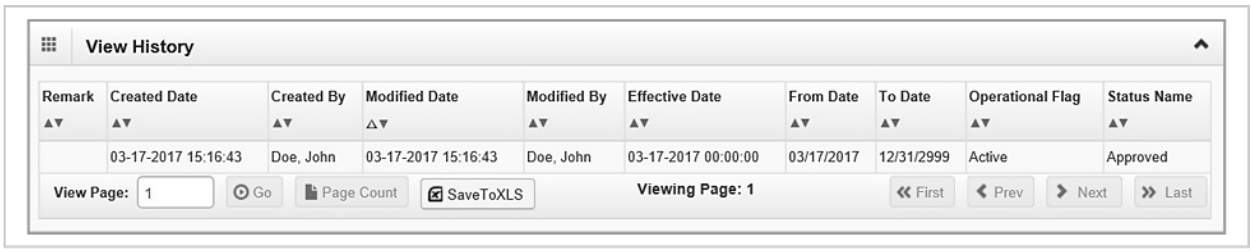
evoBrix PMIS captures the 10-digit NPI data from providers during the enrollment process and verifies the same against the NPPES database through a real-time call to ensure that the NPI, provider name, and provider entity type match the data registered with NPPES. Also, the system checks to ensure that the NPI entered by the provider is not deactivated, or of incorrect type. evoBrix PMIS also checks the validity of NPI data monthly.

PMNT04

The Contractor's solution shall record and display begin and end dates for specific provider enrollment and demographic data (e.g., license, eligibility period, physical address) and provide access to historical provider record information.

evoBrix PMIS records and displays the begin and end dates for provider enrollment and demographic data (e.g., license, eligibility period, physical address) and provide access to historical provider record information. evoBrix PMIS maintains a complete audit trail of changes made to any data stored within the system as shown in Figure 3.10.11-5. This includes provider demographic, license, and eligibility period too. Audit trail entries include:

- Remark – A free-form text entry field that allows the user to provider a narrative statement concerning the action taken
- Date Modified – The date the change was applied to the system
- Modified By – User ID of the person or system acting on the change
- Effective date – The date evoBrix PMIS began using the updated information
- From date – The beginning date of the effective date span
- To date – The end date of the effective date span



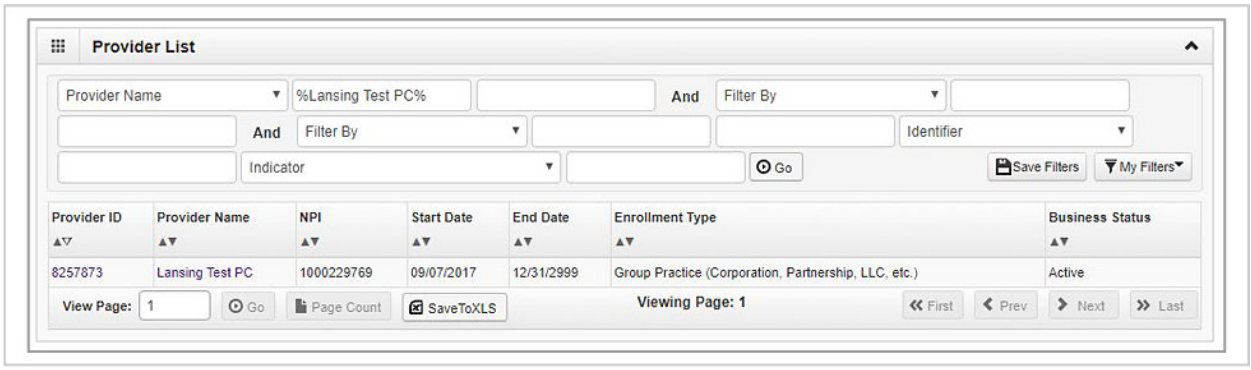
MTPSM-3-399

Figure 3.10.11-5. History of Audit Trail. This screen lists the history of changes made to provider enrollment and demographic data.

PMNT05

The Contractor shall use a standardized format for provider names that differentiate between first name, middle name/initial, last name, and business or corporate names and allows flexible searches based on the provider name.

The evoBrix PMIS solution provides a BPW to collect provider information through a series of steps. The Provider Basic information step collects First Name, Middle Name/Initial, Last Name for individuals and collects Business name for Organizations through a standardized format. Once the data is stored in the system, State staff can search for providers based on any of those data elements as shown in Figure 3.10.11-6.



MTPSM-3-400

Figure 3.10.11-6. Provider Search Screen. Users can search for a specific provider by different search criteria, including name, through this screen.

PMNT06

The Contractor's solution shall allow provider records to be associated and linked by tax identification number (TIN) and parent organizations.

evoBrix PMIS collects the provider's tax identification number as part of the first step during the enrollment process. This tax identifier is verified against the state treasury file for validity. Any organization that uses same tax identifier will have the same tax level indicators that were previously assigned by the organization that first registered with that tax identifier.

Additionally, evoBrix PMIS gives the ability for the providers to associate with active billing providers. This is achieved through the Associate Billing Provider step in the BPW which becomes mandatory or optional based on the Applicant Type and Enrollment Type selection. The system provides the option to search for and confirm the billing provider based on NPI or Provider ID. Providers can associate with one or more billing providers based on the business status of the billing provider. The system prevents association of inactive billing providers.

PMNT08

The Contractor's solution shall allow for collection and maintenance of site visit, finger printing and background check information (e.g., the type of site visit (e.g., field representative, pre enrollment, program staff), date the site visit/ finger print/background check completed, reason and outcome if applicable).

The evoBrix SiteVisitPro (SVP) solution is a portable application that the State staff can take with them directly to provider locations on their unannounced site visits. The application is mobile enabled for tablets, eliminating the need for paper forms. This application supports organizations in performing site visits using real-time provider information directly from evoBrix PMIS, thereby eliminating redundant data entry. The solution also supports capturing the outcome of the site visit.

The evoBrix SVP solution helps identify fraudulent providers by capturing specific information about the provider's practice. The evoBrix SVP solution can be accessed from anywhere using a wireless connection. The application:

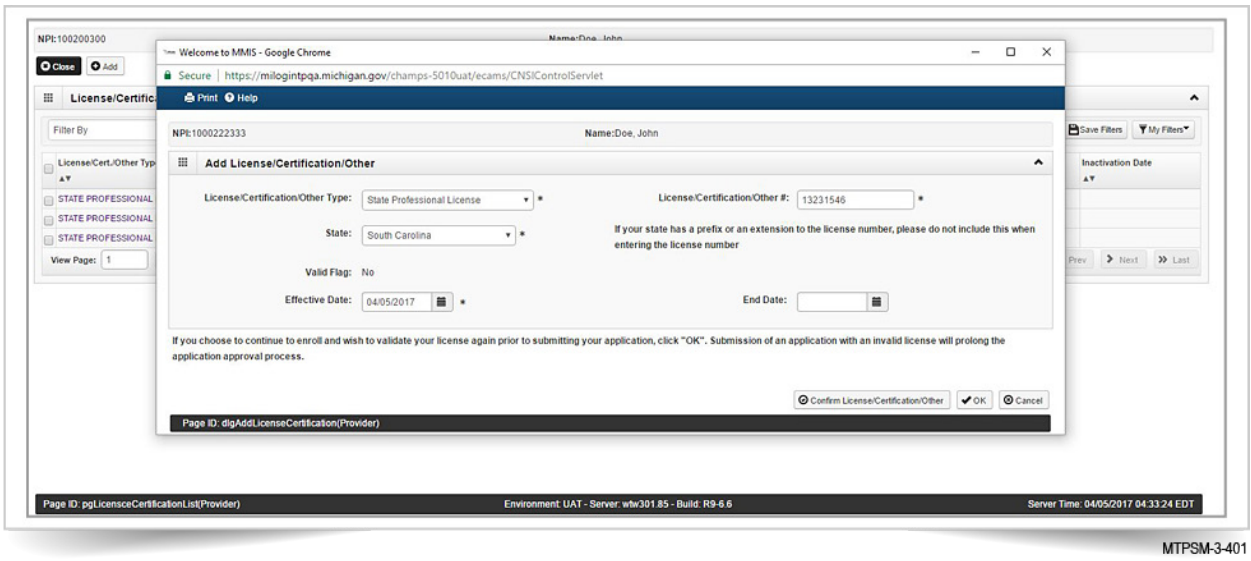
- Streamlines SiteVisitProcessing using a real-time system, eliminating paper forms
- Eliminates periods of inactivity on the site visits through alerts to the appropriate State staff
- Decreases the time it takes to approve or reject a provider's application for enrollment
- Eliminates redundant data entry and manual updates to the Medicaid Provider Enrollment system

The system provides the ability to track fingerprinting and also supports performing criminal background checks against public records through the evoBrix Provider Credentialing Services (PCS) solution.

PMNT09

The Contractor's solution shall collect and maintain licensure information to include at a minimum, licensing state, license number, licensure begin and end dates.

evoBrix PMIS collects provider licensure information as part of the provider enrollment process. The licenses requirement is determined by the pre-configured Provider Type and Specialty/Sub Specialty Matrix. As part of the "Add License/Certification/Other" step shown in Figure 3.10.11-7, the provider is asked to enter license information such as In-State Professional License, Out of State Professional License, DEA, NCPDP, Board Certificates etc. Once the license number and State information is entered, the system verifies the validity of the License through evoBrix PCS solution. Thus, the system not only captures license number, license state, begin date and end date for the license, but also verifies the validity of each license entered.



MTPSM-3-401

Figure 3.10.11-7. Add License/Certification/Other Screen. Based on the configuration of Provider Type and Specialty/Subspecialty combination the Licenses/Certification/Other Type is populated with required types for provider to enter the credentials.

PMNT10

The Contractor's solution shall collect and maintain the Pay for Performance (P4P) information from Medicare.

The evoBrix PMIS solution uses resources from Center for Medicare and Medicaid Services (CMS) like MCSIS (Medicaid and Children's Health Insurance Program State Information Sharing System) and Medicare exclusions in Provider Screening. evoBrix PMIS collects and maintains data from CMS to perform screening of providers. The system can be configured to use CMS resources including Pay for Performance (P4P) information from Medicare using the existing model.

PMNT11

The Contractor's solution shall collect and maintain date specific (as applicable) provider endorsement and accreditation information.

The evoBrix PMIS solution collects board certification details including the certification number, start date, and expiry date from providers as part of the "Add License/Certifications/Other" step during the enrollment process. It then verifies the data against the American Board of Medical Specialties (ABMS) maintained in the system. A complete history of the license/certification information can be maintained in the system including renewal, activation or inactivation dates of license.

PMNT12

The Contractor's solution shall collect and maintain malpractice insurance information including expiration date.

The evoBrix PMIS solution collects provider Licensure information including license number, state, board, start date, and expiry date during the enrollment process through an enrollment BPW step. This step can also be leveraged to collect and maintain provider malpractice insurance information. This information can then be verified against any State identified source.

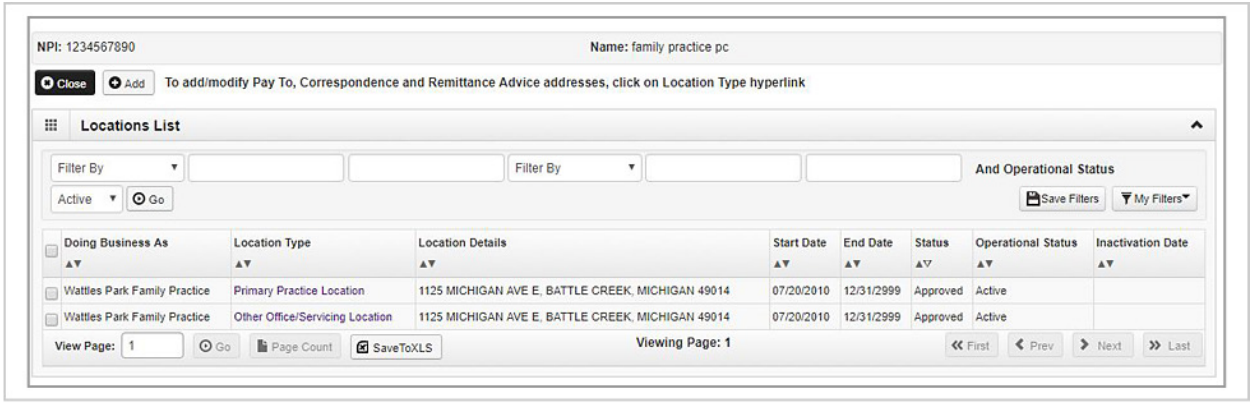
PMNT13

The Contractor's solution shall provide dynamic navigation that allows users to have one click access to additional detail for summary information (e.g., from the providers screen, select a specific location to view location details such as address, contact(s), office hours).

evoBrix PMIS provides an interactive enrollment application that comes with structured, online screens driven by the enrollment BPW. The wizard guides the provider step-by-step through the enrollment process. It allows the providers to navigate, view, validate, and modify any information in the application up to point of final submission for review and approval. Once the provider completes the first "Basic Information" step, they can jump to any other subsequent step and are not constrained to follow the sequential flow. Also, the BPW determines certain steps to be optional for a provider based on the data they enter and these will be high-lighted as "Optional" for them to complete.

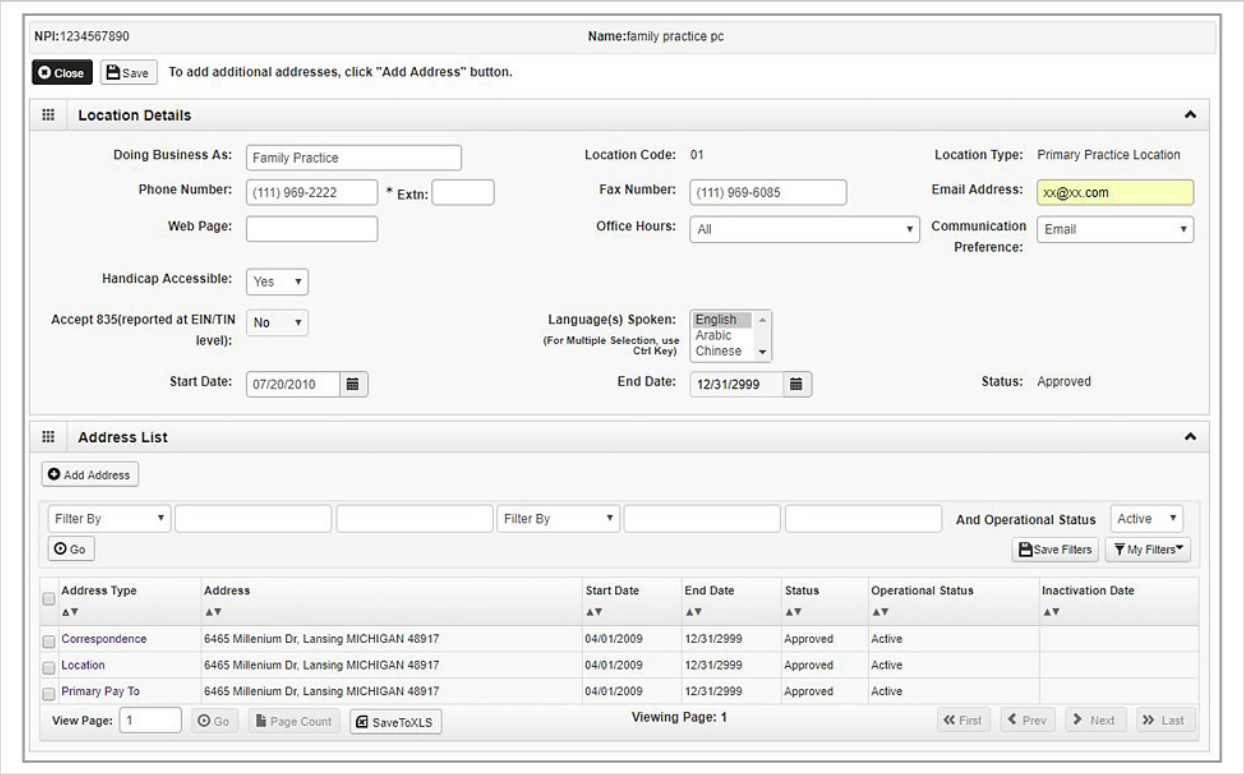
State staff can view the screens either through provider mode or expert mode. They can also switch to any screen to get detailed information from that screen.

Figure 3.10.11-8 and Figure 3.10.11-9 show examples of a location list (summary) screen and a location detail screen that illustrate the capability of the system to allow one click access to additional detail for summary information.



MTPSM-3-402

Figure 3.10.11-8. Provider Locations List Screen. This screen displays summary information about each location associated with the provider.



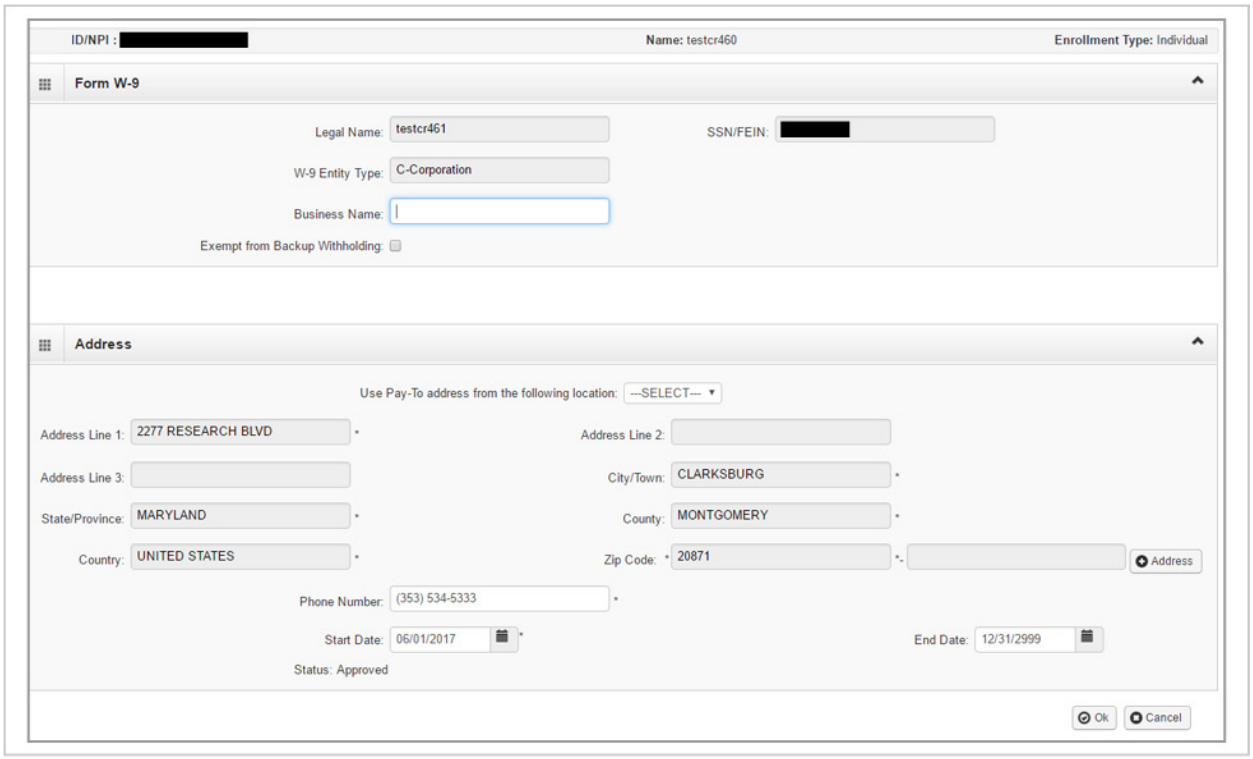
MTPSM-3-403

Figure 3.10.11-9. Provider Location Detail Screen. This screen presents detailed information about a specific location for a provider.

PMNT14

The Contractor's solution shall collect and store standardized W-9 information that reflects the owner of the EIN and the Doing Business As (DBA) name.

evoBrix PMIS includes functionality to allow for providers to enter their W-9 information as part of their enrollment process. Figure 3.10.11-10 shows evoBrix functionality for providers to enter/update W-9 information including Name and TIN (SSN/FEIN).



MTPSM-3-194

Figure 3.10.11-10. Provider W-9 Screen. Providers have the option to enter/update their W-9 information within evoBrix PMIS.

PMNT15

The Contractor's solution shall provide the capability to reactivate terminated providers without requiring a complete re-enrollment.

evoBrix PMIS maintains the status of providers' eligibility through a field called "Business Status." All eligible providers participating in the Medicaid program are set to Active Status, while the terminated ones are moved to Inactive/Closed Status. If a provider needs to be reactivated in the system, the State staff can initiate a temporary revalidation cycle for that provider so that they can login to the system and revalidate their credentials to provide proof of eligibility. When a provider initiates revalidation, the system pre-populates their current information in the screens. However, they do have to verify each step to ensure that their information is valid for each.

Thus, evoBrix PMIS allows providers to be reactivated without requiring a complete re-enrollment. It also performs a comprehensive screening of the providers during this revalidation window to ensure that they are eligible to be re-enrolled.

PMNT16

The Contractor's solution shall track and support provider review schedules to ensure providers continue to meet program eligibility requirements and initiate notification(s) to the provider, agency staff, and modules of State healthcare programs agreements and contracts.

The evoBrix PMIS solution provides:

- A streamlined, configurable process for automated provider revalidation
- The ability to configure the revalidation interval by federally defined risk category (high, moderate, and limited) or by provider type/specialty
- The ability to send revalidation notices to begin the revalidation for each provider
- The ability to systematically terminate the enrollment in the event of incompletion by the revalidation due date

Team CNSI's PCS solution supports monthly screening of providers against federal databases. This comprehensive screening of providers meets the post-enrollment screening criteria defined by CMS.

evoBrix PMIS generates correspondences to the providers, informing them about the need to maintain their eligibility within the system. Providers receive letter correspondences or emails on trigger of related events. Figure 3.10.11-11 lists some of these.

Correspondence Title	Description
License/Certification Term in 45 Days' Notice	This letter is generated for all providers whose license/certification expires within the next 45 days.
License Termination Notice	This letter indicates the provider license has expired and that provider enrollment is end dated.
Provider Revalidation 90 Day Notice	This letter is generated for all providers who have 90 days to revalidate their enrollment.
Provider Revalidation 30 Day Notice	This letter is generated for all providers who have not revalidated their enrollment and have 30 more days to complete their revalidation.
Provider Revalidation Termination Notice	This letter is generated for all providers who have not revalidated their enrollment within the 90 day time frame and system terminates the enrollment.
Provider Revalidation Intermediate Cycle Notice	This letter is generated for all providers who have not revalidated in their intermediate cycle and system terminates the enrollment after the due date.
Sanctioned Notice	This letter indicates that the provider has been Sanctioned and is no longer eligible to participate in the Medicaid Program effective from sanction date.
Suspended Notice	This letter indicates that the provider has been Suspended and is no longer eligible to participate in the Medicaid Program effective from suspension date.

Figure 3.10.11-11. The evoBrix PMIS Correspondences/Notifications. These notifications help ensure providers continue to meet program eligibility requirements.

Also, any enrollment status change for providers as a result of the provider review is communicated to the Health Plans through file exchanges.

PMNT17

The Contractor's solution shall accept, validate and store new and updated provider information entered by internal users.

©2017 CNSI

evoBrix PMIS accepts, validates, and stores modifications to the provider enrollment data and routes the modification request to State staff for their review. Authorized State users can then review the modification request and either accept or reject it. If accepted, the modified data will be tagged with an effective date as of the modification and the history of changes will be maintained for audit purpose.

PMNT18

The Contractor's solution will collect, store, maintain and display current and historical addresses by type (e.g., physical address, correspondence address and billing address) and include begin and end dates.

evoBrix PMIS collects provider location information during the enrollment process. Providers must specify at least one primary practice location and one or more servicing locations. As part of this enrollment step, the system collects a physical address, a correspondence (mailing) address, and a "Pay To" (billing) address. All addresses are verified against the most current USPS address database to verify the authenticity of the same.

evoBrix PMIS also accepts, validates, and stores modifications to all provider enrollment data including location information and the modified address will be tagged with an effective date as of the modification historical address will be end-dated. The history of changes will be maintained for audit purposes.

PMNT19

The Contractor's solution will collect, store, maintain and display current and historical Drug Enforcement Administration (DEA) number(s) including begin and end dates.

The evoBrix PMIS solution collects the Drug Enforcement Administration (DEA) number(s) along with the begin and end dates from the providers during the enrollment process as part of the "Add Licenses/ Certification/Other" enrollment step. As with other license types, DEA can be configured to either be mandatory or optional for providers based on Provider Type and Specialty/Sub-Specialty combination. The system also checks if the DEA license is valid and belongs to the provider who is enrolling in the system.

PMNT20

The Contractor's solution will collect, store, maintain and display provider business relationships (e.g., ownerships and managing entities) for use in provider screening and ongoing monitoring activities.

evoBrix PMIS collects, stores, and maintains provider business relationships such as owners, managing employees, board of directors, principals, partnerships, and other owned entities as part of the enrollment process. Within evoBrix PMIS, an owner is defined to be any individual or entity who is associated with the provider as a board of director, has partnership, is a managing employee, or an entity which holds a stake in the organization. Figure 3.10.11-12 shows the enrollment step through which the provider controlling interest/ownership information is collected.

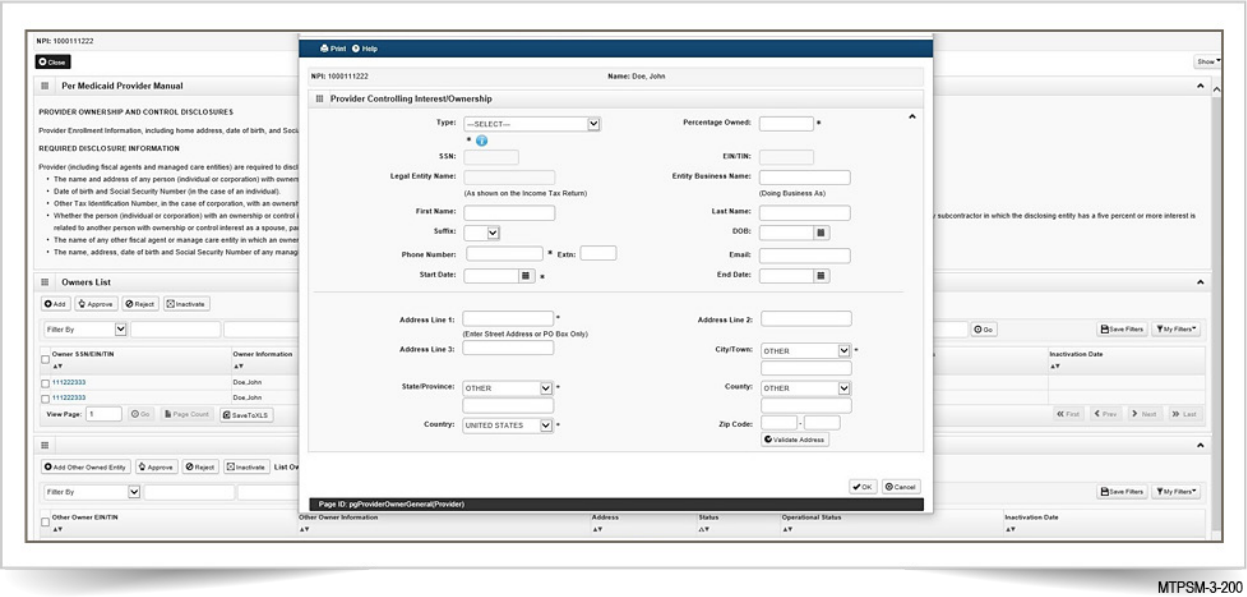


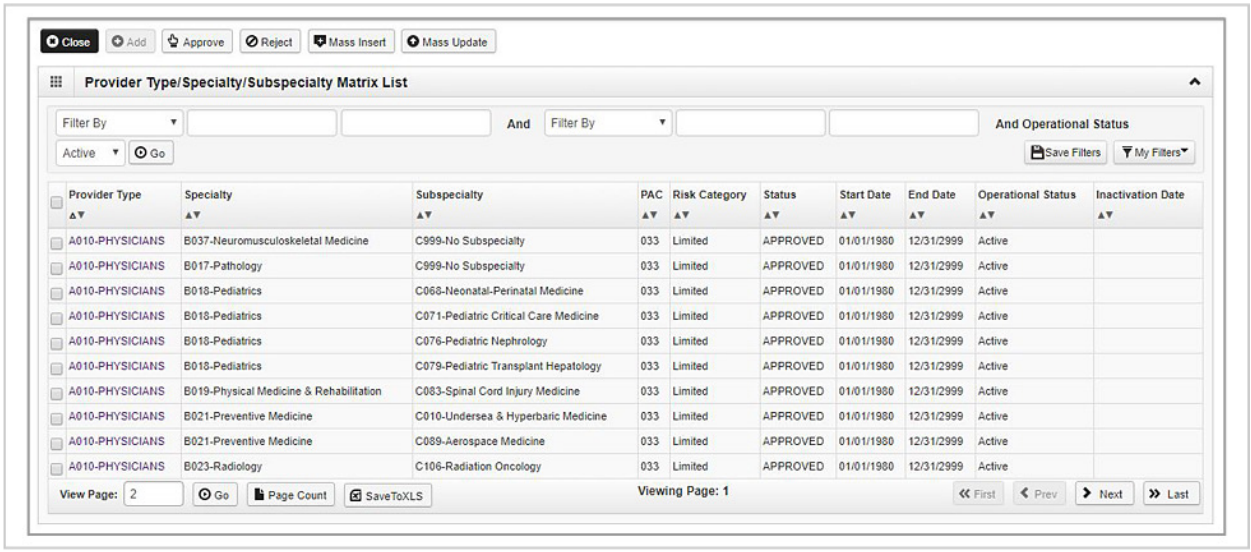
Figure 3.10.11-12. Provider Controlling Interest/Ownership. The evoBrix PMIS provides the ability for the provider to enter ownership information as part of the enrollment process.

This step is configurable and can be driven by State-defined rules. Certain owner types must be entered based on the enrollment and applicant type of the provider. All this information is sent for screening and monitoring, as required by the ACA. Apart from listing the owners, the provider also needs to enter the relationship between the owners.

PMNT21

The Contractor's solution shall have the ability to perform mass updates to provider information using flexible selection criteria.

The evoBrix PMIS solution allows authorized State staff to perform mass updates to provider data through the "Administer" menu option. State staff can define new provider type(s) and specialty/subspecialty combinations. The "mass update" feature allows the user to add newly-defined specialty/subspecialty to all providers of a specific type and to end-date any discontinued specialty/subspecialty combinations as shown in Figure 3.10.11-13. This makes it easy for authorized enrollment unit staff to quickly apply changes affecting multiple providers. Also, this screen provides the ability for the authorized staff to define license/certification requirements for each provider type and specialty/subspecialty combinations.



MTPSM-3-404

Figure 3.10.11-13. Mass Update Feature. The evoBrix PMIS provides ability for the State staff to perform mass inserts or updates by Provider Type/Specialty/Subspecialty combinations.

PMNT22

The Contractor's solution shall provide indicators to identify providers that are Fee-for-Service (FFS), Managed Care Organization (MCO) network only, or participating in any other healthcare programs (e.g., medical homes).

evoBrix PMIS has a built-in feature to identify provider servicing type such as Fee-for-Service (FFS) or Managed Care Organization (MCO) network during the time of enrollment. Appropriate indicators are set for the providers automatically based on their servicing type upon approval of the enrollment. State healthcare programs can be configured as part of the Provider Type/Specialty/Sub-Specialty Matrix for the providers to choose and associate to.

PMNT23

The Contractor's solution shall provide the capability to capture and crosswalk subpart NPIs used by Medicare (but not Medicaid) to facilitate COB claims processing.

evoBrix PMIS collects the provider's Tax ID (SSN or FEIN) and NPI as part of the basic information. The evoBrix PMIS can also store multiple alternate identifiers, which allows for cross-referencing information with legacy system, federal, or other state agencies. Team CNSI will configure the list of allowable alternate identifier types as a part of the solutioning phase to facilitate COB claims processing.

PMNT24

The Contractor's solution shall auto-populate fields with valid data where required.

The evoBrix PMIS solution auto populates data where possible, based on user input, to minimize data that has to be manually entered by the users. For instance, within the address validation screen, the provider is

only required to enter Street name and Zip code of their location. The rest of the details are pulled from USPS and auto populated in the screen, thus preventing invalid address input.

PMNT25

The Contractor's solution shall allow internal users to add and view free-form and structure notes on or associated with individual provider files.

The evoBrix PMIS solution provides the capability for State staff to record and view comments/remarks in various screens. For instance, the State staff can enter and save comments within the Provider Enrollment Review Page as shown in Figure 3.10.11-14.

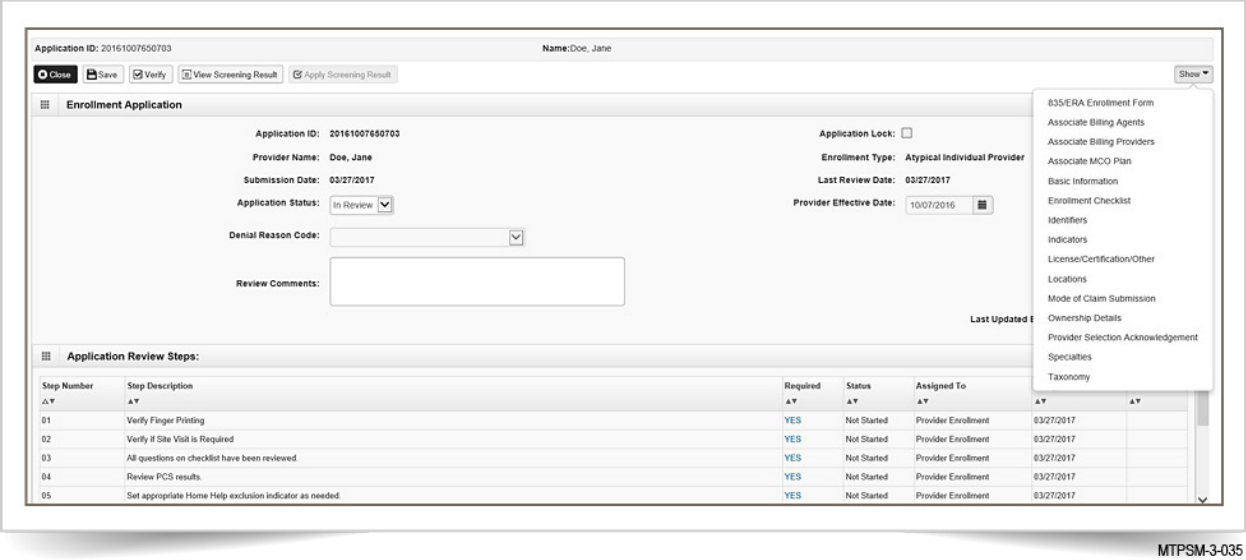


Figure 3.10.11-14. Provider Enrollment Review Page. This page allows State staff to enter and save comments or remarks.

The comment function provides the State staff with free-form text field to record their comments concerning denial or approval of an application or any actions taken related to a specific step in the checklist.

PMNT26

The Contractor's solution shall allow authorized internal users to link and unlink individual practitioners from and to billing providers with the ability to link an individual provider to multiple billing providers. Each relationship shall include an effective date when initiated and an end date associated with the termination of the affiliation.

evoBrix PMIS gives the ability for providers to be associated with active billing providers. This is accomplished through the "Associate Billing Provider" step in the enrollment BPW. This step is either mandatory or optional based on the Applicant Type and Enrollment Type selection. The system provides an option to search for and confirm the Billing Provider based on NPI or Provider ID. Providers can be associated with one or more billing providers based on the business status of the billing provider. The association start and end dates are recorded during the process. Providers cannot be associated with

inactive billing providers. Figure 3.10.11-15 shows how the provider can select a billing provider based on the NPI and ID search.

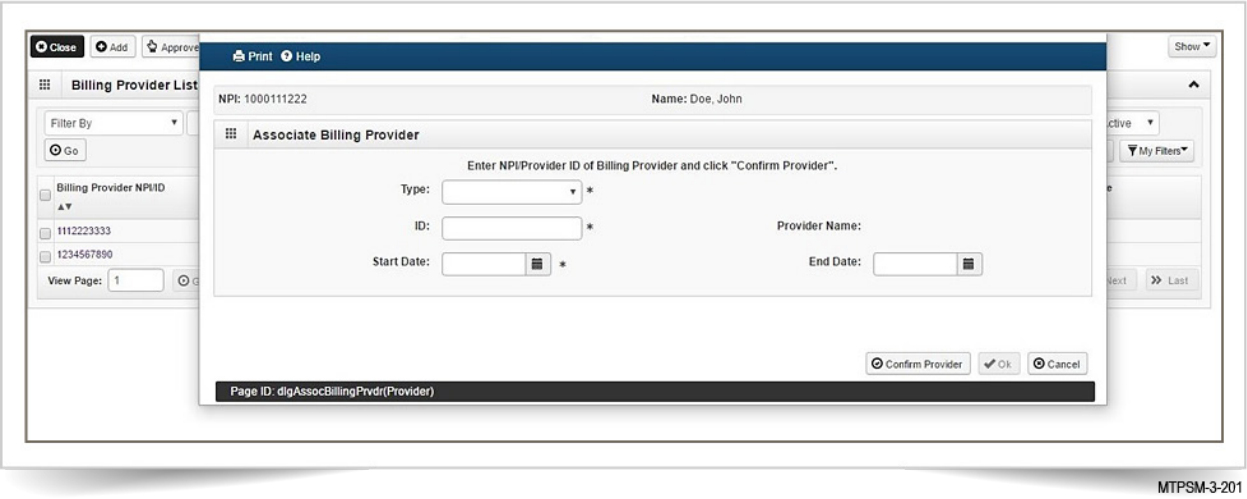
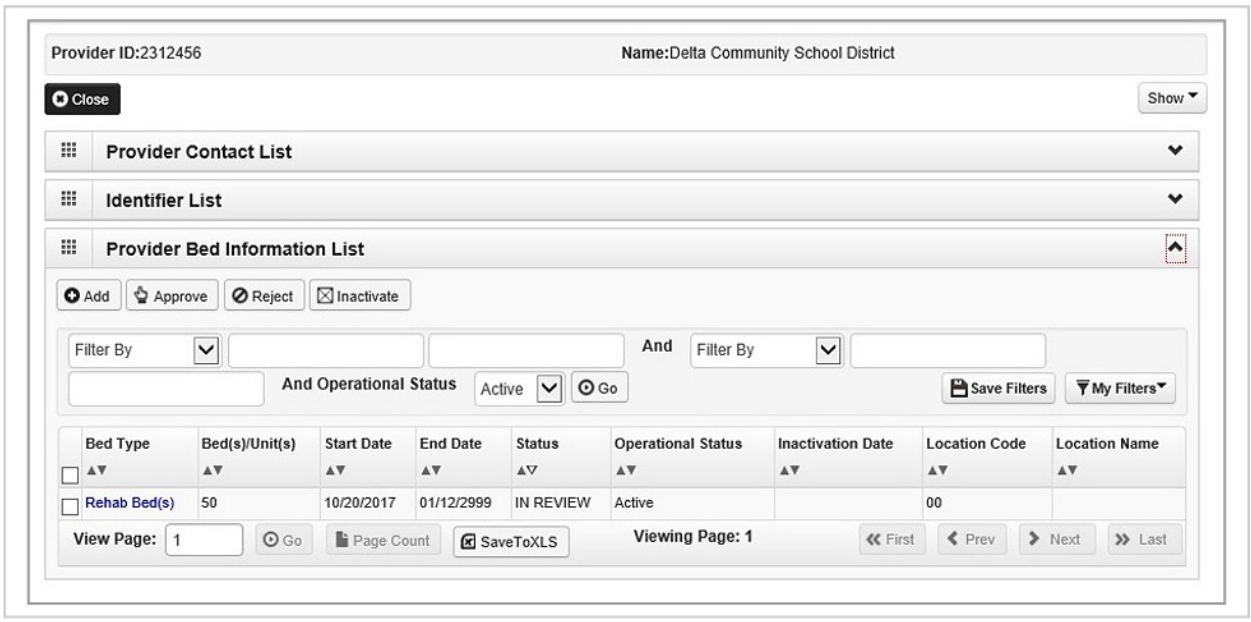


Figure 3.10.11-15. Associate Billing Provider Screen. The evoBrix PMIS gives the ability for the providers to associate with active Billing providers through this screen.

PMNT27

The Contractor's solution shall collect, store and maintain multiple provider contacts, including the contact name, title, contact type, telephone number, email address and location.

The evoBrix PMIS solution collects, stores, and maintains provider contact information. This is accomplished through the "Additional Information" step of the enrollment BPW as shown in Figure 3.10.11-16. Based on the Provider Type/Specialty/Subspecialty combination, the system can require specific contact type information. The contact details captured by the system include contact name, title, type, phone, email address, and location.



MTPSM-3-405

Figure 3.10.11-16 Additional Information Screen. The evoBrix PMIS solution collects, stores, and maintains provider contact information through this screen.

PMNT28

The Contractor's solution shall have the capability to indicate providers who are suspended or under review or investigation and a method for indicating the reason for the suspension or in review status.

evoBrix PMIS allows authorized State staff to suspend or terminate enrollment eligibility based on pre-defined State policy. There could be multiple reasons for suspending or terminating providers and the reason for the action is recorded via the indicator mechanism available in the system. Following are a few of the relevant indicators that are available for the use of the State staff:

- Sanctioned Source
- Disenrollment Reason Code
- Voluntary Termination
- License Expiry/Lapsed/Suspended
- Date of Death Verified Source

Each indicator comes with a remark and date fields to record and track any notes in chronological order as the state staff member is initiating an action.

PMNT29

The Contractor's solution shall allow authorized users to enter, view and update provider data (e.g., demographic data, taxonomy, banking information).

The evoBrix PMIS solution allows authorized State staff to enter, view, and modify provider data. Once a specific provider is located through the provider list page, the user can drill down on the provider detail

and perform modifications to provider data using expert mode. Figure 3.10.11-17 shows the Provider Detail page using which the State staff maintain provider data.

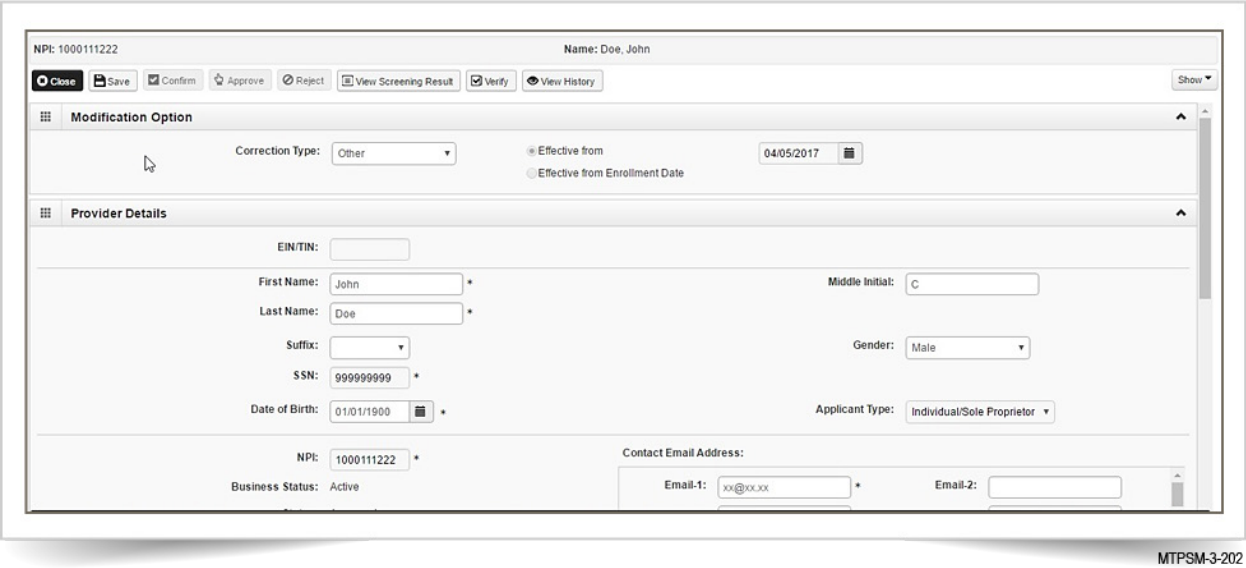


Figure 3.10.11-17. Provider Detail Screen. This screen gives the State staff the ability to view provider details and modify them in expert mode

PMNT30

The Contractor's solution shall allow authorized users to retroactively update provider data.

The evoBrix PMIS solution allows authorized staff to view and modify provider data. This includes the ability to update the data with retroactive effective period. This flexibility is limited to the staff with the appropriate privilege.

PMNT31

The Contractor's solution shall store and display geographic codes for provider locations.

evoBrix PMIS collects, stores, and displays geographic codes for provider locations.

PMNT32

The Contractor's solution shall have configurable event based workflow to instantiate information requests, correspondence or electronic notifications throughout the provider lifecycle.

Team CNSI's integrated workflow management solution supports improved automation, configurable work routing, and task management. It is table-driven with configurable rules, and supports task routing, assignment, and tracking capabilities.

Team CNSI's solution includes a configurable workflow process that provides the flexibility to define State-specific Business process rules. Provider Enrollment applications can be forwarded to specific

Organization Units or to a specific user within a group. Different combinations of Enrollment Types/Provider Types and Specialties can be configured to route the applications to departments specialized in that area. The workflow process can also be configured to initiate information requests throughout the provider lifecycle.

PMNT34

The Contractor's solution shall have the ability to suspend the provider record for providers that fail to respond to requests (e.g., revalidation, recertification, and updated licensure) in compliance with all federal and State policies and regulations.

As part of the revalidation process, evoBrix PMIS solution automatically dis-enrolls/end-dates the provider eligibility upon failure to revalidate, or renew any mandatory Certifications or Licenses which are required to meet Federal and State Policies and Regulations. evoBrix PMIS sends termination notice to providers upon termination of the provider eligibility. The termination process can be configured based on State-approved processes and procedures.

PMNT35

The Contractor's solution shall allow for mass updates to provider status based on criteria defined by the department (e.g., group practice changes) and initiate notification to the providers and appropriate programs.

The evoBrix PMIS solution provides the ability for authorized State staff to perform mass updates to provider status based on State defined criteria.

evoBrix PMIS has a batch-generation service that enables generation of correspondences for mass mailing based on user-selected criteria. For example, the system generates License Termination Letters to send to providers in the event of license expiry. Another example is the system generated Revalidation Termination Letter sent to the providers in the event of providers not completing the revalidation within the revalidation period.

PMNT36

The Contractor's solution shall have the ability to end date provider participation in specific programs while maintaining participation in other programs and initiate notification(s) to the provider, agency staff, and modules.

evoBrix PMIS gives the ability for providers to associate with multiple Manage Care Programs as part of the "Associate MCO Program" enrollment step. During this step, the effective begin and end dates are recorded for each program. The system provides the ability to end date provider participation in a specific program by updating the end date for that association. This will not affect the provider participation in the other programs.

PMNT37

The Contractor's solution shall record and display multiple instances of specific provider enrollment and

demographic data (e.g., license, eligibility period, physical address, CLIA levels) and provide access to historical provider record information.

evoBrix PMIS records and displays provider enrollment and demographic data. It maintains a complete audit trail of changes made to any data stored within the system, including but not limited to provider demographic data, license information, and eligibility period.

PMNT38

The Contractor's solution shall validate email addresses associated with the provider account through a confirmation and/or activation email process that requires the user to respond to activate the email account for agency communication.

evoBrix PMIS will validate email address entered by authorized user in the basic information step during enrollment process that requires the user to respond to activate email account for agency communications.

PMNT39

The Contractor's solution shall collect and maintain provider data necessary to support other module functions (e.g. claims processing, service authorizations, and reporting functions).

evoBrix PMIS collects and maintains provider data required to support other module functions such as claims processing, service authorizations, and reporting functions. For instance, provider specialty and mode of claim submission information required for claims processing are captured by evoBrix PMIS.

PMNT40

The Contractor's solution shall provide the ability to interface with external systems to automate verification and validation of provider information and credentials for enrollment, screening and monthly monitoring (e.g., CMS data matching, licensure, Social Security Administration's Death Master File, the National Plan and Provider Enumeration System (NPPES), the List of Excluded Individuals/Entities (LEIE), the Excluded Parties List System (EPLS)), and provide online alerts or notifications via workflow when adverse results or mismatches occur.

evoBrix PMIS offers PCS solution which provides both pre- and post-enrollment screening processes. The evoBrix PMIS PCS solution, in partnership with LexisNexis, provides full compliance with the ACA Provider Enrollment Screening requirements.

The evoBrix PMIS PCS solution screens providers against Federal databases such as OIG (for LEIE), SAM (EPLS). It also supports plugging in additional data sources such as MCSIS, CMS-MED sanction files.

Pre-enrollment screening results are available in real-time through online screens for the State staff to review.

PMNT41

The Contractor's solution shall require and capture termination reasons for all provider terminations.

The business status screen within the evoBrix PMIS allows authorized users to terminate the eligibility of providers by changing the provider business status. System will require and capture the reason for the status change (e.g., terminate/suspend due to sanctioning or licensing authority) in the remarks field. If a provider's eligibility is end-dated by the system as part the automated batch monitoring/screening process, it will set the appropriate indicators for the provider indicating the reason for termination.

PMNT42

The Contractor's solution shall collect, process and maintain the data elements necessary to enroll trading partners with the department to support HIPAA X12 transactions.

evoBrix PMIS allows users to establish trading partners in conformance with HIPAA standards. All submitters of EDI transactions including electronic claims will need to enroll as a Trading Partner and can select the HIPAA X12 transactions they choose to submit and receive.

Providers will be able to select their preferred method of claims submission in the Mode of Claims Submission step during the enrollment process. This enrollment step allows providers to select the submission method through EDI exchange or other methods like Paper or Direct Data Entry (DDE).

PMNT43

The Contractor's solution shall provide the ability to capture and store electronic payment information e.g., (credit card, bank account).

evoBrix PMIS provides the ability for providers to enter payment details during the enrollment process. Figure 3.10.11-18 shows the enrollment dialog for capturing payment details. After initial entry, the system suppresses all but the last four digits of the account number.

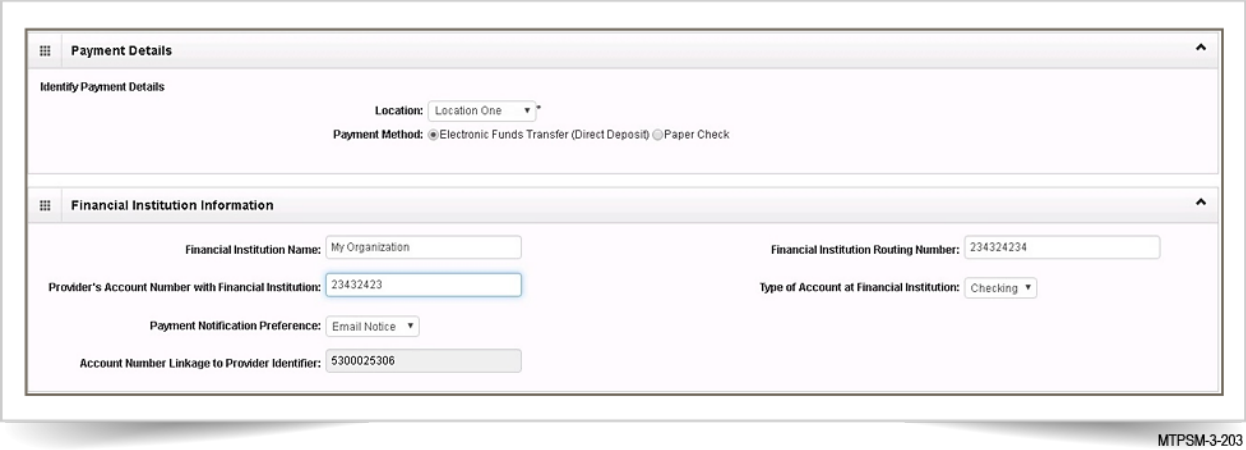


Figure 3.10.11-18. Provider Payment Preferences. In this example, the provider has elected electronic payment.

PMNT44

The Contractor's solution shall provide the ability to display payment information (e.g., provider administrative fees).

evoBrix PMIS provides the ability for providers to enter payment details during the enrollment process. After initial entry, the system suppresses all but the last four digits of the account number for display. evoBrix PMIS can also display the payment history for a provider.

PMNT45

The Contractor's solution shall provide the ability to automatically and manually unlink provider records determined to be unrelated.

The incomplete enrollment application is retained in evoBrix PMIS for 30 days. After an application has been started, provider applicants have 30 days to complete all the BPW steps and submit the application. After 30 days, an incomplete application will be automatically purged and the provider has to restart a new application. The purged application will be kept in the database until retention period for auditing purposes. This purge criterion can be configured in evoBrix PMIS to meet the State-specific retention policy.

The evoBrix PMIS centralized database eliminates duplicate enrollments using a single master record to contain all relationships the provider may have with the State. Even if a provider has multiple provider types, evoBrix PMIS retains the information under a single enrollment that is permanently linked to the provider's unique NPI and TIN combination.

The evoBrix PMIS editing functionality performs the following validations to ensure data integrity before the provider basic information can be accepted and saved:

- NPI Validation. evoBrix PMIS verifies against NPPES database to make sure the NPI, provider name, and provider entity type entered match to the data registered with NPPES.
- Duplicate Check. evoBrix PMIS verifies the entered data against the enrolled providers in the system to ensure that the NPI is not already associated with a previously enrolled provider.

The evoBrix PMIS solution also has the capability to perform additional checks, such as unique SSN validation, for atypical providers. The enrollments that are no longer required or valid could be end-dated by authorized user.

PMNT46

The Contractor's solution shall have the ability to assign classifications (e.g., provider type and specialty) to all providers including atypical providers.

evoBrix PMIS supports provider management to be controlled through a permissions matrix that define the specialties the State supports under different administrations/programs and the specific credentials, such as licensing, required by successful applicants for each defined enrollment type/specialty combination.

PMNT47

The Contractor's solution shall provide the ability to collect and maintain bed data (e.g. nursing home, hospital).

evoBrix PMIS provides ability to collect and maintain bed data at the primary location screen as shown in Figure 3.10.11-19.

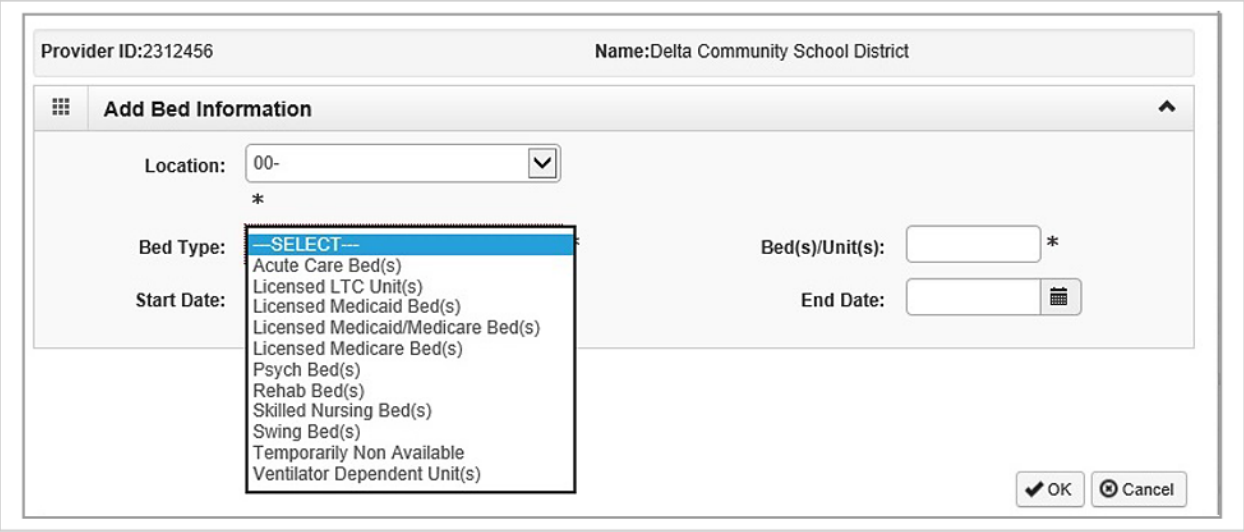


Figure 3.10.11-19. Add Bed Information Screen. User can enter bed information for the primary location using this screen.

PMNT48

The Contractor's solution shall provide the ability to collect conditional enrollment and maintenance data that is configurable by provider role (e.g., ORP, Rendering, Attending and Billing/Pay to Providers) and provider classification (e.g., case manager, physician, home health agency) and displays indicators on the provider record to distinguish the provider role(s) and classifications.

evoBrix PMIS captures provider role in Applicant Type field. The solution provides ability to configure enrollment and modification data/steps by Applicant Type (e.g., ORP, Rendering, Attending and Billing/Pay to Providers) and Provider Classification (e.g., case manager, physician, home health agency). Both Applicant Type and Provider Classification fields are displayed in basic information screen.

PMNT49

The Contractor's solution shall automate the identification of providers due to revalidate their enrollment information and initiate notification(s) to the provider, agency staff, and modules.

The evoBrix PMIS solution offers a streamlined, configurable process for automated provider revalidation according to State requirements. The evoBrix PMIS sends revalidation notices to begin the revalidation for each provider. The providers will have at least 30 days from the date of the revalidation

letter to complete the revalidation process. The providers are required to revalidate all of the enrollment steps by completing each step that is listed in the BPW screen.

evoBrix PMIS also sends reminder notices to each provider 90 days prior to the revalidation due date. evoBrix PMIS terminates enrollments automatically and sends termination notices for the providers who do not complete revalidation within 30 days. The 30-day revalidation period and 90-day reminder notice period are configurable based on DPHHS policy. evoBrix PMIS provides the ability to configure the five-year revalidation interval by risk category (high, moderate, and low) or by provider type/specialty.

PMNT50

The Contractor's solution shall support the ability to compare provider enrollment and revalidation information with PECOS if the provider is enrolled with Medicare. Depending on provider risk category, the solution shall verify completion of the fingerprint background check (if required), payment of application fee (if required) and verify Medicare ownership information matches the provider record in the provider module. If a mismatch is found, create an alert to the designated work group.

Based on the Risk Category, evoBrix PMIS will provide ability to verify completion of the fingerprint background check, payment of application fee, and compare ownership information with Medicare PECOS upon availability of data source. In the event of mismatch, the solution will provide an alert to the designated work group.

PMNT52

The Contractor's solution shall collect, validate and maintain Clinical Laboratory Improvement Amendments (CLIA) certification information including the level of certification, the specific procedures each laboratory is authorized to perform, effective and end dates, and location of the certification for use in claims adjudication.

The evoBrix PMIS solution mandates the provider to enter the CLIA certification information based on the provider's specialty. The evoBrix PMIS PCS solution will integrate with LexisNexis and other external data sources to validate the CLIA certification information.

PMNT53

The Contractor's solution shall have the ability to indicate providers using electronic funds transfer (EFT) and submitting claims electronically.

The evoBrix PMIS solution has a 'Warrant Type' indicator that specifies the mode of payment for providers. Providers will be able to select their preferred method of claims submission in the Mode of Claims Submission step. This step allows providers to select the submission method through EDI exchange or other methods like Paper or Direct Data Entry (DDE).

PMNT54

The Contractor's solution shall support communications (e.g., email, SMS, correspondence) to and from providers, track and monitor responses to department communications.

The evoBrix PMIS solution supports communications to providers through its Pitney Bowes EngageOne Base (formerly DOC1) correspondence module and through the "My Inbox" feature available within the evoBrix PMIS portal. The correspondence module also supports communications via email.

PMNT55

The Contractor shall ensure information exchanges are documented in trading partner agreements as specified in 45 CFR 162.915.

evoBrix PMIS requires provider users to accept Terms and Conditions before submitting new enrollment or changes to existing enrollment. Trading Partner Agreement to conduct business using HIPAA transactions as specified in 45 CFR 162.915 are captured in the Terms and Conditions content.

PMNT56

The Contractor's solution shall have the ability to assign an individual provider an unlimited number of valid provider classifications (e.g., physician-family practice, physician-oncologist, hospital-acute care, registered nurse-pediatrics).

evoBrix PMIS gives the ability to assign multiple specialty/subspecialty classification for providers based of the permission matrix configuration. Provider types/specialties are captured at the provider base location. The provider type/specialty and subspecialty is a matrix that can be configured based on the enrollment type.

PMNT57

The system shall allow a single provider to have more than one electronic submitter associated with their provider file, and designate one biller to receive 835 files

evoBrix PMIS allows providers to select billing agents and billing providers as part of the enrollment process. While selecting the billing providers and billing agent, the provider can authorize one billing agent to receive 835 files.

PMNT58

The Contractor's solution shall have the ability to automatically and manually link the unique provider number to other provider IDs used throughout the State enterprise (e.g. SABHRS or State Eligibility Systems IDs). The solution shall display all provider IDs.

evoBrix PMIS assigns a unique identifier called Provider ID for each provider who is participating in the State Medicaid System. This is generated at the time of enrollment approval (and also during the conversion process during which providers from the Medicaid Legacy System are brought into evoBrix PMIS). Other provider identifiers used throughout the State enterprise (e.g. SABHRS or State Eligibility Systems IDs) can be linked to the newly generated provider identifier within the evoBrix PMIS through a feature available called Identifiers. Legacy Provider ID is one such identifier that can be made available to other State Systems as part of a back-feed or other interfaces processes required by State.

PMNT60

The Contractor's solution shall be configurable to allow users to indicate the method of how required documentation will be submitted (e.g., mail and facsimile).

The evoBrix PMIS solution is configurable to allow users to indicate their preferred method for submitting documentation, including online upload, mail, or facsimile.

evoBrix PMIS provides the ability for providers to upload required documents as part of the Upload Document Step in the enrollment BPW. All the documents that are uploaded or received by Mail or Fax can be stored and archived in Team CNSI's Document Management System (DMS) which uses the IBM FileNet product.

PMNT61

The Contractor's solution shall have configurable workflow to present for validation, updates submitted online/electronically by specific criteria (e.g., program type, data type, risk level).

evoBrix PMIS provides the ability to enroll, re-enroll, modify, and revalidate provider data per the DPHHS provider enrollment requirements. The provider enrollment and maintenance process provides various capabilities including:

- Configure enrollment process workflow per state-defined criteria
- Perform enrollment process electronically
- Define industry standard provider types, specialties, and sub specialties; associate standard and non-standard taxonomies through a comprehensive permission matrix
- View/Upload attachments for uploading the supporting documentation such as copy of license, copy of any certifications with the enrollment application
- Enroll/Dis-enroll/Activate/Deactivate providers per state-provided criteria
- Collect enrollment fee for the institutional providers online payment service
- Track fingerprinting based on the provider risk category
- Support submission and processing of provider appeals and grievances including service requests tracking

evoBrix PMIS provides a decision management framework for administration that allows authorized users to configure, define, and maintain the business rules required for provider enrollment, disenrollment, re-enrollment, and maintenance activities as required by State policy. The decision management framework includes features that allow authorized users to perform the following activities:

- Define State-specific provider type and specialty/subspecialty combinations
- Configure mandatory, optional, and conditionally mandatory enrollment and re-enrollment data requirements by provider enrollment type and specialty
- Define and configure credentialing and re-credentialing rules for each unique provider type and specialty combination.

PMNT62

The Contractors solution shall support manual and automatic classification of a provider risk level status (limited to moderate to high) which shall trigger additional steps and screening as applicable.

evoBrix PMIS assigns a risk category to all provider enrollments: High, Moderate, or Limited. Prior to completing the enrollment processing, providers are subject to screening tasks based on their risk category. The assignment can be done automatically based on provider selection of Specialty/ Subspecialty at the time enrollment or modification or can be manually set by the state staff.

The screening requirement includes:

- Validation of disclosed individuals with the Office of Inspector General (OIG) Excluded Individuals database, the Excluded Parties List System (EPLS) and the Social Security Death Master List.
- In-state and out-of-state professional license verification.
- Clinical Laboratory Improvement Amendments (CLIA) and Drug Enforcement Administration (DEA) Certification verification.
- Proof of Medicare enrollment, if Medicare-enrolled.
- Validation of the NPI with the National Plan and Provider Enumeration System (NPPES).
- All providers classified as “High” and “Moderate” are subject to unscheduled and unannounced site visits. Periodic site visits are also required when existing providers re-validate their information with the timing based on the risk categorization.

Team CNSI’s PCS solution will integrate with LexisNexis and other external data sources to provide full compliance with the ACA Provider Enrollment Screening requirements during enrollment, re-enrollment, modifications, and revalidation processes.

PMNT63

The Contractor’s solution shall provide the capability for users to review enrollment and revalidation information prior to final submission of the enrollment or revalidated information.

The evoBrix PMIS solution captures the enrollment/revalidation information through BPW steps. The system provides the ability for the users to review the BPW steps before final submission of the enrollment or revalidation.

PMNT64

The Contractors solution shall support manual and automatic classification of a provider risk level status (limited to moderate to high) which shall trigger additional steps and screening as applicable.

evoBrix PMIS assigns a Risk Category to all provider enrollments automatically: High, Moderate, or Limited. The assignment can be done automatically based on provider selection of Specialty/Subspecialty at the time enrollment or modification or can be manually set by the state staff. Based on the Risk Category, the solution required triggers enrollment steps and screening process. For example, Fingerprinting is tracked based on the provider risk category.

PMNT65

The Contractor's solution shall capture and maintain at a minimum, the data set defined in Part 11 of the State Medicaid Manual and provider related TMSIS required fields.

The evoBrix PMIS solution maintains the minimum data set prescribed by Part 11 of the State Medicaid Manual and the required provider data fields as part of the provider enrollment and related records.

PMNT66

The Contractor shall collect and maintain certifications by specific industry standard or state policy (e.g., NCQA Certification and NCQA Certification Level).

The evoBrix PMIS solution provides the ability to collect, maintain certifications as part of the "Add License/Certifications/Other" step in the enrollment BPW in order to meet State requirements.

3.10.12 Self-Service Portal

This section addresses self-service portal requirements. The Provider Services module must support self-service provider enrollment and maintenance activities in addition to other self-service functions necessary to support day to day business functions including but not limited to; a provider inbox, interactive chat functionality, and a provider locator for both public and authenticated users to find actively enrolled providers based on specified criteria. The Offeror must describe their approach to meet each of the Self-Service Portal requirements defined in Attachment F, Requirements Matrix.

Team CNSI understands the State's requirements for a user friendly, convenient, dynamic, feature-rich portal with extensive self-service functionality for enrollment and maintenance activities. The web portals need to act as a window to the MT PSM and provide State staff and providers with an easy-to-use interface to conduct their MMIS business. Team CNSI's evoBrix PMIS provides a rich set of MITA-aligned features for provider enrollment, information management, and support functions. Team CNSI's evoBrix self-service portal provides a dynamic, information and feature-rich, interactive experience for State staff and external users. The solution combines a full-featured, secure, self-service portal with a comprehensive administrative framework to manage enrollment, disenrollment, inquiry, provider information maintenance, and provider support.

The Team CNSI Advantage

Team CNSI's evoBrix PMIS provides a standards-based, intuitive, feature-rich, and secure web portal solution that meets the individual needs of the State and the providers.

- Online portal furnishes a rich set of self-service functions to the provider community
- Fully-automated online enrollment and update process
- Same-day enrollment submission, review, and decision making through self-service, automation, and real-time credentialing

MTPSM-3-128

evoBrix PMIS modernizes and streamlines the many paper and manual processes that had been used in the legacy environment, while substantially increasing the ability to respond to provider requests and improve customer service. Its centralized database virtually eliminates duplicate enrollments, using a single master record to contain all relationships the provider may have with the DPHHS. Even if a provider has multiple provider types, the evoBrix PMIS solution retains the information under a single enrollment that is permanently linked to the provider's unique NPI and Taxpayer Identification Number (TIN).

The self-service portal has a configurable External Links feature that will store the links to the external applications that State staff or providers will need to access from the application. The external links are configurable separately for both State staff and providers to access external content such as In-State License, Taxonomy Codes, State Plan, Program Policy information, and Medicaid Information Bulletins and to provide links to external programs such as low-income service and programs, health plans, vital stats, waiver programs, and aging services.

The self-service portal displays inbox details for authorized users. The inbox has announcements, alerts, and other reminders. Users can acknowledge the announcement by simply selecting the announcement and deleting it from their inbox.

The self-service portal provides multiple time-saving features. It offloads the data entry workload from enrollment specialists to the provider. The easy-to-use business process wizards (BPWs) and online, real-time edits greatly reduce keying errors. All data entry is performed through data entry screens on the self-service portal, thus reducing the volume of issues and delays resulting from loss of forms in the mail, as well as the amount of time needed to process new applications and maintenance requests. The evoBrix PMIS self-service portal is highly scalable, and provides the ability to customize by adding more online capabilities to submit claims; inquire about claims status, member status and eligibility, or remittance advice; and support dynamic provider access to status, billing information, and online help, thereby reducing administrative costs.

The self-service portal offers the following benefits to providers:

- Improved access for participating providers who can now interact with the State's Medicaid program 24x7x365 rather than waiting in a call queue during business hours
- Reduced provider call volumes because they can check on the status of their application and request changes to their records directly through the self-service features
- Improved customer service because of shorter processing cycles

The self-service portal utilizes the evoBrix security platform that has the capability to administer and maintain user accounts. It has built-in functionality to allow new user registrations for both providers and State staff, and includes a workflow feature to route new user registrations to authorized State staff for their review. For providers who are successfully enrolled in the DPHHS Medicaid program, new application and provider data updates may be initiated through the provider portal. Providers must have a system-issued domain name and profile to access the provider portal. After successful enrollment, providers can use the provider portal to do the following:

- Initiate enrollment for another provider
- Update enrolled provider information
- Retrieve correspondence
- Self-administer provider domain access and user access
- Access to external systems via External Links

Interactive Chat

Team CNSI's evoBrix platform includes an online Interactive Chat solution. The solution aims to improve the customer experience, reduce costs with fewer customer service call center staff, give faster resolution to problems, and better understand customer concerns or issues. The solution allows enrolled and authenticated users to chat with a designated representative within the online self-service portal. The authorized user can initiate a chat session using a link embedded in the provider portal. The solution records the session, providing DPHHS staff the ability to access the details for reference and audit.

Online Provider Directory (OPD)

The evoBrix PMIS Online Provider Directory (OPD) provides State Medicaid provider information in a directory structure, as a listing of healthcare providers classified by provider type, specialties, credentials, demographics, service locations, affiliations, network, and contracts, along with details regarding communications, practice profile, and quality summary. This includes both individual providers, such as physicians, nurses, or pharmacists, and organizational providers, such as hospitals, clinics, agencies, and Managed Care Organizations. The OPD allows the user to search on multiple provider attributes to locate a specific enrolled provider (e.g., NPI) or group of providers sharing a common set of attributes (e.g., zip code and taxonomy). It also provides the ability to geographically locate providers in proximity to the user's current location or other location-based search attributes. This helps both public and authenticated users to find actively enrolled providers based on search criteria.

The ability for health care entities to use one trusted, single, and complete source of provider data is essential to improving system efficiencies and patient care coordination, while helping reduce costs. The public-facing provider directory, and its search capabilities, represent the most visible and key function of the broader evoBrix PMIS solution. The integrated provider data maintained within evoBrix PMIS acts as the backbone for the OPD.

Below are some of the key benefits of OPD:

- Support for coordinated care – Offers a complete one-stop option to find who, where, and how to contact other providers and care team members. Gives providers access to a rich source of accurate, complete data to find other providers (and their health information exchange addresses) for patient referrals and discharge planning.
- Increase efficiencies – Reduces duplication, as well as time and costs invested in managing and keeping the same provider information up to date in multiple directories.
- Improve security and privacy – Providers can have confidence that information they are relying on for patient care is correct.

evoBrix PMIS provides a standards-based, open, extensible platform for developing the OPD software infrastructure using a Service Oriented Architecture (SOA) approach. The core architecture leverages the Enterprise Service Bus (ESB) features within the SOA framework and provides an integration backbone that connects applications and services without directly accessing the underlying systems. It is capable of handling common industry standard service requests such as Simple Object Access Protocol (SOAP) and Representational State Transfer (REST). The ESB infrastructure allows the evoBrix PMIS solution to avoid point-to-point communication with different system(s) and/or components, in this case, the provider directory system.

The OPD is built to translate a user's search queries into Web Service calls on the evoBrix PMIS solution. The communication between the OPD and evoBrix PMIS is designed to be flexible to allow for local mapping of taxonomies to user-friendly descriptions. Web Service invocation serves as the channel for relaying real-time updates to the provider information from the OPD system back to evoBrix PMIS.

The solution is aligned with industry interoperability standards through CNSI's participation in MITA and HL7 standards as well as our continued participation in other key interoperability standards and projects.

Figure 3.10.12-1 shows the provider search page, displaying the basic search criteria.

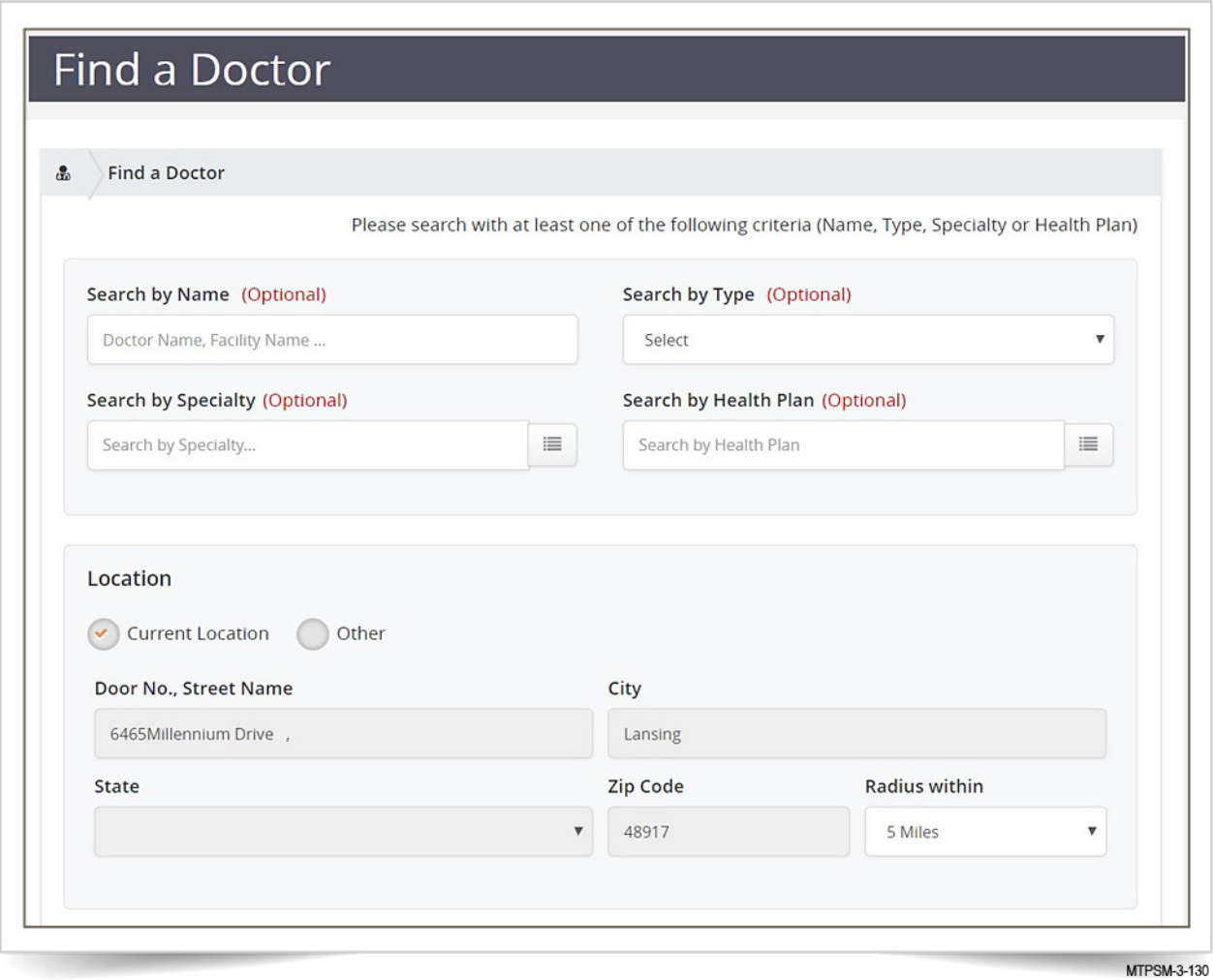


Figure 3.10.12-1. Provider Search Page. This page can be used by the public and authenticated users to search for providers using basic search criteria.

Figure 3.10.12-2 illustrates the search hint capability provided within the provider search page.

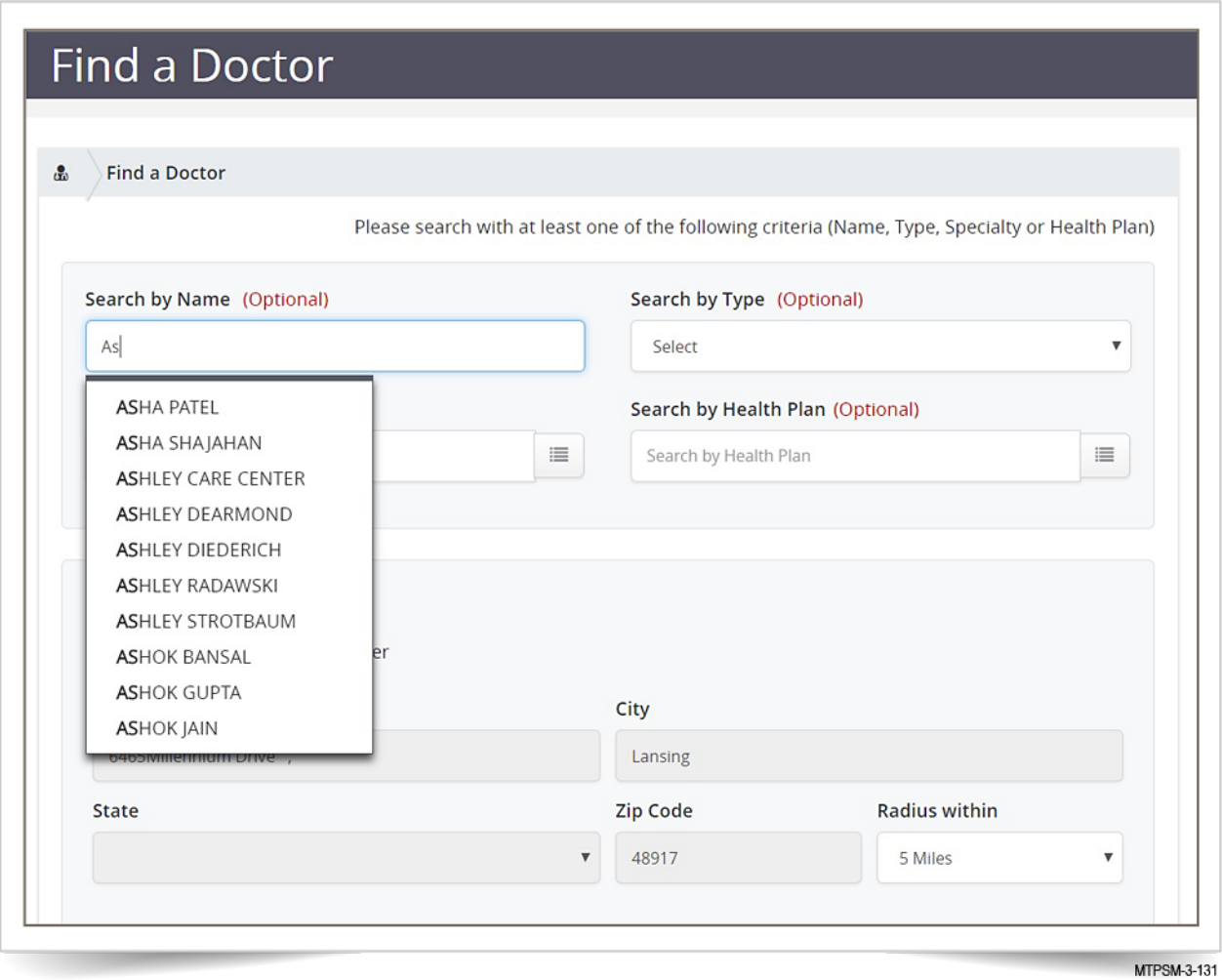


Figure 3.10.12-2. Provider Search Page Showing Search Hints. The hint feature prompts the user with matching results as the user types in the name of the provider.

Figure 3.10.12-3 shows the additional search criteria within the provider search page.

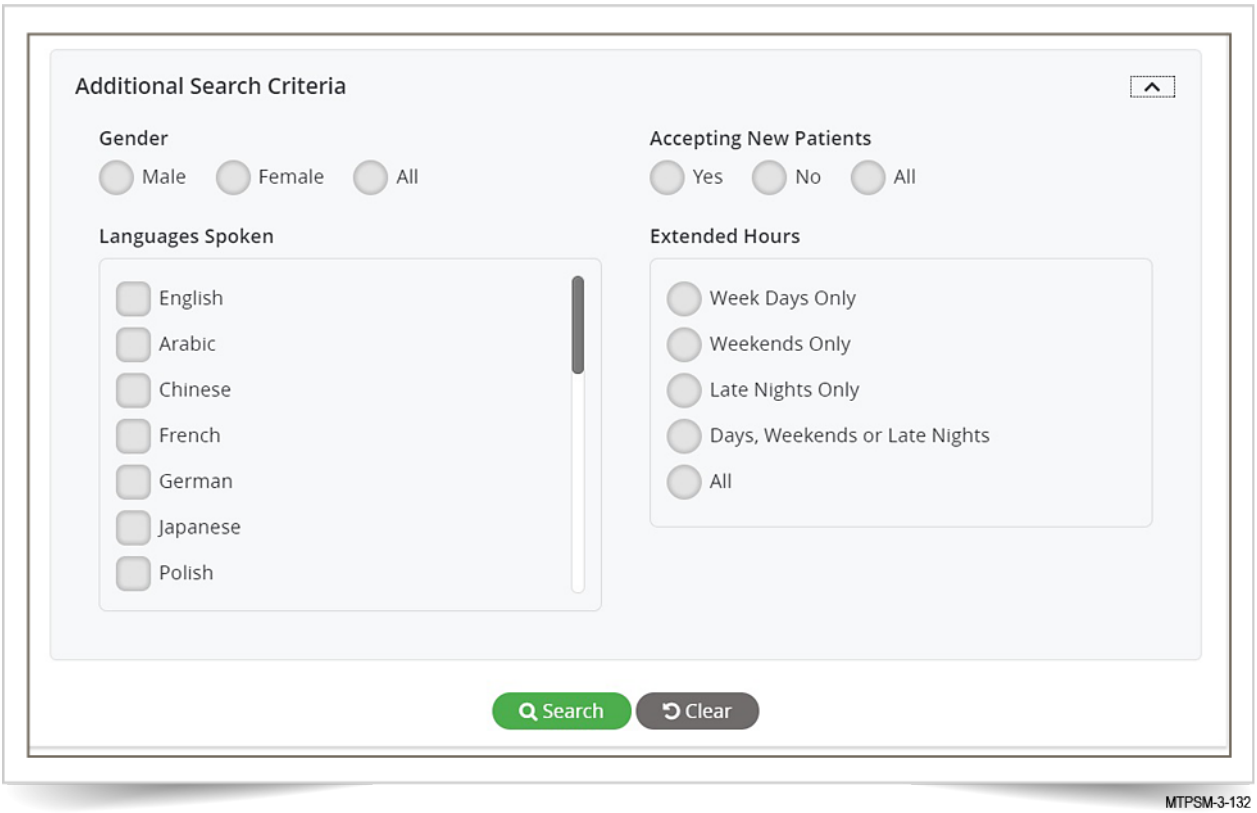


Figure 3.10.12-3. Additional Search Criteria. This section displays the additional search criteria to narrow the search results.

Figure 3.10.12-4 shows the map area within the provider search page, that aligns with the user's current location or the location specified as the search criteria.

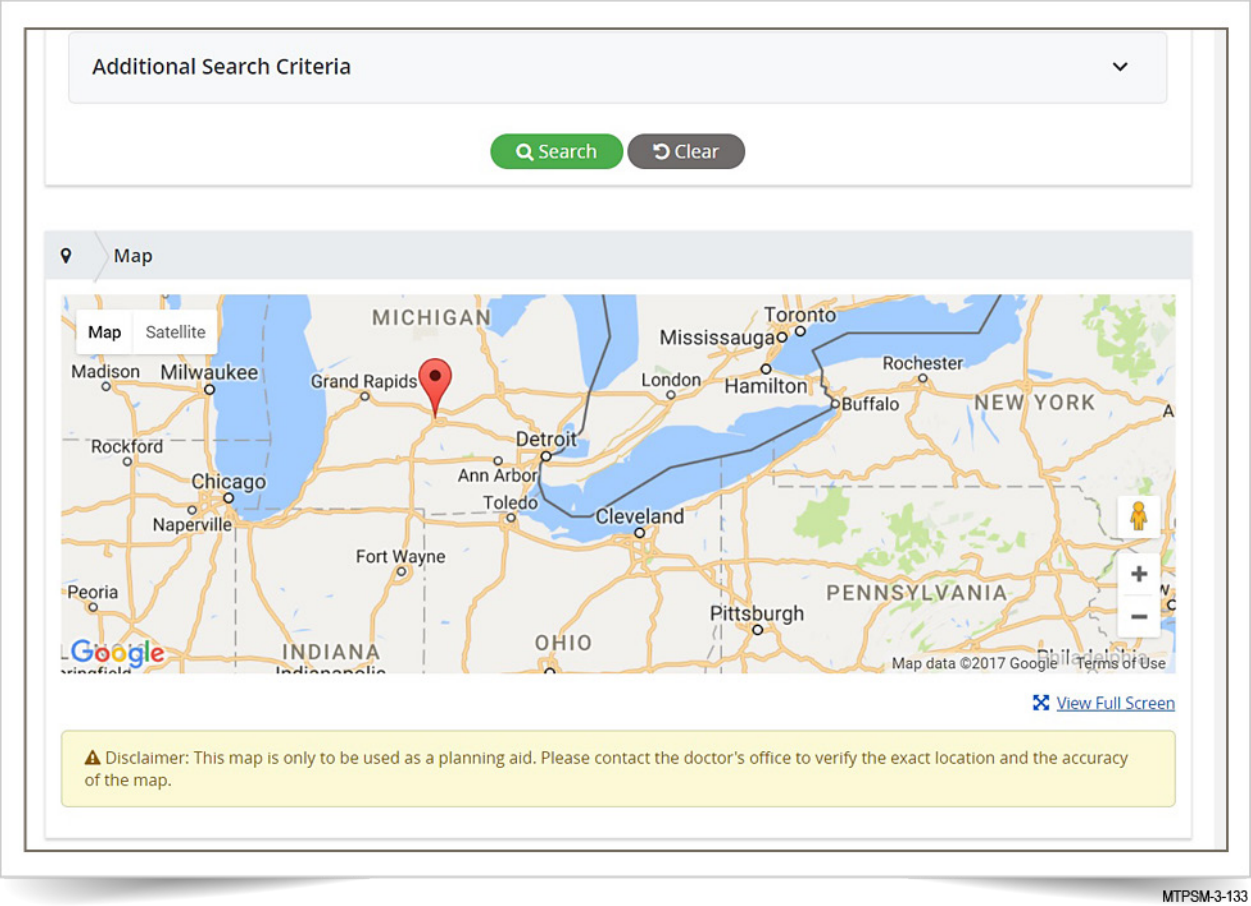


Figure 3.10.12-4. Map Section Within the Provider Search Page. This provides a visual map display to locate the providers.

Figure 3.10.12-5 shows the provider search results page. The user is presented with paginated search results along with available actions such as Modify Search and *Start Over*.

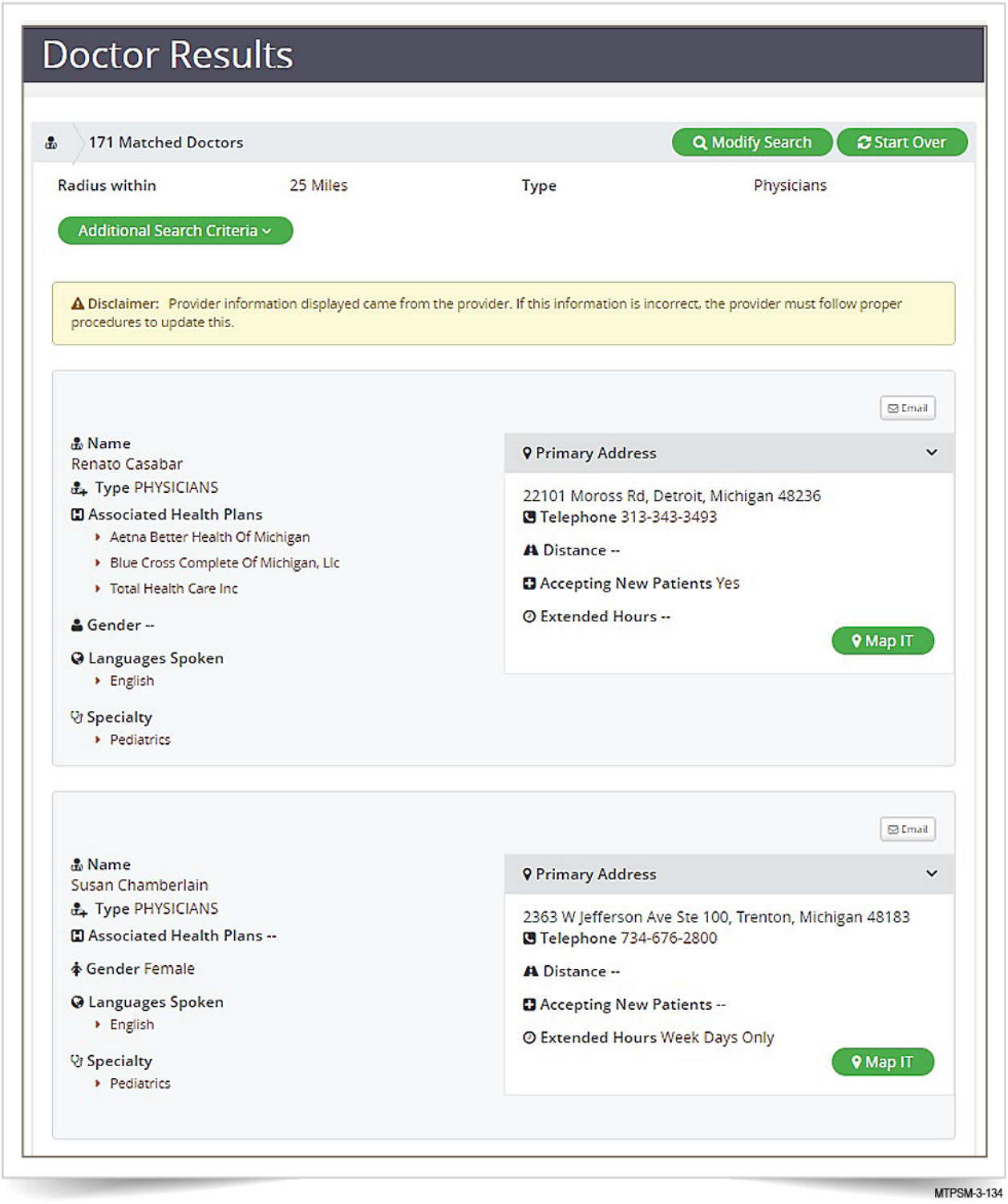


Figure 3.10.12-5. Provider Search Results Page. This displays the search results matching the criteria entered by the user.

PSER01

The Contractor's solution shall provide a self-service tool that will allow authenticated users to search by provider name (including phonetic search), NPI/API, network(s), location(s) (including city, state and zip code), provider classification(s), provider role, all languages spoken/language accommodations (e.g., English, Spanish, American Sign Language (ASL)), accessibility, gender, and whether or not a provider is accepting new patients. At a minimum the results display shall include; provider name, locations, phone numbers, provider classification(s), provider role, network(s), all languages spoken/language accommodations (e.g., English, Spanish, American Sign Language (ASL)), office hours, accessibility, whether or not a provider is accepting new patients, and any restrictions on the freedom of choice among providers in the public provider locator (e.g., ages served, gender).

evoBrix PMIS allows authorized users to access the robust Provider List screen feature from the self-service portal, a powerful function within evoBrix PMIS solution. The Provider List screen allows the user to search on multiple provider attributes to locate a specific enrolled provider (e.g., NPI) or group of providers sharing a common set of attributes (e.g., zip code and specialty). As shown in Figure 3.10.12-6, the Provider List page has three primary filters and two secondary filters, Identifier and Indicator. The user can save favorite search criteria by selecting the Save Filters button. Saved filters are retrieved under the My Filters dropdown. The list retrieved may be exported to Excel for additional analysis using the Save to XLS button. The sorting functionality on the list page allows the user to display the data in reverse chronological order.

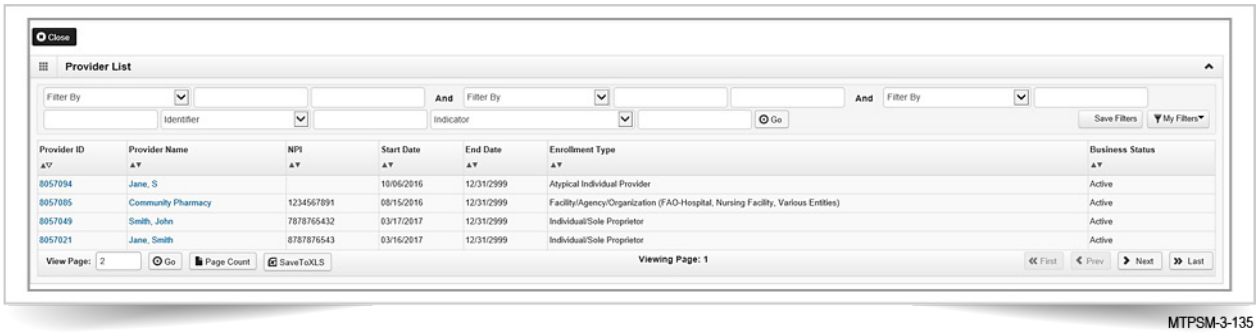


Figure 3.10.12-6. Provider List Page Showing Filter Capability. This screen highlights the three major filters the secondary filters, the Save Filters and My Filter retrievals, and Save to XLS features.

The evoBrix PMIS module has primary filters for the following:

- Applicant Type (Sole Proprietor, Rendering/Servicing Only, or Ordering/Referring/Prescribing Only)
- Application ID
- Business Status
- Business Eligibility Date Range
- Contract Number
- Program Name
- Enrollment Type
- Gender
- Handicapped Accessible
- License/Certification Type
- County
- Zip Code

- State/Province
- Town
- Phone Number
- NPI
- Primary Specialty
- Provider ID
- Provider Name
- Provider Specialty
- Provider Subspecialty
- Provider Type
- Revalidation Status
- Risk Category
- SSN/EIN/TIN
- Taxonomy
- Language Spoken

evoBrix PMIS has secondary filters for:

- Identifiers
  - Legacy Medicaid Provider ID
  - Legacy Medicaid Provider Type
  - Legacy social service program provider ID number Pharmacy Store Number
  - NCPDP Number
  - National Association of Boards of Pharmacy (NABP) number
- Indicators
  - Beneficiary Monitoring Program
  - License Name Match
  - License Status
  - Date of Death Verified Source
  - Delete Indicator
  - Disenrollment Reason Code
  - Finger Printing Status
  - Medicaid Interim Payment (MIP)
  - NCPDP Name Verified
  - Risk Level
  - Sanctioned Source
  - Screening Status
  - Servicing Type
  - Site Visit By
  - State Indicator
  - Stop Payment
  - Suspended
  - Valid EIN/TIN
  - Valid NPI
  - Valid Name
  - Valid SSN
  - Voluntary Termination
  - W9 Indicator

©2017 CNSI

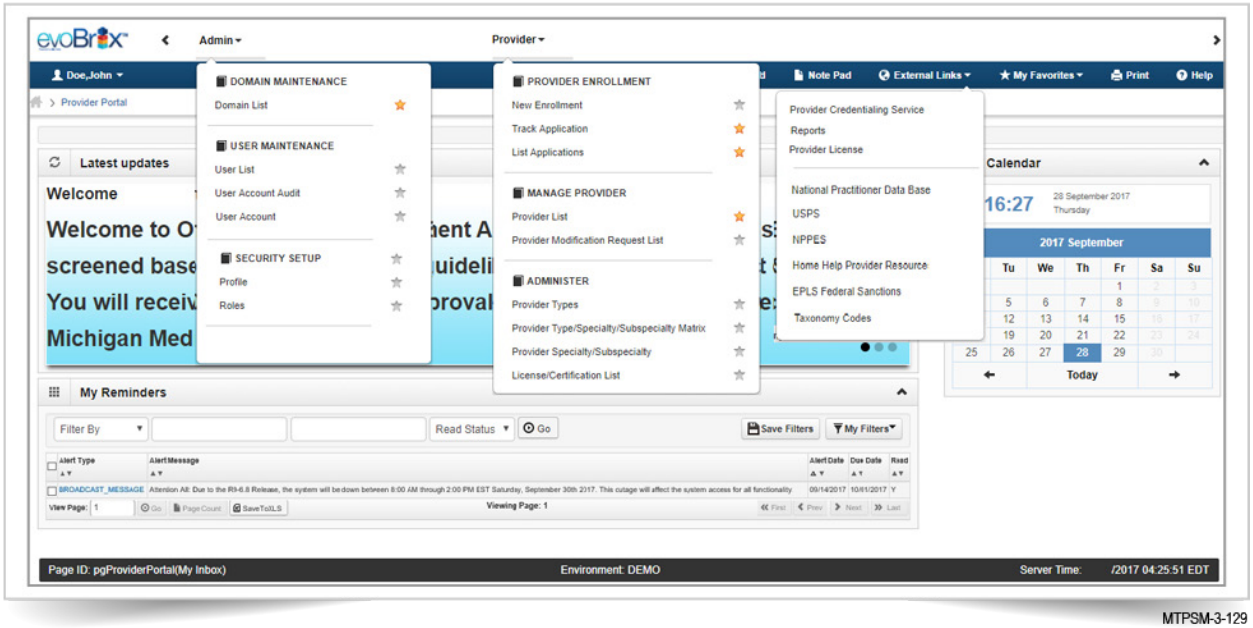
- Warrant Suppress-Fed Rpt
- Warrant Suppress-Not Fed Rpt
- Warrant Type

Once the specific provider is located on the provider list page, the user can drill down on the provider detail to view enrollment information including but not limited to provider name, locations, phone numbers, provider classifications, network associations, languages spoken, office hours, accessibility, and whether they are accepting new patients. Authorized users can perform functions such as changing provider data including demographics, location details, eligibility dates, associations, specialty/subspecialty, and license/certification.

PSER08

The Contractor's solution shall provide an online self-service tool for providers to access a provider inbox for messages and notices. The solution shall provide the ability to send, receive, and respond to messages.

The evoBrix online self-service portal displays inbox messages and banner notices for providers and State users. The inbox has announcements, alerts, and other reminders. Users can acknowledge the announcement by simply selecting the announcement and deleting it from their inbox. Figure 3.10.12-7 also highlights the inbox capability under My Reminders panel. Team CNSI's evoBrix platform includes an online Interactive Chat solution. The solution allows enrolled and authenticated users to chat with a designated representative within the online self-service portal. The authorized user can initiate a chat session using a link embedded in the provider portal. The solution records the session, providing internal staff the ability to access the details for reference and audit.



MTPSM-3-129

Figure 3.10.12-7. Self-service Portal View of Banner Message, Inbox Message, and Menu Items. This screen shows the list of Provider Enrollment menu functions and My Inbox message functions for State staff and providers.

PSER09

The Contractor's solution shall provide an online self-service tool for providers to add or remove provider account users and change user roles for all self-service functions.

The self-service portal utilizes the evoBrix security platform, which has the capability to administer and maintain user accounts. It has built-in functionality to allow an authorized user to add, remove, or inactivate a provider user account and change user roles for all self-service functions as shown in Figure 3.10.12-8 and Figure 3.10.12-9.

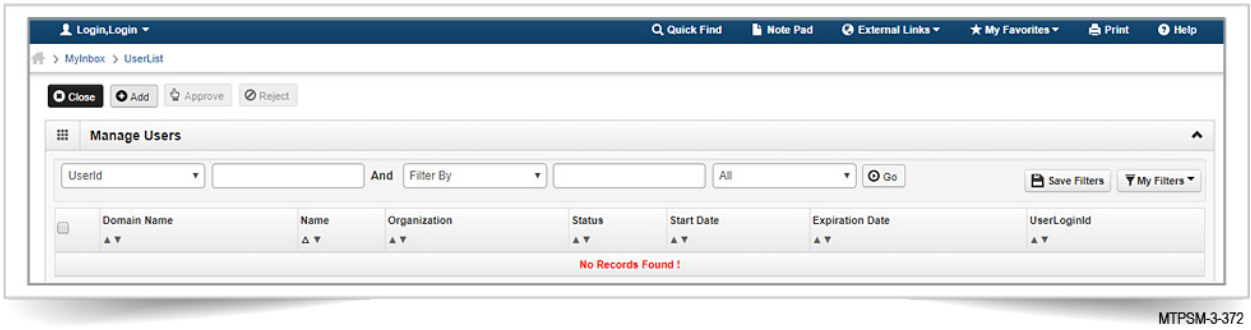


Figure 3.10.12-8. Manage Users Screen. Authorized users can add, remove, or inactivate user accounts through this screen.

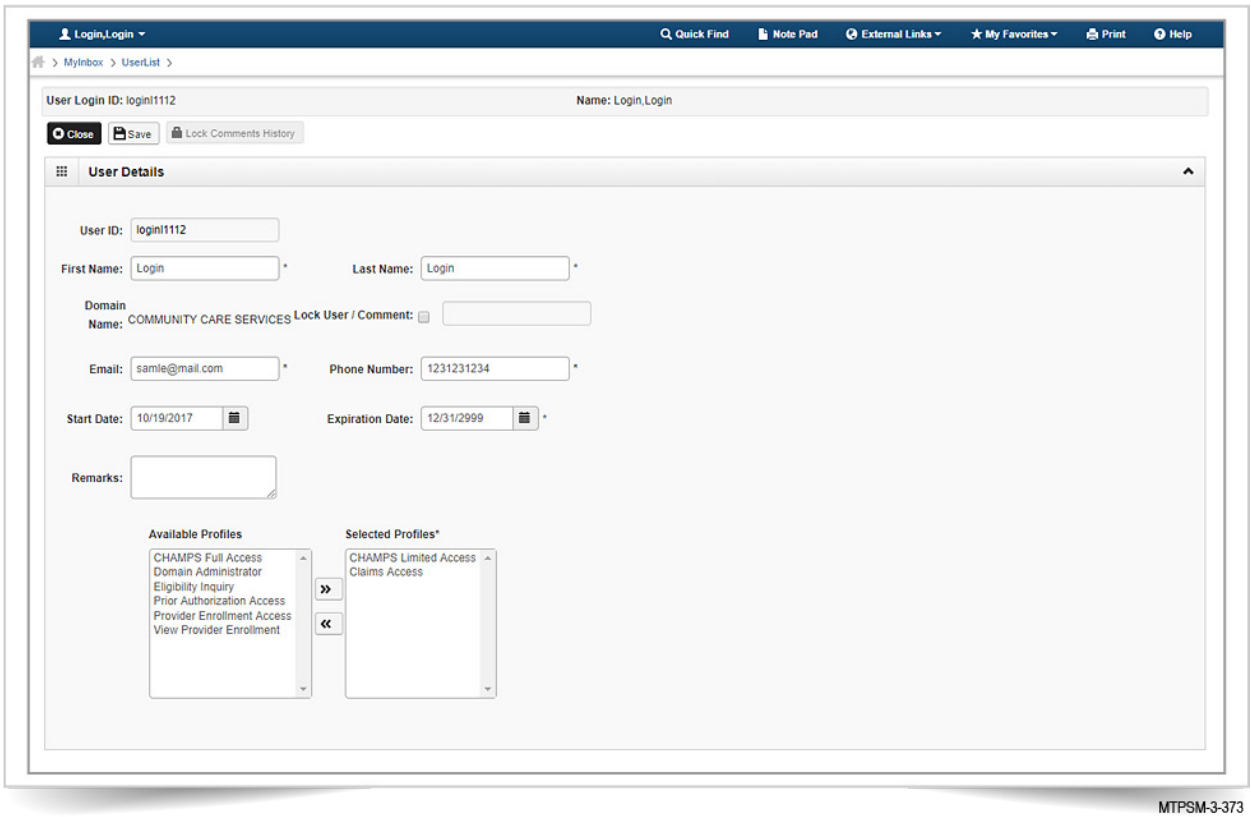


Figure 3.10.12-9. Maintain User Details Screen. Authorized users can maintain user details and associated profiles through this screen.

PSER10

The Contractor's solution shall allow individual practitioners to submit a request to link or unlink an affiliation with a billing provider. Each relationship shall include an effective date when initiated and an end date when the affiliation is terminated.

evoBrix PMIS allows authorized individual practitioners to submit a request to link or unlink an affiliation with a billing provider through the online self-service portal, as shown in Figure 3.10.12-10. The evoBrix PMIS data model is designed to capture effective date ranges for each affiliation and provides the ability to update the effective end date upon termination.

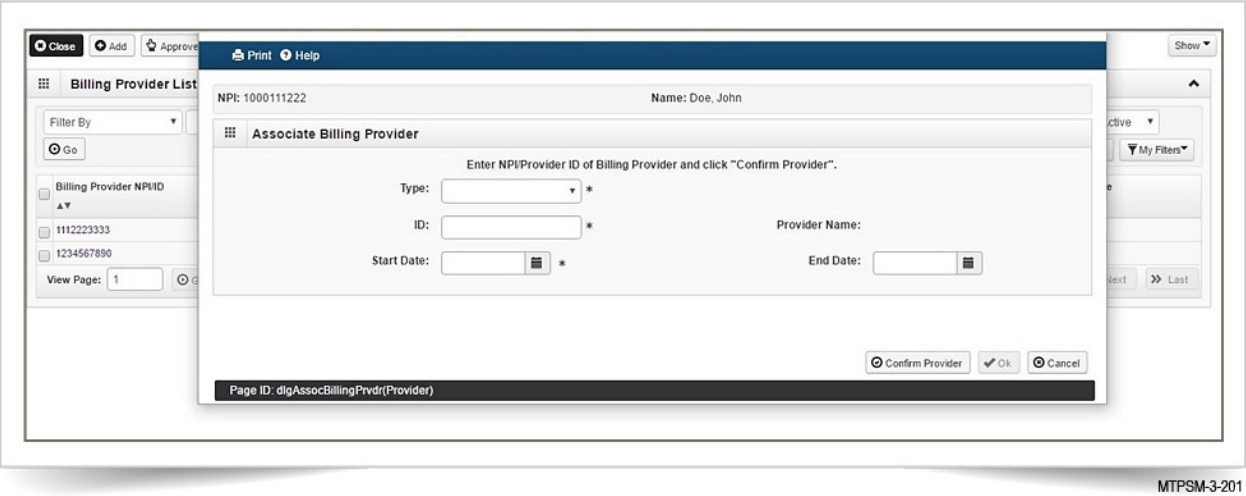


Figure 3.10.12-10. Associate Billing Provider Screen. evoBrix PMIS gives the ability for the providers to associate with active Billing providers through this screen.

PSER11

The Contractor's solution shall accept, validate and store new and updated provider information entered through the Provider Self Service tool.

evoBrix PMIS provides the ability for authorized staff and providers to view and perform updates to enrollment information through web-based data entry screens. The evoBrix PMIS solution provides the ability to accept, validate, and store new enrollments as well as modifications to existing enrollments entered through the self-service portal. Please refer to Section 3.10.11, Maintenance, for more details on provider maintenance functionality.

PSER12

The Contractor's solution shall allow authorized billing providers to link and unlink individual practitioners from and to billing providers with the ability to link an individual provider to multiple billing providers. Each relationship shall include an effective date when initiated and an end date associated with the termination of the affiliation.

evoBrix PMIS allows authorized billing providers to submit a request to link or unlink an affiliation with one or more individual practitioners through online self-service portal, as shown in Figure 3.10.12-10. The evoBrix PMIS data model is designed to capture effective date ranges for each affiliation and provides the ability to update the effective end date upon termination.

PSER15

The Contractor's solution shall provide online interactive chat functionality as a reliable transaction channel that allows enrolled and authenticated users to chat directly with a customer care representative. The chat session shall be recorded, stored, and accessible to internal staff for reference.

Team CNSI's evoBrix platform includes an online Interactive Chat solution. The chat process flow is depicted in Figure 3.10.12-11. The solution aims to improve the customer experience, reduce costs with fewer customer service call center staff, give faster resolution to problems, and better understand customer concerns or issues. The solution allows enrolled and authenticated users to chat with a designated representative within the online self-service portal. The authorized user can initiate a chat session using a link embedded in the provider portal. The solution records the session, providing internal staff the ability to access the details for reference and audit.



Figure 3.10.12-11. Chat Process Flow. Overview of the chat session life cycle between a client and agent using the evoBrix chat solution.

All chat session transactions are stored and archived for future references and auditing purposes. Both customers and staff can view the history, as shown in Figure 3.10.12-12.

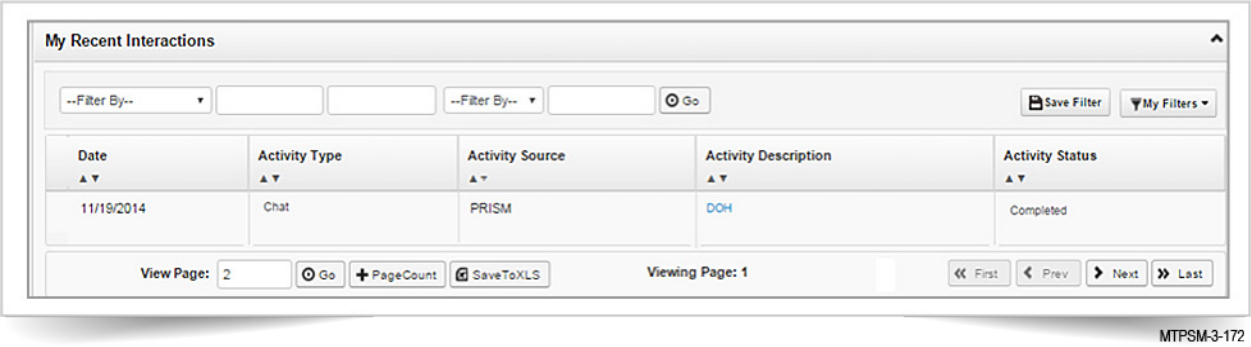


Figure 3.10.12-12. Chat Session History. The solution provides ability for authorized users to view chat history.

PSER16

The Contractor's solution shall include a configurable self-service tool that allows active and inactive providers to update and validate their provider record through direct data entry via the web, based on selected criteria.

The evoBrix PMIS allows authorized active and inactive providers to update and validate enrollment information through self-service direct data entry screens based on the selected criteria. Please refer to Section 3.10.11, Maintenance, for more details on provider maintenance functionality.

PSER17

The Contractor's solution shall a provide public provider search feature that will allow users to search by provider name (including phonetic search), network, location(s) (including city, state and zip code), provider classification(s), all languages spoken/language accommodations (e.g., English, Spanish, American Sign Language (ASL)), accessibility, gender, and whether or not a provider is accepting new patients. At a minimum the results display shall include; provider name, network(s) location(s), phone numbers, provider classifications, all languages spoken/language accommodations (e.g., English, Spanish, American Sign Language (ASL)), office hours, accessibility, whether or not a provider is accepting new patients, and any restrictions on the freedom of choice among providers in the public provider locator (e.g., ages served, gender).

The evoBrix Online Provider Directory (OPD) allows the authorized user to search on multiple provider attributes to locate a specific enrolled provider (e.g., NPI) or group of providers sharing a common set of attributes (e.g., zip code and taxonomy). The search feature allows user to search by provider name (including phonetic search), network, location (including city, state and zip code), provider classification (Provider Type and Specialty), languages spoken, accessibility, gender, and whether they are accepting new patients. It also provides the ability to geographically locate providers in proximity to the user's current location or other location-based search attributes. This helps both public and authenticated users to find actively enrolled providers based on search criteria.

The solution displays provider details not limited to provider name, network, location, phone numbers, provider classifications, languages spoken, office hours, accessibility, and whether they are accepting new patients, after matching the criteria entered by the user.

PSER22

The Contractor's solution shall provide online key contact information at a minimum by program type and business process.

evoBrix PMIS provides the ability to capture key contact information in the enrollment process by program type and business process, as shown in Figure 3.10.12-13.

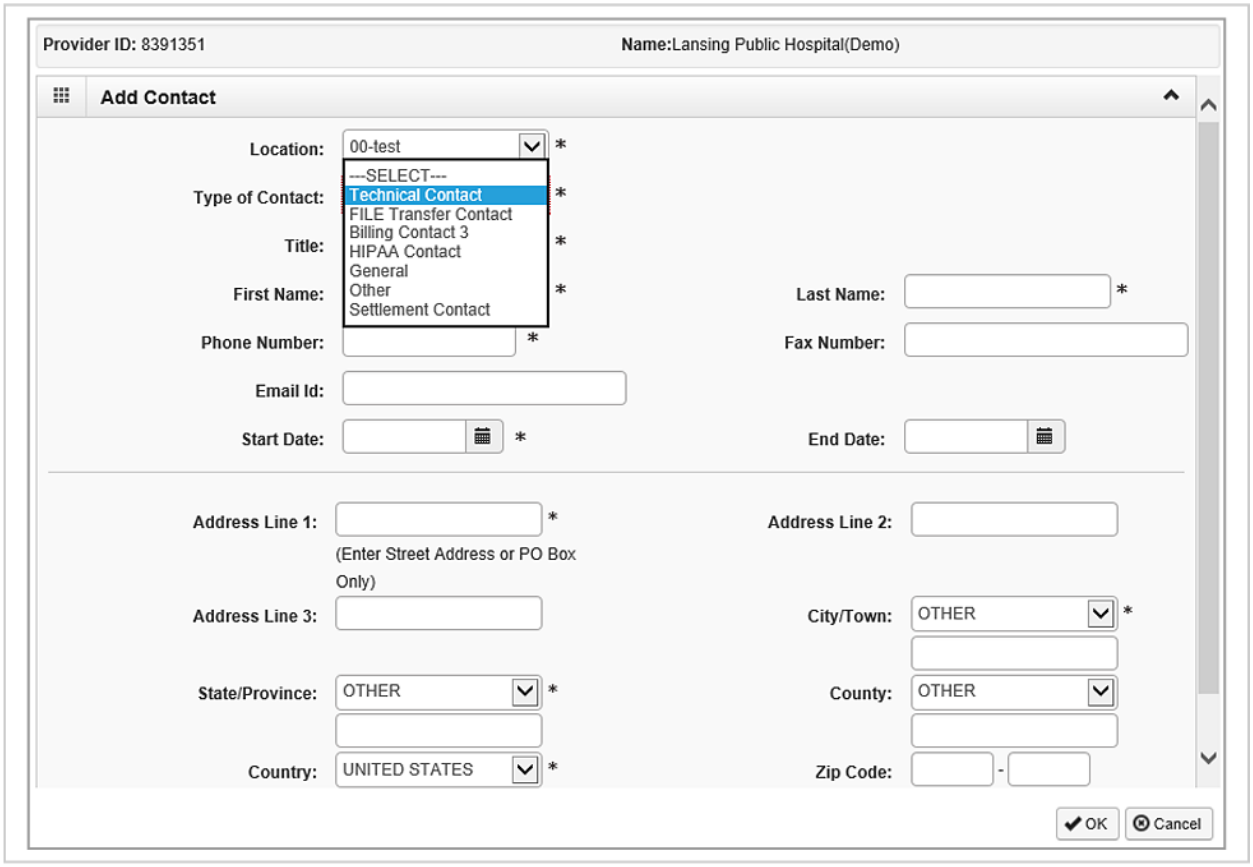


Figure 3.10.12-13. Add Contact Screen. evoBrix PMIS gives the ability to capture contact information during the enrollment process.

PSER25

The Contractor's solution shall provide links to relevant web resources (e.g., State and Federal websites, and other entities determined by the State to be appropriate for the self-service portal).

The evoBrix PMIS self-service portal has a configurable External Links feature, as shown in Figure 3.10.12-7, to web resources that will store the links to the external applications that State staff or

providers will need to access from the application. The external links are configurable separately for both State staff and providers to access external content such as In-State License, Taxonomy Codes, State Plan, Program Policy information, Medicaid Information Bulletins, and to provide links to external programs such as low-income services and programs, health plans, vital stats, waiver programs, and aging services.

PSER26

The Contractor's solution shall allow enrolled providers, enrolled trading partners, State users, and other users designated by the State, access to the secure areas of the self-service portal following successful authentication through single sign-on.

The evoBrix PMIS solution supports access management capabilities including authorization and seamless integration with the DPHHS Single Sign-On. The solution offers a role-based security model to enforce security and privacy of data through the use of profiles, as shown in Figure 3.10.12-9. The request originating from evoBrix PMIS is validated and the response is encrypted to ensure the protection of the data being transferred through the network. History of the data accessed is maintained for audit trail. Also, role-based access is not only limited to the validation at the time of login but also applied at the data element level, whereby only users such as enrolled providers, trading partners, State staff, and others designated by State with authenticated roles can access that data, avoiding breach of data privacy.

evoBrix RBAC security framework comes bundled with a user interface that allows authorized users to manage role-based and group-based security at the data element/field level. The evoBrix Security Framework is implemented through the conceptual network of user accounts, domains, profiles, roles, pages, and page controls. Each user within the evoBrix PMIS solution is associated with a unique user account. User domains map to departments within an organization. Users are required to select a domain when they are registering to access the system. Profiles control user access to the evoBrix PMIS screens and associated functionality. Each profile may be associated with one or more roles. A role is granted access to specific pages and page controls within those pages.

Access is defined at four levels:

- No Access: A role does not have any access to a given page and therefore cannot access it.
- View Only Access: A role is granted with view only access to a page.
- Full Access: A role is granted full access to a page, including the ability to modify data elements or invoke actions.
- Controlled Access: A role has limited access to a page and can only view or update specific elements within the page. Security is defined at the level of page (data) elements or controls. Privileges for each page element are defined as No Access, View Only, and Full Access.

PSER28

The Contractors solution shall create and present a tracking or confirmation number when provider information is updated via the self-service portal.

evoBrix PMIS generates a unique 14-digit Application ID as a tracking number which allows providers to track and resume an incomplete application via self-service portal, as shown in Figure 3.10.12-14. The application number also allows providers to check on the status of their submitted application.

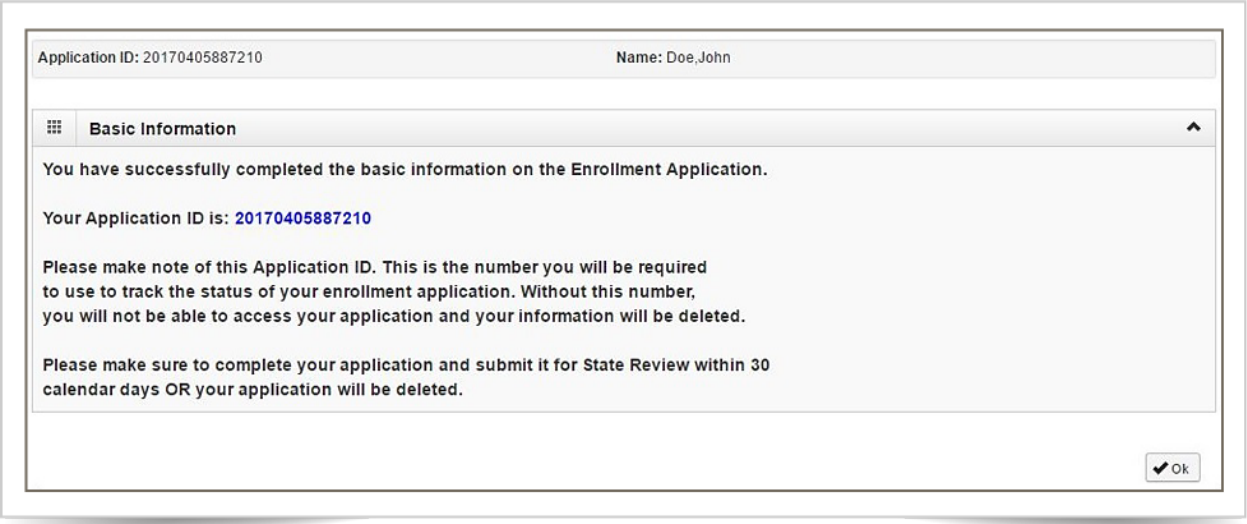


Figure 3.10.12-14. Application ID Generation. After basic information is successfully completed, the system generates an Application ID for tracking the application by providers.

Please note that responses to sections 3.10.13, Option A Provider Services, through 3.10.14, Option B Provider Services, have been submitted under separate files, respectively.

3.10.15 Reporting

This section addresses reporting requirements. The Contractor's solution shall provide an established library of standardized operational reports as well as the ability to create a wide array of configurable detail level and summary level reports, dashboards and queries. The Offeror must describe in their response their approach to meet the Reporting requirements defined in Attachment F, Requirements Matrix.

Team CNSI's evoBrix PMIS solution offers a robust and comprehensive framework to provide powerful reporting capabilities. The reporting framework is built on the evoBrix PMIS solution's scalable data architecture and business process management layer, which ensures data integrity and enables accuracy and consistency in reporting. Team CNSI implements a portfolio of tools to provide a comprehensive view into evoBrix platform, its underlying transactional data and reports.

Team CNSI's Reporting Solution will support all the business needs for successful Montana Provider Services Module (MT PSM) operations including:

The Team CNSI Advantage

Team CNSI brings a proven reporting solution designed on certified components, with robust reporting infrastructure and decision-making capabilities, which will assist the State in focusing on Provider Services.

- Web-based IBM Cognos business intelligence suite provides the flexibility to incorporate changes in a quick time frame
- Scalable data architecture for evoBrix online system
- "Out-of-the-box" reports that are proven and being leveraged in multiple states
- Ad hoc reporting capability designed to create customized reporting
- Identity management and security: end users will be able to conduct single sign on (SSO) to seamlessly navigate from evoBrix to IBM Cognos BI

MTPSM-3-070

- System operations reporting through Online Transaction Processing (OLTP) Operational Reporting and HealthBeat *(Refer to Section 3.10.8 Performance Standards for more details on HealthBeat)*
- Business operations and Service Level Agreement (SLA) under Operational Reporting (using HealthBeat)
- Reports required by State and Federal regulations
- Performance standard and throughput reporting through Operational statistics reporting and HealthBeat dashboards
- Capability to report transactional data directly from the System of Record to analyze real-time operational conditions or research
- Ad hoc reporting designed to create customized reporting that contain information specific to one or multiple subsystems per business requirements

Team CNSI proposes to implement industry-leading, highly powerful Business Intelligence (BI) tool IBM Cognos BI for the new MT PSM that will offer flexibility while ensuring ease of use. IBM Cognos BI tools also provide a suite of easy-to-use drag and drop interfaces for users, enabling them to create personal ad hoc reports, without the knowledge of any programming language. A variety of reports can be supported, including but not limited to canned/scheduled reports, on-demand reports, and ad hoc reports. The IBM Cognos BI suite provides users with much more independence by allowing them to import data using tailor-made reports, fulfilling their requirements. Team CNSI will leverage the scalable data architecture and report templates that are already built and available within evoBrix to configure DPHHS specific requirements.

In the sections below, we will discuss in detail how Team CNSI's reporting solution enables DPHHS to:

- Create, modify, save and manage reports
- Utilize pre-built operational, management and non-management reports necessary for proper operations maintenance and system performance
- Enforce security features with respect to reports access and privileges
- Leverage granular data to create custom detail or summary reports from ad hoc models in OLTP

evoBrix Reporting and Business Intelligence Infrastructure and Tools

IBM Cognos BI has an industry-leading suite of tools for business intelligence. IBM Cognos BI Report Studio and Query Studio tools provide very powerful capabilities to business users for creating sophisticated canned or ad hoc reports to manage daily operations. The tools are implemented in a web-based portal for easy access, making it a zero-footprint platform. IBM Cognos BI also provides an advanced framework, so that security can be implemented via groups and roles. By integrating the State's single sign-on (SSO) integration platform for federated identity management with evoBrix and Team CNSI's reporting solution, it offers a unique secure SSO experience without replicating user credentials across multiple directory stores, which would increase risk of account compromise potentially leading to unauthorized access to highly sensitive PHI or PII data in the system.

IBM Cognos BI Content Store is a data/content repository, used to store report outputs, which are made available through IBM Cognos BI Connection Portal. A single repository eliminates concerns of documents residing in multiple locations and therefore supports collaborative work between State users. Figure 3.10.15-1 shows a high-level architecture of Team CNSI's Reporting solution for evoBrix PMIS.

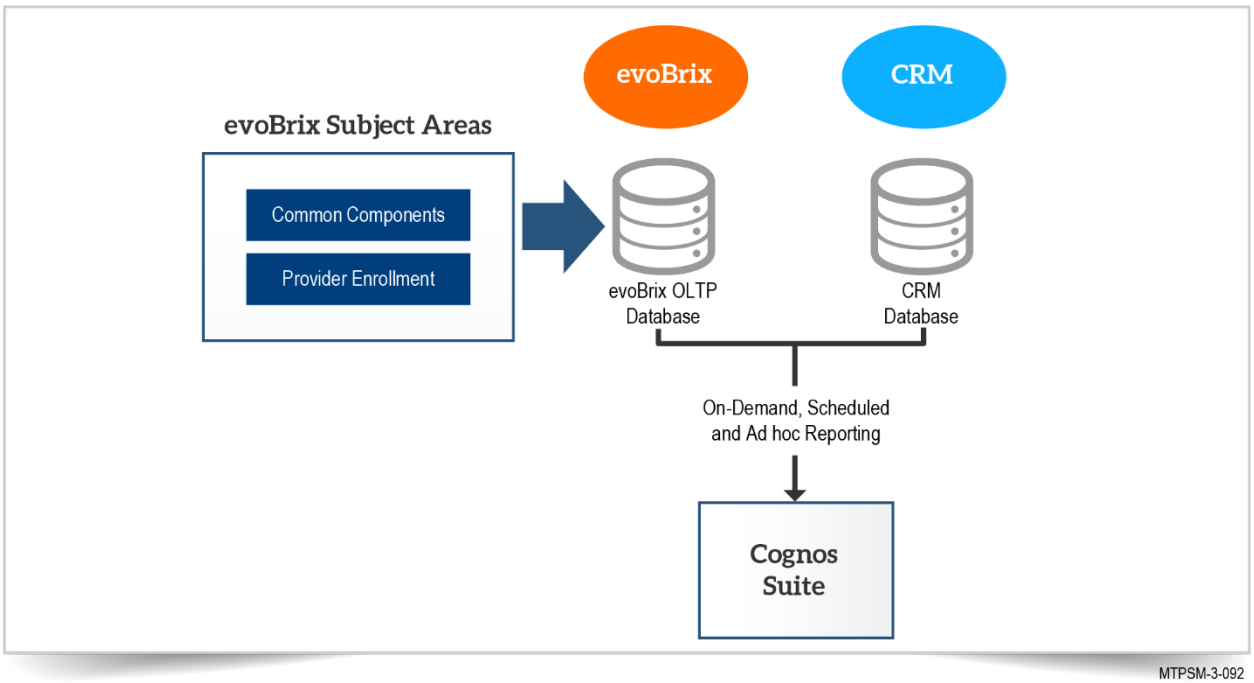


Figure 3.10.15-1. evoBrix Reporting Architecture. This architecture diagram shows data flow from different systems into IBM Cognos BI.

Team CNSI's reporting solution, which uses the IBM Cognos BI suite, offers a variety of tools that can cater and scale to varying business requirements. Some of the critical tools that are part of the BI suite are:

- IBM Cognos BI Event Management, which uses event triggers for generation of a certain analysis or report.
- IBM Cognos BI My Data Sets feature, which allows users to upload data from Excel or CSV to integrate their personal data into their reports.
- IBM Cognos BI Report Studio and Query Studio tools, which is most commonly leveraged in evoBrix OLTP. Both tools provide powerful professional reporting capabilities. IBM Cognos BI Report Studio is a web browser based Integrated Development Environment (IDE), used to configure pre-built reports. It exposes an extensive feature set that provides complex reporting capabilities, including multi-media options to be used in the reports, such as graphs, tables, maps etc. Both studio tools provide great flexibility in calculating and formatting results that produce better-looking reports and polished layouts. Figure 3.10.15-2 and Figure 3.10.15-3 show report design layouts for Query and Report Studio, respectively.

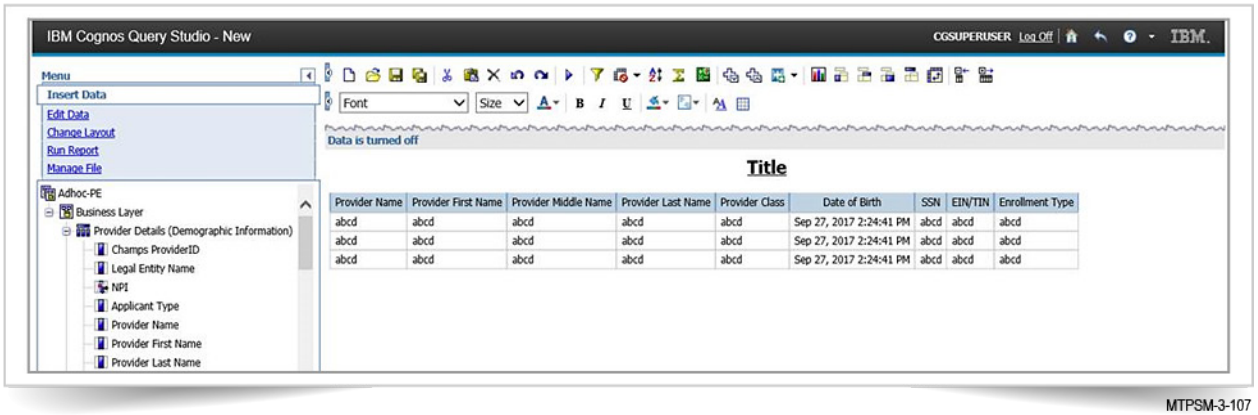


Figure 3.10.15-2. Query Studio Report Design Layout. A sample layout showing how a report can be configured in IBM Cognos BI using Query Studio.

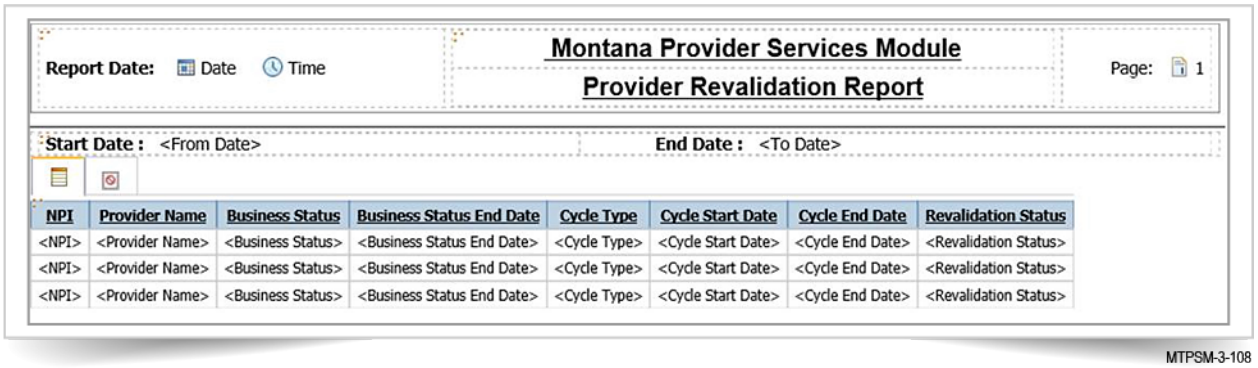


Figure 3.10.15-3. Report Studio Report Design Layout. A sample layout showing how a report can be configured in IBM Cognos BI using Report Studio.

Reports Enhancement and Operational Releases

Team CNSI's reporting solution enhancements are closely tied to and follow the evoBrix operational release processes. All components tied to reports (pre-built reports and ad hoc models) and report functionality is version maintained and could be reverted in conjunction with the corresponding operational release rollback. This ensures that once a report is defined and operational, the integrity of that report is maintained through software changes, including, but not limited to, upgrades, patches, fixes, defect corrections, and enhancements. Please refer to Section 3.10.4, Operations, Maintenance, and Configuration, for more details on Operational Release processes.

Reports Security and Privacy

In IBM Cognos BI suite, security can be enforced at multiple levels: at login, at the report level (only authorized users can see specific reports), at the report element level (certain elements can be hidden from certain users by applying user-based filters), and at the row level (filters can be set so that users can only see a subset of the data, such as only their own enrollees). IBM Cognos BI access is secured by setting permissions and enabling user authentication. Each entry in IBM Cognos BI Connection is secured to define who can read, edit, and run the entry. evoBrix controls access to sensitive information through a highly configurable Role-based Access Control (RBAC) setup. This ensures the ability to control, read, and access rightful information.

Reports Diagnostic Framework

IBM Cognos BI Reports Diagnostic Framework (RDF) provides an excellent technique to proactively identify report failures, perform analysis using report failure patterns, execution time trends and usage statistics. Some of the highlights of this state-of-the-art framework are:

- Failure Statistics: Providing an insight about the report failures and its pattern
- Performance Statistics: Diving in the report execution times which can help and locate the expensive reports before client identifies them
- Usage Statistics: Giving an idea about the maximum used/executed reports by users
- PHI/PII access Statistics: Helping to identify users accessing the PHII/PII information

Figure 3.10.15-4 shows different statistics visuals that are derived from underlying granular information at the report level. The view provides the flexibility to view the trends in both summarized and granular fashion.



Figure 3.10.15-4. RDF Performance Metrics Screen. Performance Metrics showing statistical information regarding the solution's performance and throughput.

Reports Access and Navigation

In Team CNSI's reporting solution, users who should have access to reports are set up with profiles that allow them access to the IBM Cognos BI Connection Portal. The portal is accessed from the "External Links" tab within evoBrix and displays several attributes of reports such as Report Name, Run Frequency, Output Format, and Restricted Flag (based on user security and access privileges). IBM Cognos BI Connection Portal also allows users to search and filter on any of the displayed attributes. For example, a user can filter on reports with the word "provider" in the Report Name. The content (Reports) of the portal page is based on the Security Matrix User Profiles, and will vary with user profiles. Figure 3.10.15-5 shows the home page of the IBM Cognos BI Connection Portal.



Figure 3.10.15-5. IBM Cognos Connection Portal. Screenshot showing IBM Cognos BI Connection Portal from which reports can be accessed and shared among users.

Report Types and Delivery

Scheduled Reports

Scheduled reports are automatically generated based on a fixed schedule, finalized during requirements gathering. Users are notified via auto-generated emails once the report execution completes on a given schedule. Team CNSI's reporting solution contains several management and operational reports that are scheduled to run from the transaction OLTP, on a daily/weekly basis. These reports will also be made available through IBM Cognos BI Connection Portal for viewing and retrieval. The report outputs are archived and integrated into IBM Cognos BI Content Store and could be retained according to pre-defined retention policies. Figure 3.10.15-6 shows various scheduled report output versions in IBM Cognos BI Connection Portal.

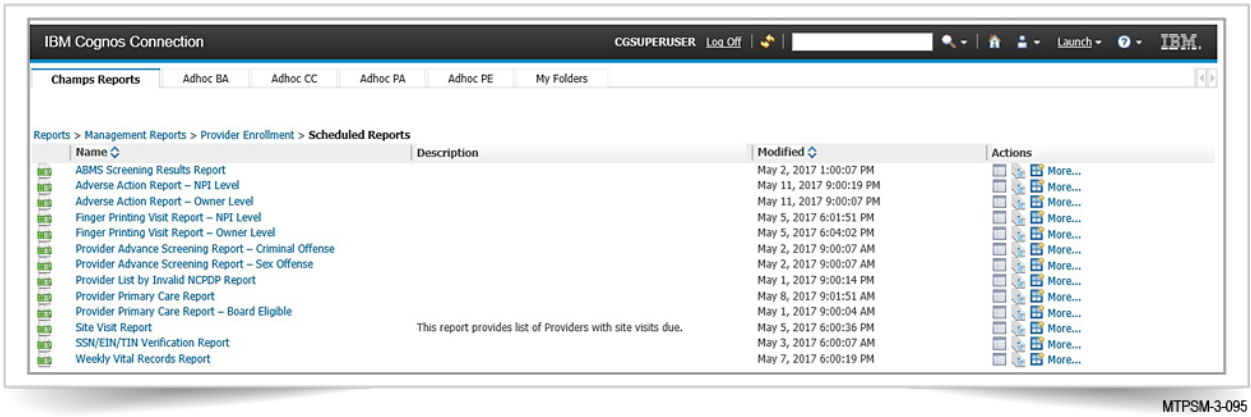


Figure 3.10.15-6. IBM Cognos Connection Portal. Screenshot showing different report outputs for scheduled reports in IBM Cognos Connection Portal.

On-Demand Reports

On-Demand Reports are generated based on user action. These reports are generally parameterized and will require some user input before they can be executed. The prompts may be based on dates, numbers or text. IBM Cognos BI validates user input values in the correct format. It will be up to the discretion of the user to save the reports locally, view, or discard them, as these outputs will not be available in the IBM Cognos BI Content Store repository. IBM Cognos BI Connection Portal allows users to access on-demand reports.

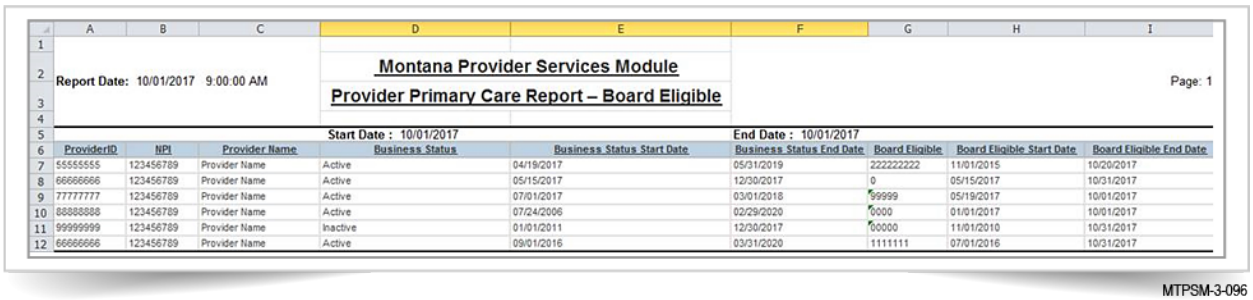
Ad Hoc Reports

In the context of MT PSM, ad hoc reporting is a frequent occurrence. Hence, it is important to have a tool that provides an easy interface to create and execute reports. IBM Cognos BI suite of tools offers Query

Studio for analytical users to create, modify, view, and change the appearance and the distribution of ad hoc reports.

Team CNSI's ad hoc reporting for evoBrix PMIS is facilitated by OLTP, using IBM Cognos BI Query Studio. This is in turn integrated with the evoBrix application. IBM Cognos BI Packages, a set of metadata objects, are designed to contain information relating specifically to one or multiple subsystems per business requirements. Packages contain data elements, organized in a user-friendly way which makes it easy to navigate and identify data elements. The complexity of the tables and relationships is hidden from the user for an enhanced self-service user experience.

Users can simply drag and drop the business elements required into their workspace to create their own customized ad hoc report. Due to the granular nature of data storage in OLTP, reports could be created at different aggregation levels (detail or summary) tied to various dimensions. Though this is applicable to pre-built reports as well, ad hoc reporting provides the user with the flexibility to create their own customized reports. They can also execute, generate the query or report, and can save in various formats including HTML, Excel, CSV, and PDF. Figure 3.10.15-7 shows a sample ad hoc report in Excel format.



Report Date: 10/01/2017 9:00:00 AM

Montana Provider Services Module

Provider Primary Care Report – Board Eligible

Page: 1

Start Date : 10/01/2017 End Date : 10/01/2017

ProviderID	NPI	Provider Name	Business Status	Business Status Start Date	Business Status End Date	Board Eligible	Board Eligible Start Date	Board Eligible End Date
55555555	123456789	Provider Name	Active	04/19/2017	05/31/2019	222222222	11/01/2015	10/20/2017
66666666	123456789	Provider Name	Active	05/15/2017	12/30/2017	0	05/15/2017	10/31/2017
77777777	123456789	Provider Name	Active	07/01/2017	03/01/2018	99999	05/19/2017	10/01/2017
88888888	123456789	Provider Name	Active	07/24/2006	02/29/2020	0000	01/01/2017	10/01/2017
99999999	123456789	Provider Name	Inactive	01/01/2011	12/30/2017	00000	11/01/2010	10/31/2017
66666666	123456789	Provider Name	Active	09/01/2016	03/31/2020	1111111	07/01/2016	10/31/2017

MTPSM-3-096

Figure 3.10.15-7. Excel Format Output. Screenshot showing a sample ad hoc report in Excel format.

**Note: Report shown with de-identified data.*

Operational Data Reporting

Operational Reporting from OLTP transactional system is mainly categorized into Management and Non-Management Reports. Under each of these categories, they are further classified by different subjects/ business areas, as is shown in Figure 3.10.15-8. Clicking a subject area allows the user to look at available reports within that subject area. Clicking on a report opens a prompt page associated with that report. The section "List of included System Reports" describes all operational reporting under Management and Non-Management that is prebuilt into Team CNSI's reporting solution for evoBrix PMIS.

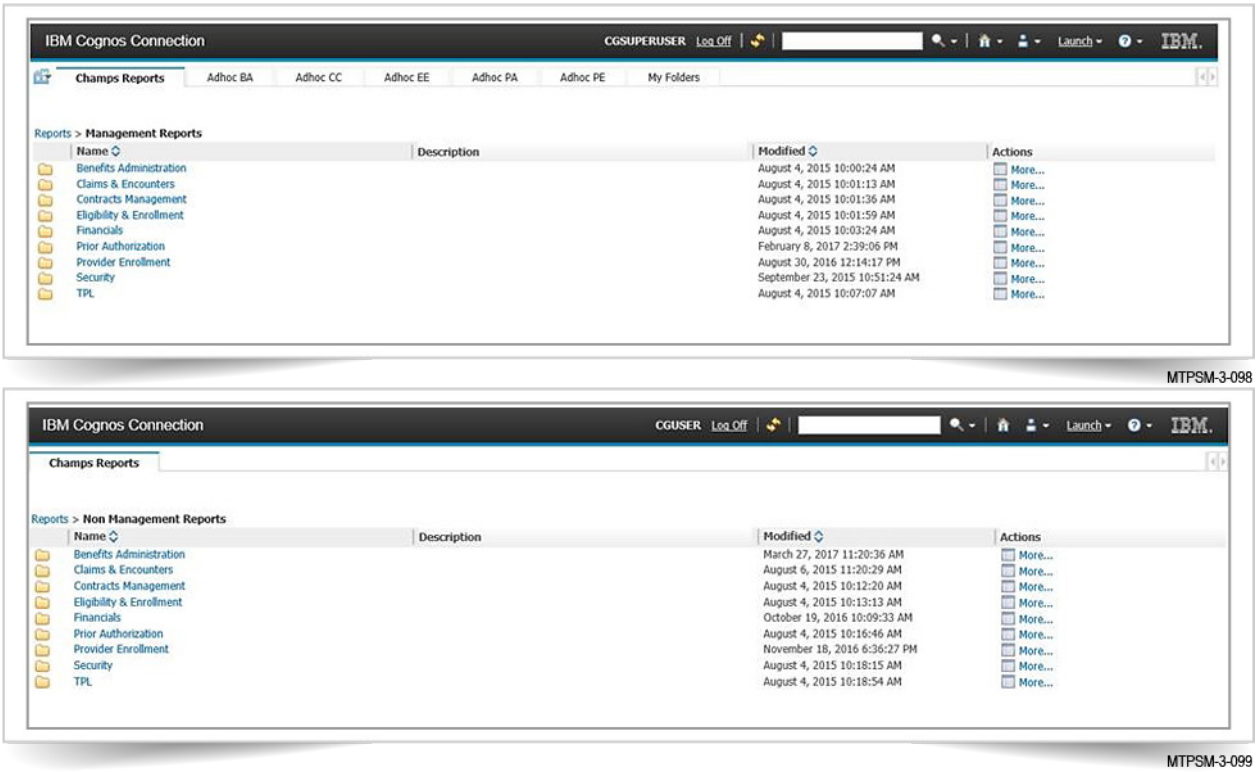


Figure 3.10.15-8. Reports Classification. Screenshots from IBM Cognos Connection Portal showing the report hierarchy for Management and Non-Management reports.

IBM Cognos BI Viewer allows the user to change formats, so that reports can be viewed in HTML, Excel, CSV, or PDF. Figure 3.10.15-9 shows a sample report in IBM Cognos BI Viewer. The user can change output formats by click of a button.

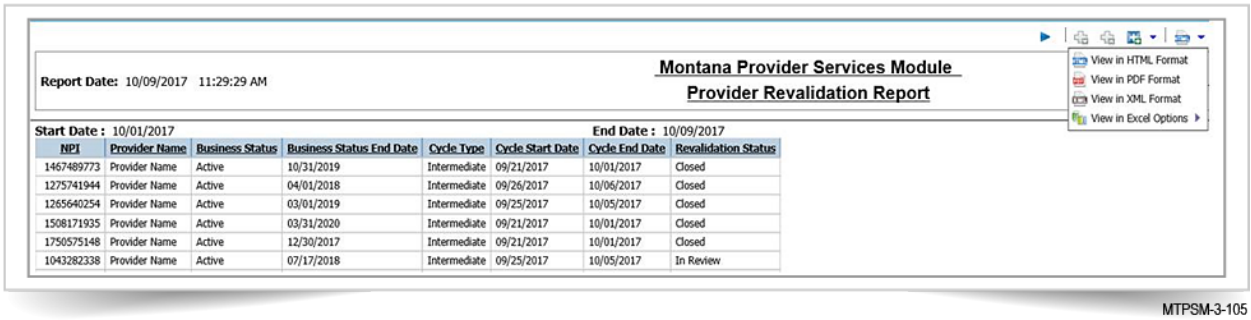


Figure 3.10.15-9. IBM Cognos BI Viewer. Screenshot showing a sample report output in IBM Cognos BI Viewer.

**Note: Report shown with de-identified data*

Features and Benefits to State of Montana

Figure 3.10.15-10 lists the features of Team CNSI's reporting solution that benefit PMIS business operations and efficient functioning of the system compared to similar reporting solutions.

Features of Team CNSI's Reporting Solution for evoBrix PMIS	Benefits
Proven OLTP data model with granular level of data	Our solution provides granularity and details that are not available in typical off-the-shelf solutions for ad hoc reporting and analysis purposes.
IBM Cognos BI Business Intelligence suite of tools provide powerful reporting capability	Reports are delivered to the end user over the web and can be made available directly for authorized DPHHS users. The end user can access all the reports themselves and can print/save them as needed.
Ad hoc Reporting Capabilities	Using ad hoc reporting capabilities from OLTP, users will be able to access and aggregate data with different dimensions from underlying detail data to help them during reconciliation and decision making.
Prebuilt Reports/Templates	Team CNSI's reporting solution comes with several pre-built operational, decision making reports and templates that can be leveraged starting day one of implementation.
Single Sign On	evoBrix has the ability to leverage single sign-on from the application into IBM Cognos BI environment, reducing the risk of account compromise and unauthorized access to highly sensitive PHI or PII data in the system.
IBM Cognos BI Connection Portal	evoBrix integrated IBM Cognos BI Connection Portal offers the State a seamless navigation from functional evoBrix to reporting, a single point of access for all reports
IBM Cognos BI Content Store	Our solution supports collaboration and communication among all State users and across all divisions and functional areas through Web-based technologies.

Figure 3.10.15-10. Benefits to MT DPHHS. List of evoBrix reporting solution features that sets it apart from similar platforms.

List of Included System Reports for evoBrix PMIS

Figure 3.10.15-11 lists all the pre-built reports that come with Team CNSI's reporting solution for evoBrix PMIS, that are functional from day one of implementation.

Report Name	Report Description
835 Authorizations By Provider Report	This report provides list of all Billing Agent Association and 835 Authorization report.
ABMS Screening Results Report	This report provides a list of those providers whose board certificate has changed from "Yes" to "No" during the batch monthly screening process.
Adverse Action Report – NPI Level	This report will be generated with list of adverse actions ("SUSPENDED" and "SANCTIONED SOURCE") for providers on a particular day.
Adverse Action Report – Owner Level	This report will be generated with list of adverse actions ("SUSPENDED" and "SANCTIONED SOURCE") for Owners on a particular day.
Enrollment Application Referrals and Activity Returns by Provider Type	This report is used to evaluate Enrollment Application Referrals and Activity Returns at the Provider type level.
Enrollment Application Referrals/Activity Returns by User	This report is used to evaluate Enrollment Application Referrals and Activity Returns at the user level.
ERA Enrollment Report	This report is used to print the ERA Agreement that a provider agreed upon when enrolling into evoBrix or submitting a modification request.

Report Name	Report Description
Finger Printing Visit Report – NPI Level	This report provides a list of providers with fingerprinting due date based on NPI. The on-demand report will pull the reports based on input dates.
Finger Printing Visit Report – Owner Level	This report provides a list of providers with fingerprinting due date based on ownership. The on-demand report will pull the reports based on input dates.
Home Help Verification Submission Status Report	This report will be used to identify the providers that have not submitted a verification form for the selected service month(s).
Home Help Verification Submission Status Summary Report	This report will provide the total Verification Submissions that have been submitted, saved, and not submitted for the selected month.
Print Permission Matrix Report	This report is used to print the Permission Matrix.
Print Provider Information Report	This report is used to print the Provider information for active providers. This report will also include all active pharmacy providers.
Print Terms and Conditions Report	This report is used to print the Terms and Conditions that a provider agreed upon enrolling into evoBrix.
Provider Advance Screening Report – Criminal Offense	This report provides a list of providers who have criminal offenses.
Provider Advance Screening Report – Sex Offense	This report provides a list of providers who have sex offenses.
Provider List by Invalid NCPDP Report	This report lists Pharmacy providers with an Invalid NCPDP ID.
Provider List by Invalid NPI Report	This report lists providers by Invalid NPI.
Provider Primary Care Report	This report provides a list of all providers who have the primary care specialties/subspecialties selected and who have the Board Certified, Board Eligible and or Eligible Claims Found set.
Provider Primary Care Report – Board Eligible	This report provides a list of all providers that have “Board Eligible” under the license/certification step and their Board Eligible end-date will end during the current month.
Provider Processing Statistics Modification Requests by Provider Type	This report is used to evaluate Modification Request statistics at the Provider Type level.
Provider Processing Statistics Modification Requests by User	This report is used to evaluate modification request statistics at the State Approver (user) level.
Provider Processing Statistics New Applications by Provider Type	This report is used to evaluate New Application statistics at the provider type level.
Provider Processing Statistics New Applications by User	This report is used to evaluate new application statistics at the user level.
Provider Revalidation Report	This report provides a list of providers with Cycle End-Date matching the date range submitted for the report.
Sanctioned-License Expired Pharmacy Providers	This report provides a list of pharmacy providers that have a disciplinary sanction and/or whose licenses have expired.

©2017 CNSI

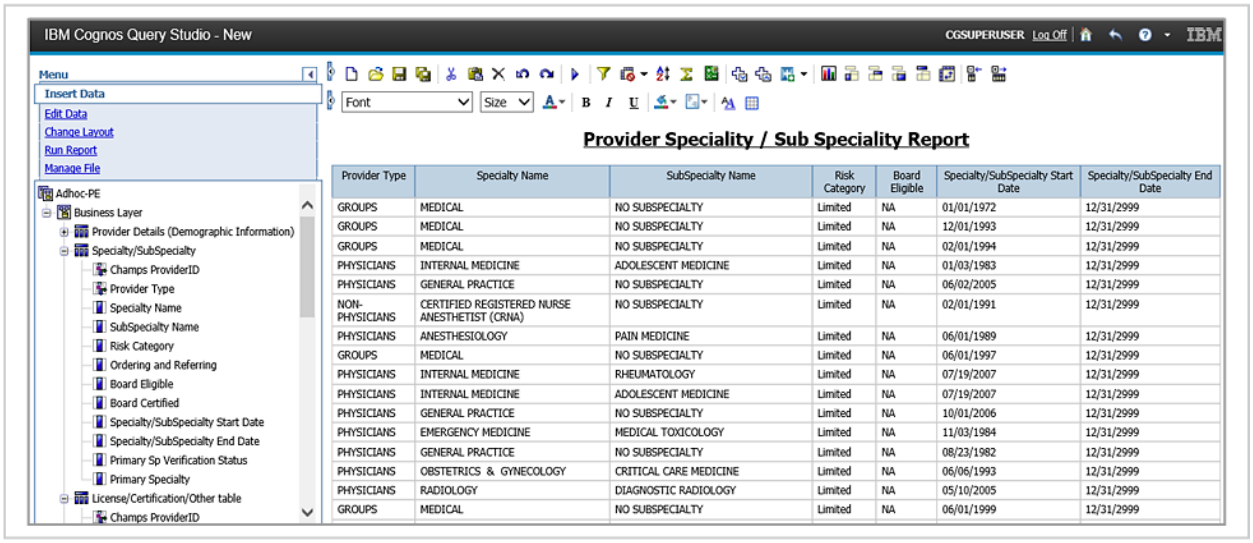
Report Name	Report Description
Site Visit Report	This report provides a list of providers with site visits due.
SSN/EIN/TIN Verification Report	This report provides a list of providers whose "SSN Verified," "EIN/TIN Verified," or "Name Verified" has been set to no.
Vital Records Report	List of providers that were updated to "deceased" within the date range selected.

Figure 3.10.15-11. Standardized Operational Reports for evoBrix PMIS. List of configurable detail and summary level reports offered by the evoBrix reporting solution.

REP01

The Contractor's solution shall include a query tool that allows users to easily query data necessary to support state healthcare programs business needs.

Team CNSI's reporting solution enables users to design customized reports according to individual requirements using ad hoc reporting. IBM Cognos BI Query Studio leverages ad hoc models for analytical users to create, modify, and view the appearance and the distribution of ad hoc reports. IBM Cognos BI Packages, a set of metadata objects, are designed to contain information relating specifically to one or multiple subsystems per business requirements. Packages contain data elements, organized in a user-friendly way, which makes it easy to navigate and identify data elements. The complexity of the tables and relationships is hidden from the user for an enhanced self-service user experience. Users can simply drag and drop the business elements into their workspace to create customized ad hoc reports. The reports could either be at a summary or detail level due to granular level of data storage in evoBrix OLTP. Figure 3.10.15-12 shows a sample ad hoc report designed in IBM Cognos BI Query Studio based on ad hoc provider model.



Provider Type	Specialty Name	SubSpecialty Name	Risk Category	Board Eligible	Specialty/SubSpecialty Start Date	Specialty/SubSpecialty End Date
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	01/01/1972	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	12/01/1993	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	02/01/1994	12/31/2999
PHYSICIANS	INTERNAL MEDICINE	ADOLESCENT MEDICINE	Limited	NA	01/03/1983	12/31/2999
PHYSICIANS	GENERAL PRACTICE	NO SUBSPECIALTY	Limited	NA	06/02/2005	12/31/2999
NON-PHYSICIANS	CERTIFIED REGISTERED NURSE ANESTHETIST (CRNA)	NO SUBSPECIALTY	Limited	NA	02/01/1991	12/31/2999
PHYSICIANS	ANESTHESIOLOGY	PAIN MEDICINE	Limited	NA	06/01/1989	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	06/01/1997	12/31/2999
PHYSICIANS	INTERNAL MEDICINE	RHEUMATOLOGY	Limited	NA	07/19/2007	12/31/2999
PHYSICIANS	INTERNAL MEDICINE	ADOLESCENT MEDICINE	Limited	NA	07/19/2007	12/31/2999
PHYSICIANS	GENERAL PRACTICE	NO SUBSPECIALTY	Limited	NA	10/01/2006	12/31/2999
PHYSICIANS	EMERGENCY MEDICINE	MEDICAL TOXICOLOGY	Limited	NA	11/03/1984	12/31/2999
PHYSICIANS	GENERAL PRACTICE	NO SUBSPECIALTY	Limited	NA	08/23/1982	12/31/2999
PHYSICIANS	OBSTETRICS & GYNECOLOGY	CRITICAL CARE MEDICINE	Limited	NA	06/06/1993	12/31/2999
PHYSICIANS	RADIOLOGY	DIAGNOSTIC RADIOLOGY	Limited	NA	05/10/2005	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	06/01/1999	12/31/2999

MTPSM-3-361

Figure 3.10.15-12. A Sample Ad-hoc Report. A sample ad hoc report designed in IBM Cognos BI Query Studio based on ad hoc provider model.

REP07

The Contractor's reporting tool shall provide the ability to design and execute a queries using one or more wild cards (e.g., %, *,?) and operators (e.g. =, , >, >=, <, <=, IN, BETWEEN, LIKE, IS NULL or IS NOT NULL) to provide data when searching or reporting.

Team CNSI's reporting solution provides the option for parameterized reporting in On Demand reports, that enables users to access specific information that they are interested in. These reports expect prompt users to enter query values that could be numbers, date, or text. The parameters supported include all operators such as =, >, >=, <, <=, IN, BETWEEN, LIKE, IS NULL or IS NOT NULL and "% " for wild card search in case users wish to search for a pattern based results. Figure 3.10.15-13 shows a sample parameterized report based on wild card search and operators, in IBM Cognos BI Viewer.

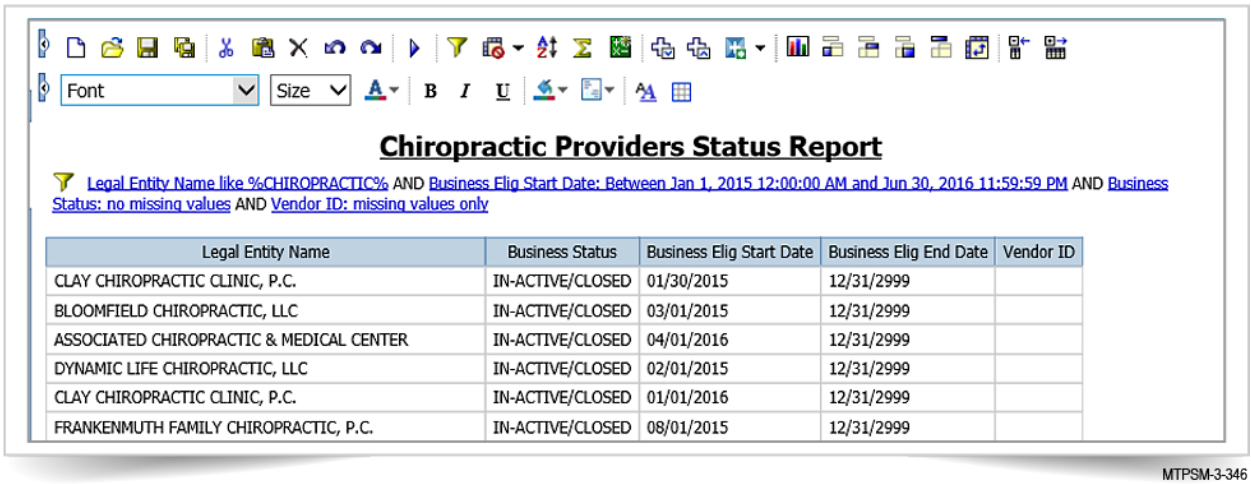


Figure 3.10.15-13. A Sample Parameterized Report. A sample of a pre-built IBM Cognos BI parameterized report that shows wildcard search pattern.

REP103

The Contractor's solution shall have the capability to display data in a variety of formats (e.g., standard reports, graphs, charts, maps, dashboards) without the need to export data to another tool.

Team CNSI's reporting solution leverages an extensive feature set provided by IBM Cognos BI Query Studio (Ad-hoc Reporting) and Report Studio (pre-built On Demand and Scheduled Reporting) to address complex reporting requirements, including but not limited to multi-media options such as graphs, charts or dashboards, resulting in more visually appealing reports and layouts. Figure 3.10.15-14 and Figure 3.10.15-15 show various report styles available and a sample pre-built report in a graph format (designed in IBM Cognos BI Report Studio) respectively.

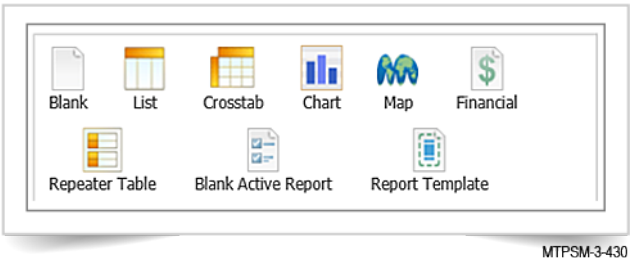


Figure 3.10.15-14. Report Styles Available in IBM Cognos BI. Various report styles available in IBM Cognos BI Query and Report Studio.

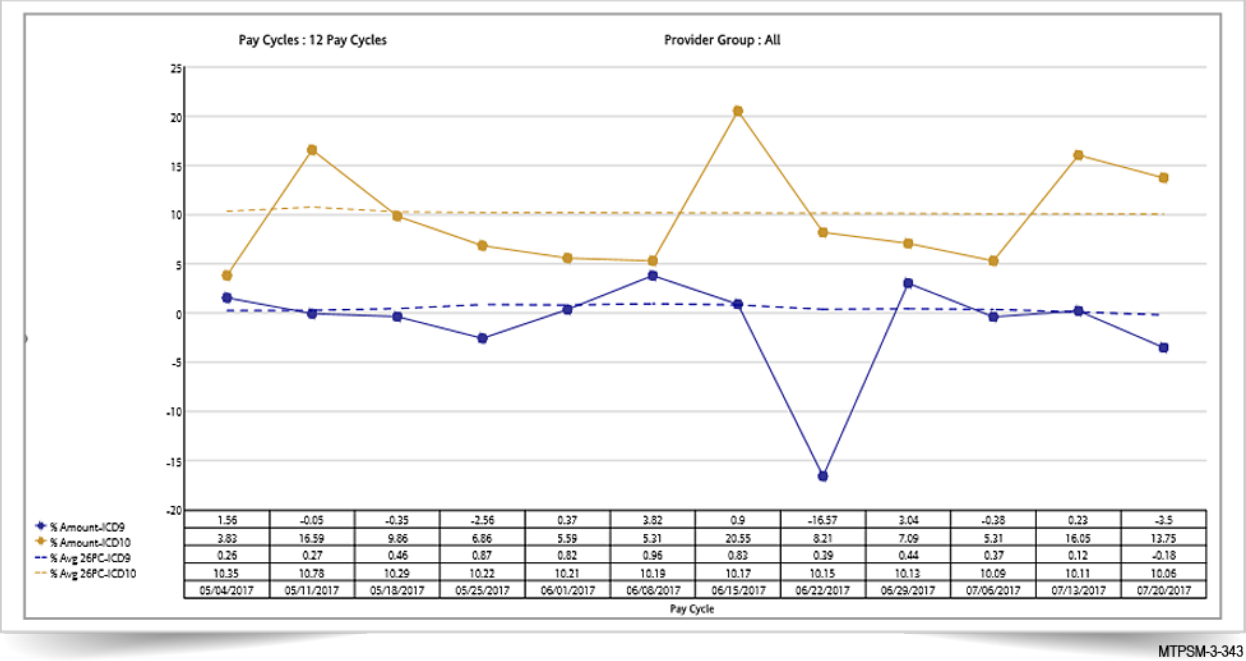


Figure 3.10.15-15. A Sample Graph-based Report. A sample of pre-built IBM Cognos BI Report Studio report that represents data in the form of a graph.

REP104

The Contractor's solution shall have the ability for authorized users to selectively retrieve, view, export, and print reports (or portions of reports).

Team CNSI's reporting solution facilitates authorized users to export their report outputs in various formats including HTML, Excel, CSV, and PDF, which could then be printed locally. Figure 3.10.15-16 shows how to view/export a report in IBM Cognos BI Viewer. The reports can be exported in a certain format according to user's preference. Predefined filters or designing report query parameters help selectively retrieve results into report output as well.

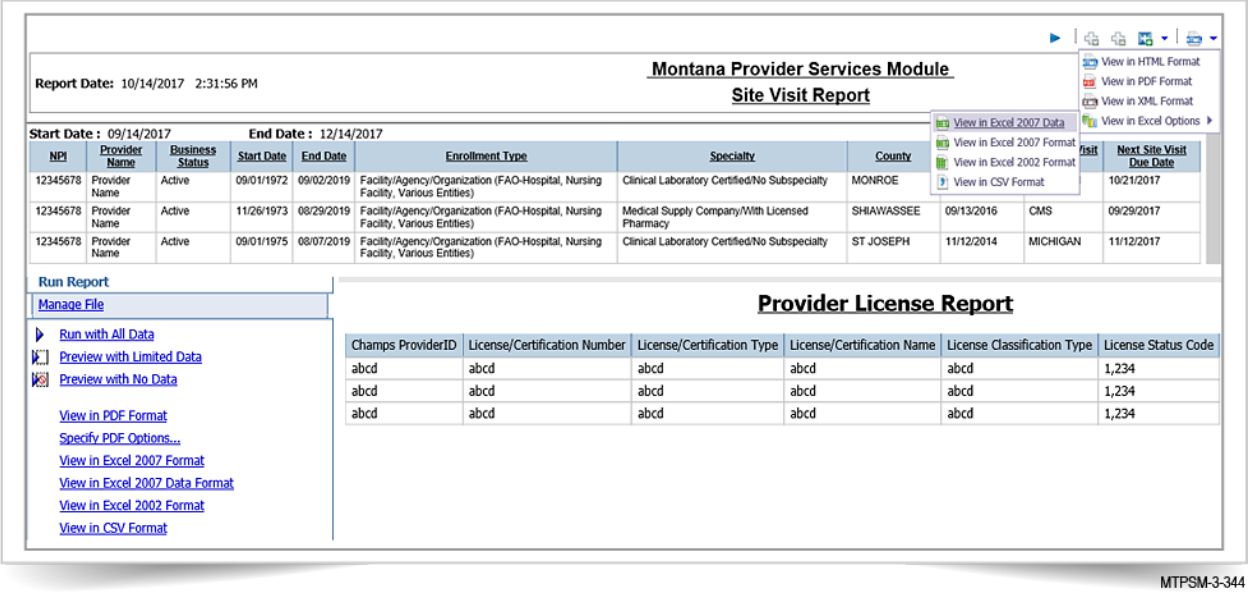


Figure 3.10.15-16. Report Export Formats. A sample of a pre-built IBM Cognos BI Report Studio report, that shows how to view or export a standard report in different formats.

REP107

The Contractor's solution shall have the capability to allow authorized users to view query parameters along with query results.

Team CNSI's reporting solution provides the option for parametrized reports in On Demand Reporting. The prompts may be dates, numbers or text. Depending on the design on the report, the query parameters may be viewed along with the report output. Figure 3.10.15-17 shows a sample parameterized report, showing the actual query parameter values provided.

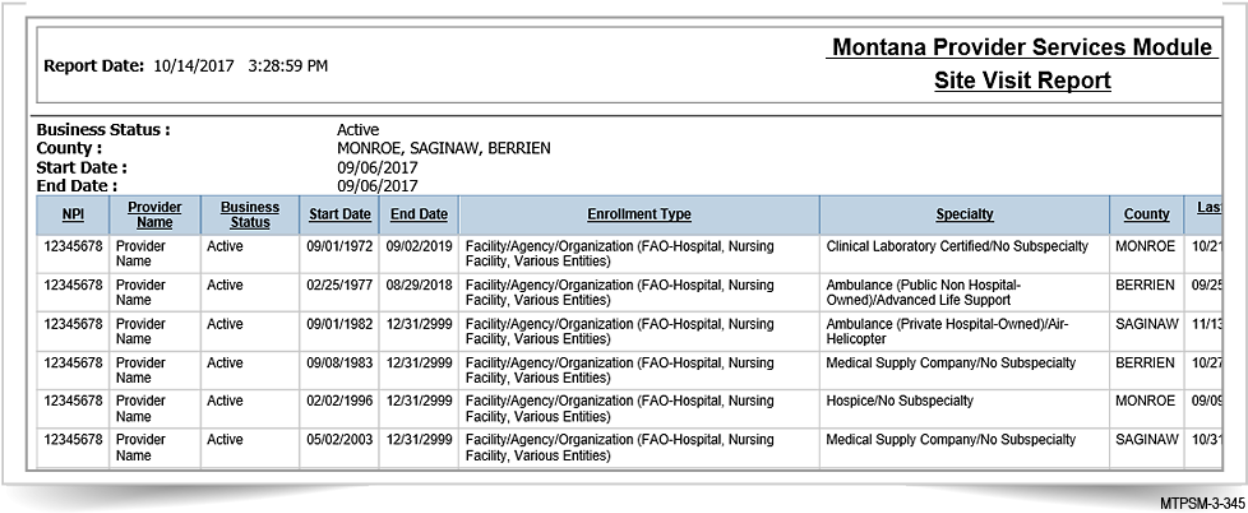


Figure 3.10.15-17. Parameterized Report Output. A sample of a pre-built IBM Cognos BI Report Studio report output in IBM Cognos BI Viewer. Note that the query parameters are displayed along with the output.

REP110

The Contractor shall update dashboards in real-time or on a schedule approved by the State.

Team CNSI's HealthBeat solution provides configurable, automated, and real-time visibility into business operations, SLA compliance, and system monitoring. HealthBeat enables the setup of a hierarchy of MITA business, system, and application objectives or goals that can be linked with metrics to events and services. This will allow Team CNSI and DPHHS using evoBrix to monitor the health of business and system processes not only in the short term but also over the long term to track historical trends. Figure 3.10.15-18 shows sample HealthBeat dashboards reporting provider status. Please refer to Section 3.10.8, Performance Standards, for more details on HealthBeat.

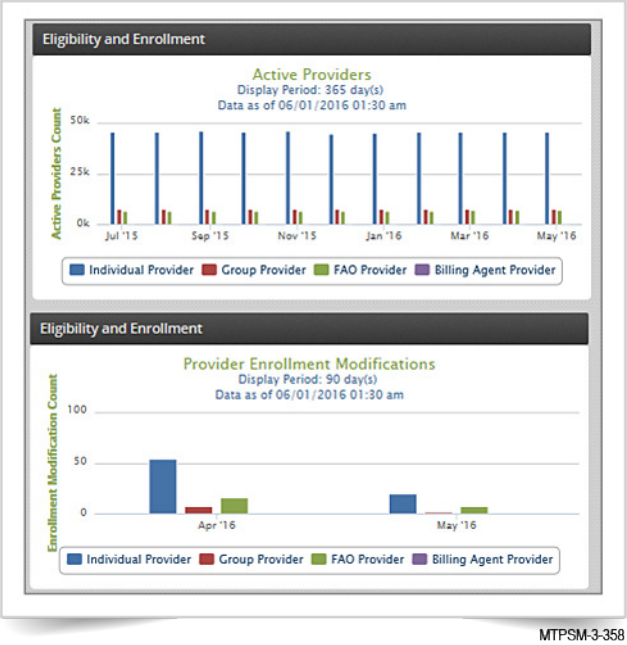
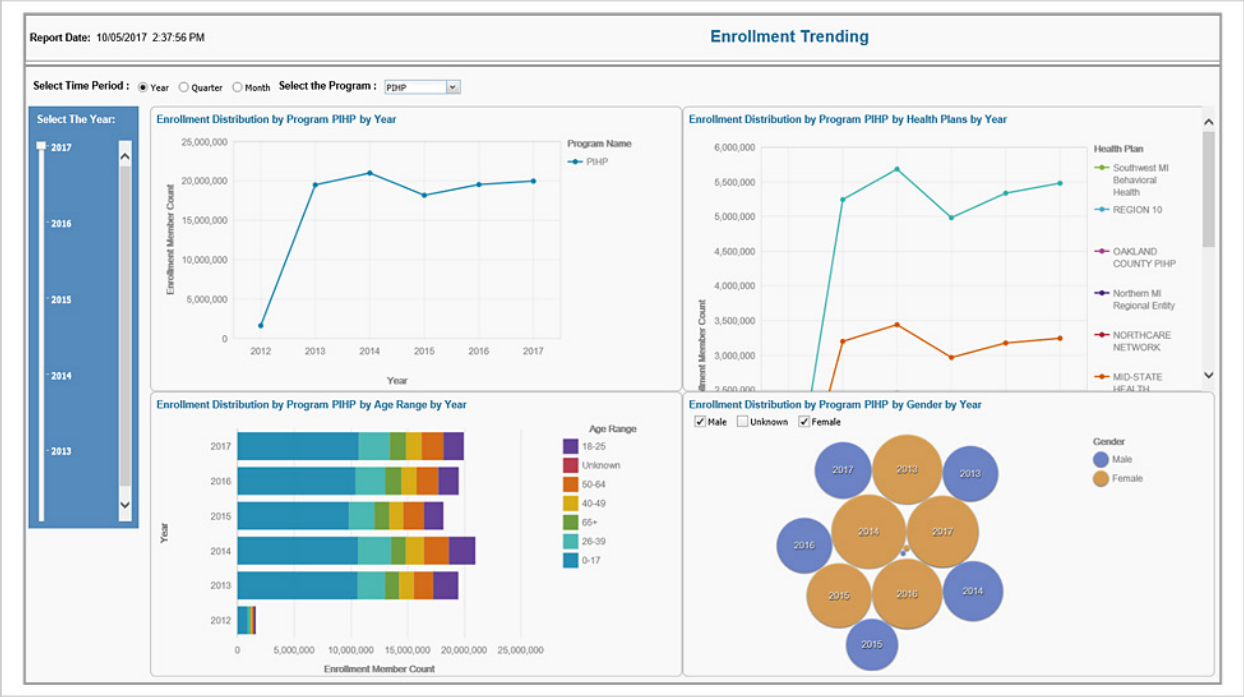


Figure 3.10.15-18. HealthBeat Dashboards. A sample of pre-built HealthBeat dashboards reflecting provider enrollment and active statuses on a real-time basis.

REP111

The Contractor's solution shall allow authorized users to design, save and share configurable dashboards and reports.

Team CNSI's reporting solution leverages IBM Cognos BI Workspace that allows authorized users to view, use, and modify dashboard objects which were created in IBM Cognos BI Real-time Monitoring. In IBM Cognos BI Workspace, users can combine dashboard objects that receive data from various data marts in evoBrix PMIS into a single workspace and have a 360-degree view of their business. Dashboard objects created in IBM Cognos BI Real-time Monitoring Dashboard are shared with IBM Cognos BI Workspace. Any changes to Real-time Monitoring are reflected on the Workspace immediately. Figure 3.10.15-19 shows a sample dashboard designed in IBM Cognos BI Workspace.



MTPSM-3-359

Figure 3.10.15-19. IBM Cognos BI Active Dashboard. A sample of pre-built IBM Cognos BI Active Dashboard.

REP112

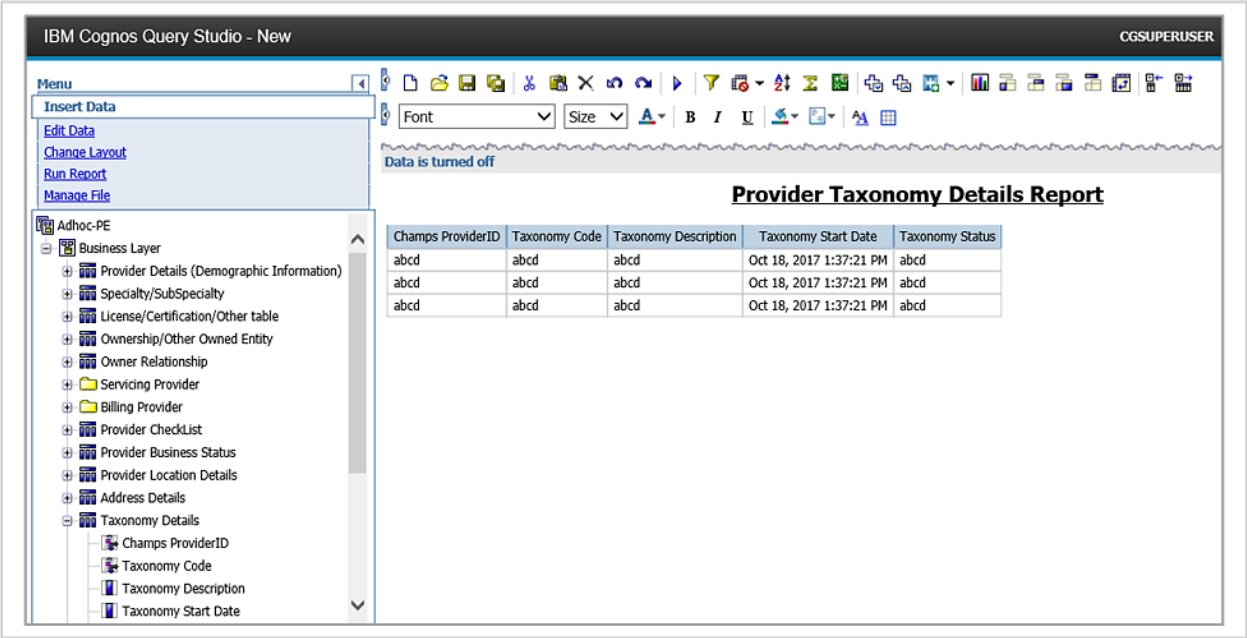
The Contractor's solution shall provide report, dashboard and query templates for authorized users to modify and reuse.

Team CNSI's reporting solution uses IBM Cognos BI Workspace Advanced that enables users to perform advanced data exploration and author simple reports. Any requirement to perform detailed analysis and report authoring will have users seamlessly graduate to Workspace Advanced, where they can perform more advanced data exploration such as adding additional measures, conditional formatting, and advanced calculations. IBM Cognos BI Workspace Advanced can also be launched directly from the IBM Cognos BI Connection Portal. With Cognos Workspace Advanced, users can create reports with relational or dimensional data sources, to show in lists, crosstabs, or charts.

IBM Cognos BI Query Studio is the reporting tool that will facilitate users to create simple queries and reports in IBM Cognos BI Business Intelligence. In Query Studio, users can:

- Connect to a data source to view data elements in a tree hierarchy in ad hoc models. Users may expand the query subjects to see query item details.
- Design/create customized reports which can be saved, modified, copied or reused.
- Improve the layout or appearance of your report. For example, user can create a chart, add a title, specify text and border styles, or reorder columns for easy comparison.
- Use filters, summaries, and calculations to compare and analyze data.
- Drill up and drill down to view detail or summary information.

Both Cognos Workspace Advanced and Query Studio could be used to create query templates which could be modified by users to design complex reports according to business requirements. Figure 3.10.15-20 shows a sample ad hoc query template designed in IBM Cognos BI Query Studio.



MTPSM-3-360

Figure 3.10.15-20. Ad hoc Query Template. A sample ad hoc query template designed in IBM Cognos BI Query Studio displaying the query subjects based on the ad hoc provider model within evoBrix PMIS.

REP116

The Contractor's solution shall provide an established library of standardized operational reports as well as the ability to create a wide array of configurable detail level and summary level reports, dashboards and queries.

Team CNSI's evoBrix PMIS solution comes with a standard repository of operational reports out-of-the-box, which quickly facilitates the provider business operations team members' ability to address day-to-day operational needs. These reports are configurable both at the detail and summary Team CNSI's HealthBeat solution also provides configurable, automated, and real-time visibility into business operations, SLA compliance, and system monitoring using real-time dashboards. Figure 3.10.15-21 shows a list of system included reports available from day one of implementation.

Report Name	Report Description
835 Authorizations By Provider Report	This report provides list of all Billing Agent Association and 835 Authorization report.
ABMS Screening Results Report	This report provides a list of those providers whose board certificate has changed from "Yes" to "No" during the batch monthly screening process.
Adverse Action Report – NPI Level	This report will be generated with list of adverse actions ("SUSPENDED" and "SANCTIONED SOURCE") for providers on a particular day.

Report Name	Report Description
Adverse Action Report – Owner Level	This report will be generated with list of adverse actions ("SUSPENDED" and "SANCTIONED SOURCE") for Owners on a particular day.
Enrollment Application Referrals and Activity Returns by Provider Type	This report is used to evaluate Enrollment Application Referrals and Activity Returns at the Provider type level.
Enrollment Application Referrals/Activity Returns by User	This report is used to evaluate Enrollment Application Referrals and Activity Returns at the user level.
ERA Enrollment Report	This report is used to print the ERA Agreement that a provider agreed upon when enrolling into evoBrix or submitting a modification request.
Finger Printing Visit Report – NPI Level	This report provides a list of providers with fingerprinting due date based on NPI. The on-demand report will pull the reports based on input dates.
Finger Printing Visit Report – Owner Level	This report provides a list of providers with fingerprinting due date based on ownership. The on-demand report will pull the reports based on input dates.
Home Help Verification Submission Status Report	This report will be used to identify the providers that have not submitted a verification form for the selected service month(s).
Home Help Verification Submission Status Summary Report	This report will provide the total Verification Submissions that have been submitted, saved, and not submitted for the selected month.
Print Permission Matrix Report	This report is used to print the Permission Matrix.
Print Provider Information Report	This report is used to print the provider information for active providers. This report will also include all active pharmacy providers.
Print Terms and Conditions Report	This report is used to print the Terms and Conditions that a provider agreed upon enrolling into evoBrix.
Provider Advance Screening Report – Criminal Offense	This report provides a list of providers who have criminal offenses.
Provider Advance Screening Report – Sex Offense	This report provides a list of providers who have sex offenses.
Provider List by Invalid NCPDP Report	This report lists Pharmacy providers with an Invalid NCPDP ID.
Provider List by Invalid NPI Report	This report lists providers by Invalid NPI.
Provider Primary Care Report	This report provides a list of all providers who have the primary care specialties/subspecialties selected and who have the Board Certified, Board Eligible and or Eligible Claims Found set.
Provider Primary Care Report – Board Eligible	This report provides a list of all providers that have "Board Eligible" under the license/certification step and their Board Eligible end-date will end during the current month.
Provider Processing Statistics Modification Requests by Provider Type	This report is used to evaluate Modification Request statistics at the Provider Type level.
Provider Processing Statistics Modification Requests by User	This report is used to evaluate modification request statistics at the State Approver (user) level.
Provider Processing Statistics New Applications by Provider Type	This report is used to evaluate New Application statistics at the provider type level.

©2017 CNSI | 3.10-652

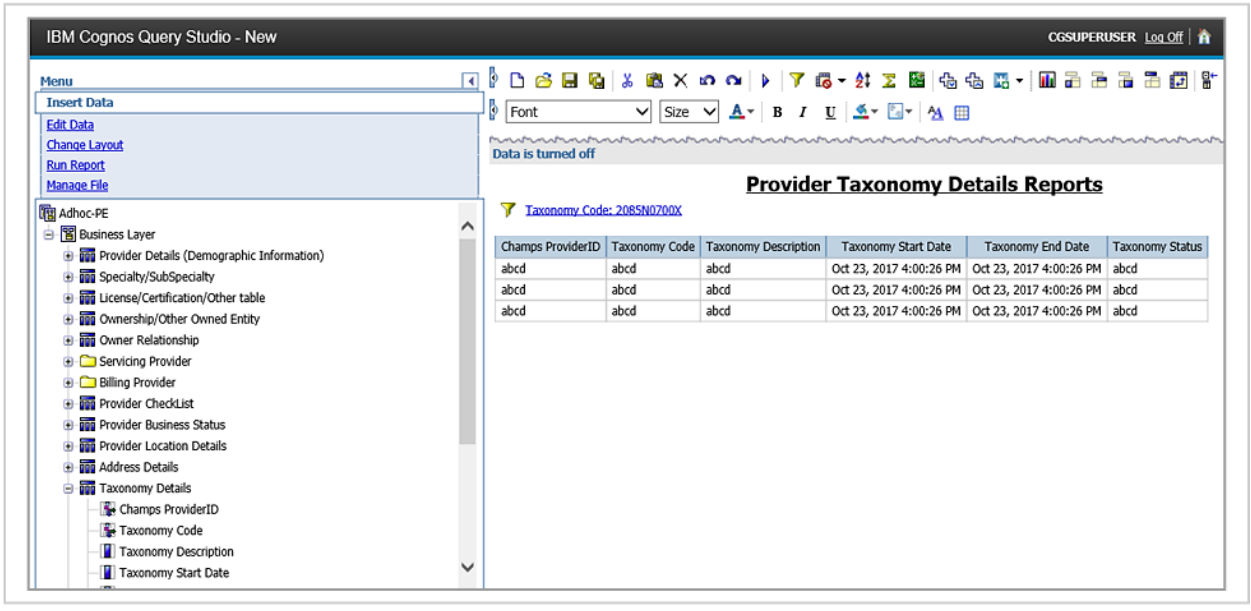
Report Name	Report Description
Provider Processing Statistics New Applications by User	This report is used to evaluate new application statistics at the user level.
Provider Revalidation Report	This report provides a list of providers with Cycle End-Date matching the date range submitted for the report.
Sanctioned-License Expired Pharmacy Providers	This report provides a list of pharmacy providers that have a disciplinary sanction and/or whose licenses have expired.
Site Visit Report	This report provides a list of providers with site visits due.
SSN/EIN/TIN Verification Report	This report provides a list of providers whose "SSN Verified," "EIN/TIN Verified," or "Name Verified" has been set to no.
Vital Records Report	List of providers that were updated to "deceased" within the date range selected.

Figure 3.10.15-21. Standardized Operational Reports for evoBrix PMIS. List of configurable detail and summary level reports offered by the evoBrix reporting solution.

REP118

The Contractor's solution shall have the capability to produce reports or display output data by National Provider Identifier (NPI), proprietary ID, or by a subset of the provider's practice or taxonomy.

As described earlier, about parameterized reports in REP07 and REP107, Team CNSI' reporting solution for evoBrix PMIS provides user with the ability to generate reports based on various query parameters. These parameters may include but not limited to NPI, provider ID, and taxonomy. Figure 3.10.15-22 shows a sample IBM Cognos BI Query Studio Report designed to display NPI, Provider ID and Taxonomy information.



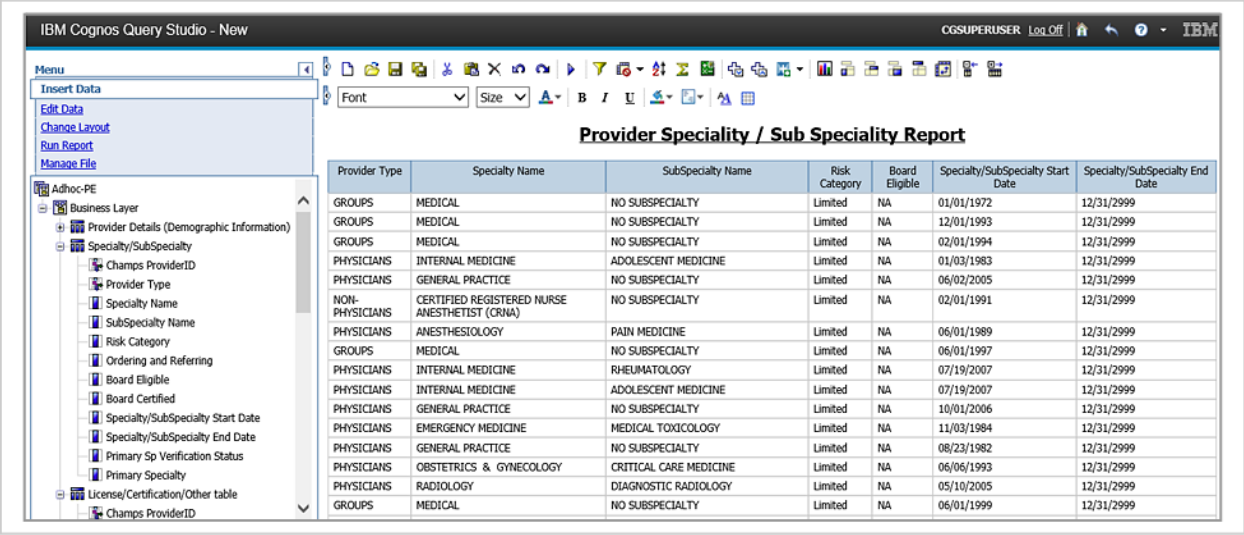
MTPSM-3-431

Figure 3.10.15-22. Provider Information Report Filtered by Taxonomy. A sample ad hoc report designed in IBM Cognos BI Query Studio to display NPI, Provider ID, and Taxonomy information.

REP128

The Contractor's solution shall provide ad hoc query capability for retrieval of data relevant to specific operational and program business units.

Team CNSI's ad hoc reporting for evoBrix PMIS is facilitated by OLTP, and is in turn integrated with evoBrix application. IBM Cognos BI Packages are designed to contain information relating to multiple subsystems per business requirements. These packages contain data elements, organized in a user-friendly way making it easier to navigate and identify data elements. Users can simply drag and drop the business elements required into their workspace to create their own customized ad hoc report. Due to the granular nature of data storage in OLTP, reports could be created at different aggregation levels (detail or summary) tied to various dimensions. Figure 3.10.15-23 shows a sample provider specialty report designed on ad hoc models using IBM Cognos BI Query Studio.



Provider Type	Specialty Name	SubSpecialty Name	Risk Category	Board Eligible	Specialty/SubSpecialty Start Date	Specialty/SubSpecialty End Date
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	01/01/1972	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	12/01/1993	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	02/01/1994	12/31/2999
PHYSICIANS	INTERNAL MEDICINE	ADOLESCENT MEDICINE	Limited	NA	01/03/1983	12/31/2999
PHYSICIANS	GENERAL PRACTICE	NO SUBSPECIALTY	Limited	NA	06/02/2005	12/31/2999
NON-PHYSICIANS	CERTIFIED REGISTERED NURSE ANESTHETIST (CRNA)	NO SUBSPECIALTY	Limited	NA	02/01/1991	12/31/2999
PHYSICIANS	ANESTHESIOLOGY	PAIN MEDICINE	Limited	NA	06/01/1989	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	06/01/1997	12/31/2999
PHYSICIANS	INTERNAL MEDICINE	RHEUMATOLOGY	Limited	NA	07/19/2007	12/31/2999
PHYSICIANS	INTERNAL MEDICINE	ADOLESCENT MEDICINE	Limited	NA	07/19/2007	12/31/2999
PHYSICIANS	GENERAL PRACTICE	NO SUBSPECIALTY	Limited	NA	10/01/2006	12/31/2999
PHYSICIANS	EMERGENCY MEDICINE	MEDICAL TOXICOLOGY	Limited	NA	11/03/1984	12/31/2999
PHYSICIANS	GENERAL PRACTICE	NO SUBSPECIALTY	Limited	NA	08/23/1982	12/31/2999
PHYSICIANS	OBSTETRICS & GYNECOLOGY	CRITICAL CARE MEDICINE	Limited	NA	06/06/1993	12/31/2999
PHYSICIANS	RADIOLOGY	DIAGNOSTIC RADIOLOGY	Limited	NA	05/10/2005	12/31/2999
GROUPS	MEDICAL	NO SUBSPECIALTY	Limited	NA	06/01/1999	12/31/2999

MTPSM-3-361

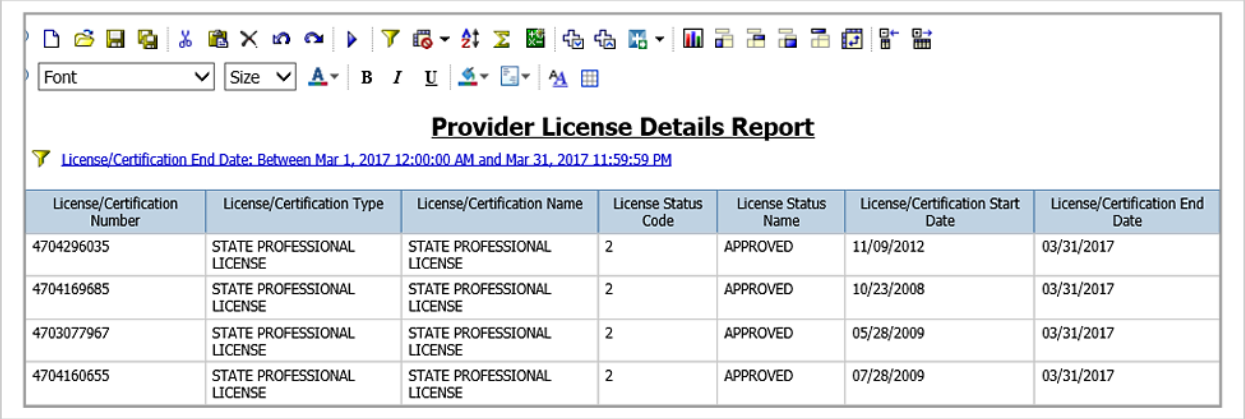
Figure 3.10.15-23. Ad hoc Model Based Report. A sample ad hoc report designed in IBM Cognos BI Query showcasing the query subjects derived from ad hoc provider model.

REP129

The Contractor's solution shall provide an online adhoc reporting tool that allows authorized users access to provider and trading partner data (e.g., provider enrollment status, alphabetic and numeric provider listing, re-certification listing, revalidation listing, group affiliation listing, provider classification listing, and category of service listing).

Team CNSI's ad hoc reporting for evoBrix PMIS comprises of IBM Cognos BI Packages that provide authorized users with access to provider and trading partner enrollment information. IBM Cognos BI Packages, a set of metadata objects, are designed to contain information relating specifically to provider information such as enrollment status, provider listing, classification, service categorization, certification, and re-validation. Packages contain data elements, organized in a user-friendly way which makes it easy to navigate and identify data elements. Users can simply drag and drop the business elements into their workspace to create customized ad hoc reports. The reports could either be at a summary or detail level

due to granular level of data storage in evoBrix OLTP. Figure 3.10.15-24 shows a sample ad hoc report designed in IBM BI Cognos Query Studio to display provider licensing information



Provider License Details Report

License/Certification End Date: Between Mar 1, 2017 12:00:00 AM and Mar 31, 2017 11:59:59 PM

License/Certification Number	License/Certification Type	License/Certification Name	License Status Code	License Status Name	License/Certification Start Date	License/Certification End Date
4704296035	STATE PROFESSIONAL LICENSE	STATE PROFESSIONAL LICENSE	2	APPROVED	11/09/2012	03/31/2017
4704169685	STATE PROFESSIONAL LICENSE	STATE PROFESSIONAL LICENSE	2	APPROVED	10/23/2008	03/31/2017
4703077967	STATE PROFESSIONAL LICENSE	STATE PROFESSIONAL LICENSE	2	APPROVED	05/28/2009	03/31/2017
4704160655	STATE PROFESSIONAL LICENSE	STATE PROFESSIONAL LICENSE	2	APPROVED	07/28/2009	03/31/2017

MTPSM-3-366

Figure 3.10.15-24. Ad hoc Report for Provider Licensing Information. A sample ad hoc report designed in IBM Cognos BI Query displaying information regarding Provider Licensing

REP130

The Contractor's reporting tool shall provide current and historical information about user access. The report shall include both standardized data in addition to allowing user input of run criteria such as user IDs, roles/privileges/authorizations, and configurable from and to dates.

Team CNSI's reporting solution – Common components reports will enable authorized users/supervisors to run reports regarding user access information. These reports can be scheduled or on demand. The on-demand reports can be parameterized as well, enabling reports specific to user IDs, roles/privileges/authorizations, and even configurable from and to dates. Below are a few reports that are executed out of Team CNSI's reporting solution, for user access audit information

- 60-Day No-Access Report
- Multiple ID Report
- Security Access Report
- User ID Report

Figure 3.10.15-25 shows a sample output of the standard 60-Day No-Access security report that comes with Team CNSI's reporting solution.

	A	B	C	D	E	F
1	Report Date: 10/18/2017 1:46:27 PM		Montana Provider Services Module			Page: 1
2			60-Day No-Access Report			
3	User Id	Domain	First Name	Last Name	Start Date	Expiration Date
4	User 1	AUDIT	Brian	Taylor	06/28/2017	12/31/2999
5	User 2	AUDIT	Aurora	Bridget	01/20/2017	12/31/2017
6	User 3	AUDIT	Jaster	David	10/16/2017	12/31/2999
7	User 4	CrimeVictim	Walker	Gregory	02/05/2013	12/31/2999
8	User 5	DCH	Pullum	Erickson	09/03/2010	12/31/2999
9	User 6	DCH	Heffron	Gloria	06/13/2014	12/31/2999
10	User 7	DCH	Portugal	James	01/29/2014	12/31/2999
11	User 8	DCH	Spohn	Turnbull	09/14/2009	12/31/2999
12	User 9	DCH	Lowery	DuPuis	10/03/2017	12/31/2999
13	User 10	DCH	Jha	Kara	12/12/2012	12/31/2999

MTPSM-3-362

Figure 3.10.15-25. 60 Day No Access Report. A sample output of the standard 60-Day No-Access security report that comes with Team CNSI's reporting solution.

REP131

The Contractor's solution shall track and have the capability to report both summary and detail level information pertaining to provider enrollment, disenrollment, termination, re-enrollment, revalidation, and recertification.

Team CNSI's reporting solution allows users to design their own customized reports. Provider data related to enrollment, certification, and validation could be reported at detail or summary level due to the granular storage of data in evoBrix OLTP. In addition to ad hoc reporting, Team CNSI's reporting solution also comes with a set of pre-built scheduled and on-demand reports that may contain this information. Figure 3.10.15-26 shows sample IBM Cognos BI Report Studio reports that show summary and detail versions of provider vital record statistics.

Report Date: 10/15/2017 6:00:01 PM — Montana Provider Services Module — Weekly Vital Records Summary Report — Page: 1

ProviderID	Business Status	Source	Source Count
1234567	DECEASED	Federal Vital	5
5678900	DECEASED	State Vital	3

Report Date: 10/15/2017 6:00:01 PM — Montana Provider Services Module — Weekly Vital Records Detail Report — Page: 2

ProviderID	Provider Name	Business Status	Start Date	End Date	Source	Process Date
1234567	Provider Name	DECEASED	06/12/2017	12/31/2999	Federal Vital	10/02/2017
1234567	Provider Name	DECEASED	10/06/2017	12/31/2999	Federal Vital	10/12/2017
1234567	Provider Name	DECEASED	01/02/2011	12/31/2999	Federal Vital	10/02/2017
1234567	Provider Name	DECEASED	10/09/2017	12/31/2999	Federal Vital	10/12/2017
1234567	Provider Name	DECEASED	09/03/2017	12/31/2999	Federal Vital	10/02/2017
5678900	Provider Name	DECEASED	10/07/2017	12/31/2999	State Vital	10/10/2017
5678900	Provider Name	DECEASED	09/30/2017	12/31/2999	State Vital	10/03/2017
5678900	Provider Name	DECEASED	09/25/2017	12/31/2999	State Vital	10/11/2017

MTPSM-3-363

Figure 3.10.15-26. Weekly Provider Vitals Report. Sample IBM Cognos BI Report Studio reports that show summary and detail versions of provider vital record statistics.

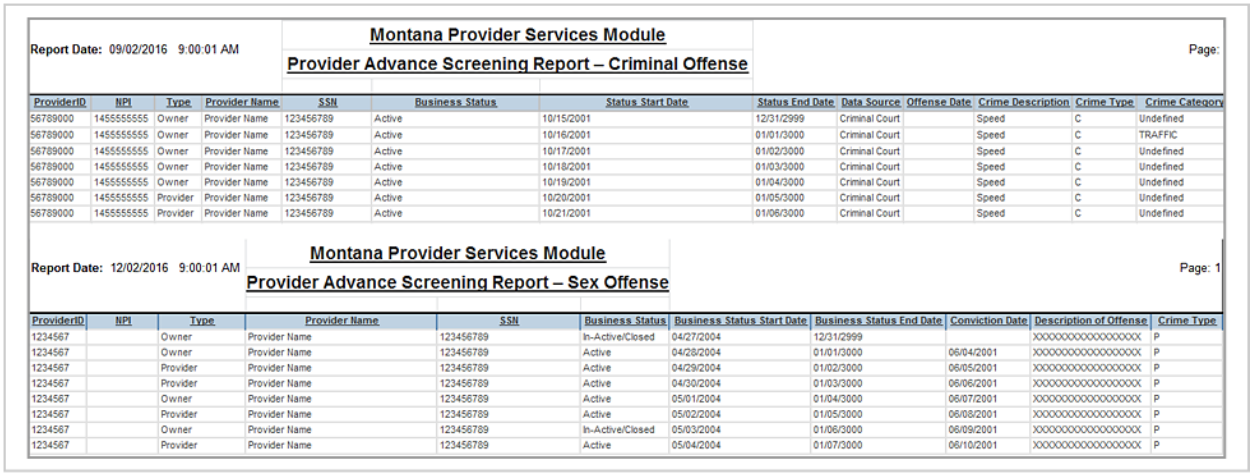
REP132

The Contractor's solution shall provide the functionality to identify, track and report the number and type of individuals associated with a provider or trading partner application (e.g., provider, facility, owner, managing employee and/or board member) including screening and monitoring results.

Team CNSI's reporting solution is capable to allowing users to design their own customized reports, when it comes to identifying, tracking, and reporting the number and type of individuals associated with a provider or trading partner application. Provider data related could be reported at detail or summary level due to the granular storage of data in evoBrix OLTP. In addition to ad hoc reporting, Team CNSI's reporting solution also comes with a set of pre-built scheduled and on demand reports that are related to provider credentialing screening and monitoring. A few of the pre-built reports are as below:

- Advance Screening Report – Criminal Offense (Provider and Owner)
- Advance Screening Report – Sex Offense (Provider and Owner)
- Sanctioned-License Expired Pharmacy Providers
- Adverse Action Report – NPI Level Report
- Adverse Action Report – Owner Level Report

Figure 3.10.15-27 shows sample report outputs for Criminal and Sex Offense Reports, designed in IBM Cognos BI Report Studio.



Report Date: 09/02/2016 9:00:01 AM

Montana Provider Services Module

Provider Advance Screening Report – Criminal Offense

Page:

ProviderID	NPI	Type	Provider Name	SSN	Business Status	Status Start Date	Status End Date	Data Source	Offense Date	Crime Description	Crime Type	Crime Category
56789000	1455555555	Owner	Provider Name	123456789	Active	10/15/2001	12/31/2999	Criminal Court		Speed	C	Undefined
56789000	1455555555	Owner	Provider Name	123456789	Active	10/16/2001	01/01/3000	Criminal Court		Speed	C	TRAFFIC
56789000	1455555555	Owner	Provider Name	123456789	Active	10/17/2001	01/02/3000	Criminal Court		Speed	C	Undefined
56789000	1455555555	Owner	Provider Name	123456789	Active	10/18/2001	01/03/3000	Criminal Court		Speed	C	Undefined
56789000	1455555555	Owner	Provider Name	123456789	Active	10/19/2001	01/04/3000	Criminal Court		Speed	C	Undefined
56789000	1455555555	Provider	Provider Name	123456789	Active	10/20/2001	01/05/3000	Criminal Court		Speed	C	Undefined
56789000	1455555555	Provider	Provider Name	123456789	Active	10/21/2001	01/06/3000	Criminal Court		Speed	C	Undefined

Report Date: 12/02/2016 9:00:01 AM

Montana Provider Services Module

Provider Advance Screening Report – Sex Offense

Page: 1

ProviderID	NPI	Type	Provider Name	SSN	Business Status	Business Status Start Date	Business Status End Date	Conviction Date	Description of Offense	Crime Type
1234567		Owner	Provider Name	123456789	In-Active/Closed	04/27/2004	12/31/2999		XXXXXXXXXXXXXXXX	P
1234567		Owner	Provider Name	123456789	Active	04/28/2004	01/01/3000	06/04/2001	XXXXXXXXXXXXXXXX	P
1234567		Provider	Provider Name	123456789	Active	04/29/2004	01/02/3000	06/05/2001	XXXXXXXXXXXXXXXX	P
1234567		Provider	Provider Name	123456789	Active	04/30/2004	01/03/3000	06/06/2001	XXXXXXXXXXXXXXXX	P
1234567		Owner	Provider Name	123456789	Active	05/01/2004	01/04/3000	06/07/2001	XXXXXXXXXXXXXXXX	P
1234567		Provider	Provider Name	123456789	Active	05/02/2004	01/05/3000	06/08/2001	XXXXXXXXXXXXXXXX	P
1234567		Owner	Provider Name	123456789	In-Active/Closed	05/03/2004	01/06/3000	06/09/2001	XXXXXXXXXXXXXXXX	P
1234567		Provider	Provider Name	123456789	Active	05/04/2004	01/07/3000	06/10/2001	XXXXXXXXXXXXXXXX	P

MTPSM-3-364

Figure 3.10.15-27. Criminal and Sex Offense Reports. Sample report outputs for Criminal and Sex Offense Reports, designed in IBM Cognos BI Report Studio.

REP133

The Contractor's solution must provide Provider Transaction Error Reporting that includes the error, the date and time the error was identified, and the provider file(s) effected.

Team CNSI's ISR solution is responsible for interface completion notifications. Exceptions on any provider processed via interfaces are captured into data structures for appropriate notification. The first stage of error handling is email notification. The notification consists of interface run times, total records loaded, and number of records that failed in processing. The threshold for reported error counts through

emails is configurable. A detailed error report extract is sent for review upon identifying more error records than the threshold value. Figure 3.10.10-28 shows a sample interface completion and error reporting for provider screening transactions.



-----Original Message-----
From: evoBrix_PROD@<state>.gov [mailto:evoBrix_PROD@<state>.gov]
Sent: Friday, July 07, 2017 5:12 PM
To: MW_Ops_Interfaces; CNSINOC; MW_TEC_SOA; MW_OPS_PESupport
Subject: DB2DB Job - (PCS monthly screening) Successful

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

**********Do Not Respond To this email**********

Interface : Provider PCS monthly screening (1268) Completed With Errors.

Interface Run Details:

Interface Run SID : 200024211
Interface ID : 1268
Interface Name : Provider PCS monthly screening
Start Time : 07/07/2017 05:08:27 PM
End Time : 07/07/2017 05:11:35 PM
Source Records : 1560
Success Records : 1558
Error Records : 2
Prerequisite Interfaces: N/A
Dependent Interfaces : N/A

All Errors logged in INTERFACE_RUN_ERROR table.

Error Specifics

Error : 1
Error Type : DATABASE ERROR
Error Description : Warning - In Review Record exists for the Provider ID - 1234567 and for the CLIA License Number 03D8765

Error : 2
Error Type : DATABASE ERROR
Error Description: Error Inserting into PCS_SCRNG_RESULTS for Provider_id: 7654321 ORA-06502: PL/SQL: numeric or value error: character string buffer too small at "PCS_BTCH_PRVDR_MNTHLY_SCRNG", line 4031

Error : 3
Error Type : DATABASE ERROR
Error Description : Warning - In Review Record exists for the Provider ID - 3334444 and for the CLIA License Number 42D2038

Error : 4
Error Type : DATABASE ERROR
Error Description : Error Inserting into PCS_SCRNG_RESULTS for Provider_id: 4445555 ORA-06502: PL/SQL: numeric or value error: character to number conversion error at "PCS_BTCH_PRVDR_MNTHLY_SCRNG", line 3894

**********Do Not Respond to This Email**********

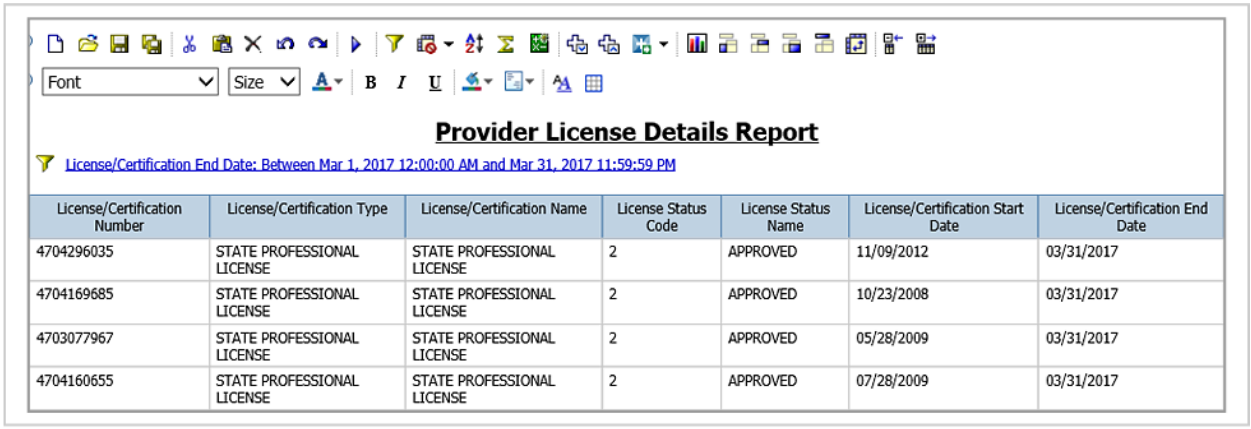
MTPSM-3-460

Figure 3.10.15-28. Team CNSI's ISR Interface Completion Notification. A sample interface completion and error reporting for provider screening in PCS.

REP134

The Contractor's solution shall have the ability for users to query using date and/or date ranges for scheduled and ad hoc reporting.

As described earlier in addressing parameterized ad hoc reporting, Team CNSI's reporting solution enables users to provide query parameters that could be date ranges or a specific date. The query parameters could also be displayed along with the report output. Figure 3.10.15-29 shows a sample IBM Cognos BI Query Studio report designed with date query parameters.



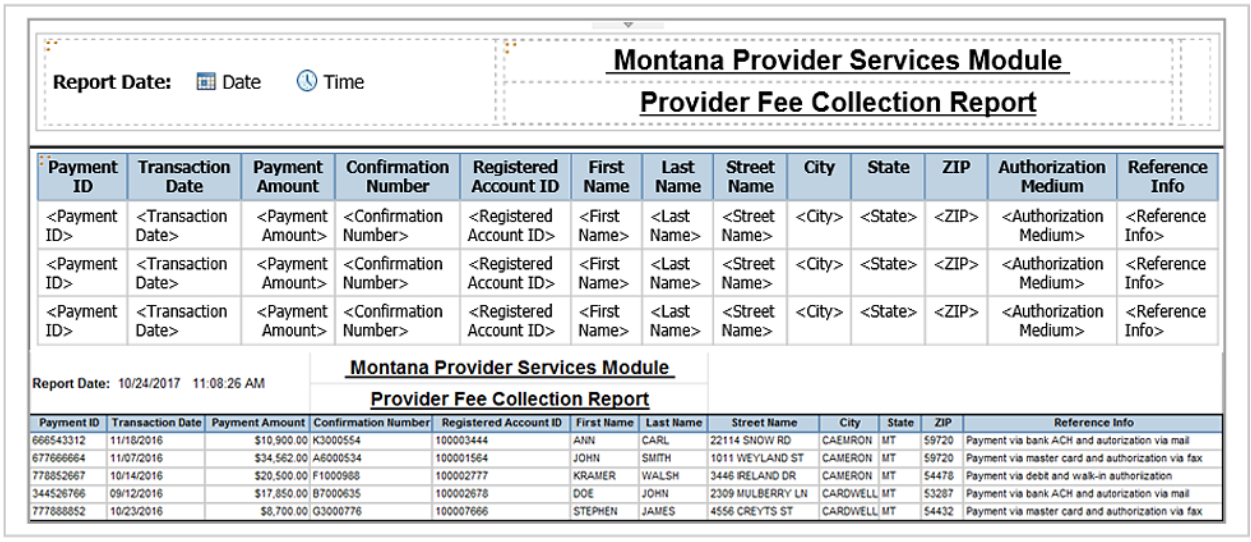
MTPSM-3-366

Figure 3.10.15-29. Parameterized Report with Query Date Ranges. A sample IBM Cognos BI Query Studio report designed with date query parameters.

REP135

The Contractor's solution shall provide the ability to report on electronic payments received through the Provider Services module (i.e., provider application fees).

Team CNSI's reporting solution enables pre-built and scheduled reporting that could be used to design reports on electronic payments received through MT PSM. The frequency of these scheduled reports can be adjusted according to DPHHS requirements. As a part of provider fee collection reporting, the reports would include but not limited to provider demographic, application fee payment status, delays or default, if any. Figure 3.10.15-30 shows the data elements in a sample Provider Fee Collection electronic payment report.



Report Date: Date Time

Montana Provider Services Module

Provider Fee Collection Report

Payment ID	Transaction Date	Payment Amount	Confirmation Number	Registered Account ID	First Name	Last Name	Street Name	City	State	ZIP	Authorization Medium	Reference Info
<Payment ID>	<Transaction Date>	<Payment Amount>	<Confirmation Number>	<Registered Account ID>	<First Name>	<Last Name>	<Street Name>	<City>	<State>	<ZIP>	<Authorization Medium>	<Reference Info>
<Payment ID>	<Transaction Date>	<Payment Amount>	<Confirmation Number>	<Registered Account ID>	<First Name>	<Last Name>	<Street Name>	<City>	<State>	<ZIP>	<Authorization Medium>	<Reference Info>
<Payment ID>	<Transaction Date>	<Payment Amount>	<Confirmation Number>	<Registered Account ID>	<First Name>	<Last Name>	<Street Name>	<City>	<State>	<ZIP>	<Authorization Medium>	<Reference Info>

Report Date: 10/24/2017 11:08:26 AM

Montana Provider Services Module

Provider Fee Collection Report

Payment ID	Transaction Date	Payment Amount	Confirmation Number	Registered Account ID	First Name	Last Name	Street Name	City	State	ZIP	Reference Info
666543312	11/18/2016	$10,900.00	K3000554	100003444	ANN	CARL	22114 SNOW RD	CAEMRON	MT	59720	Payment via bank ACH and autorization via mail
677666664	11/07/2016	$34,562.00	A6000534	100001564	JOHN	SMITH	1011 WEYLAND ST	CAMERON	MT	59720	Payment via master card and authorization via fax
778852667	10/14/2016	$20,500.00	F1000988	100002777	KRAMER	WALSH	3446 IRELAND DR	CAMERON	MT	54478	Payment via debit and walk-in authorization
344526766	09/12/2016	$17,850.00	B7000635	100002678	DOE	JOHN	2309 MULBERRY LN	CARDWELL	MT	53287	Payment via bank ACH and autorization via mail
777888852	10/23/2016	$8,700.00	G3000776	100007666	STEPHEN	JAMES	4556 CREYTS ST	CARDWELL	MT	54432	Payment via master card and authorization via fax

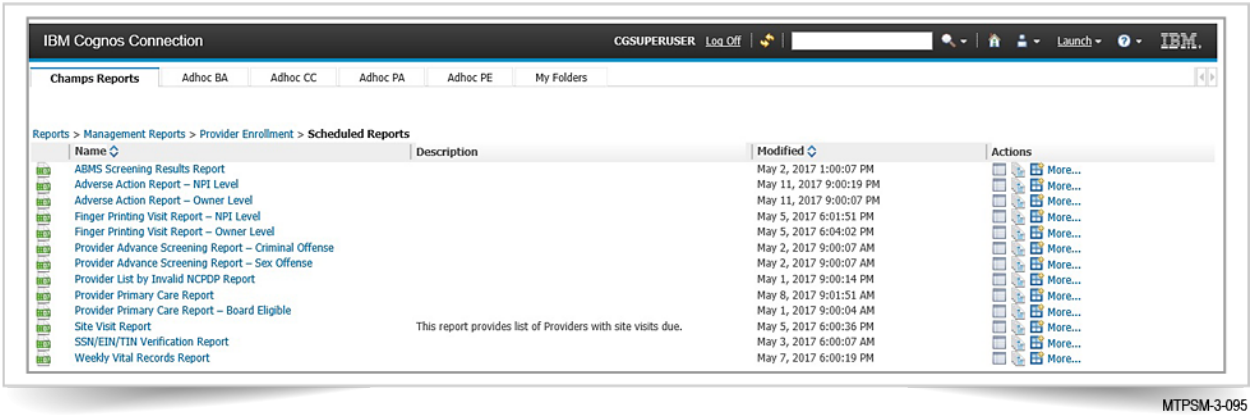
MTPSM-3-432

Figure 3.10.15-30. Provider Fee Collection Report Data Elements. A sample Report designed in IBM Cognos BI Report Studio for Provider Fee Collection.

REP136

The Contractor's solution shall provide the capability to archive and discontinue. The solution shall be capable of purging reports in compliance with the Federal and State retention policies.

Team CNSI's reporting solution contains several management and operational reports that are pre-built and scheduled to run from the transaction OLTP, on a daily/weekly basis. These reports will also be made available through IBM Cognos BI Connection Portal for viewing and retrieval. The report outputs are archived and integrated into IBM Cognos BI Content Store and could be retained according to pre-defined retention policies. Figure 3.10.15-31 shows various scheduled report output versions stored in Content Store, viewable through IBM Cognos BI Connection Portal.



MTPSM-3-095

Figure 3.10.15-31. Report Output Archival and Storage. A screenshot showing various scheduled report output versions stored in Content Store, viewable through IBM Cognos BI Connection Portal.

REP23

The Contractor's solution shall maintain reporting services that are backward compatible, and the reports functionality is preserved over major or minor releases or the contractor will provide migration support to move reports forward.

Team CNSI's reporting solution enhancements are closely tied to and follow the evoBrix PMIS operational release processes. All components tied to reports (pre-built reports and ad hoc models) and report functionality is version maintained and could be reverted in conjunction with the corresponding operational release rollback. This ensures that once a report is defined and operational, the integrity of that report is maintained through software changes including but not limited to, upgrades, patches, fixes, defect corrections, and enhancements. Please refer to Section 3.10.4, Operations, Maintenance, and Configuration, for more details on Operational Release processes.

REP31

The Contractor's reporting solution shall support initiation of reports through various methods including on-demand, scheduled requests (including non-business hours), and event-driven requests with distribution of the report results to specified secure locations.

Team CNSI's reporting solution follows three different modes of report delivery: Scheduled, On Demand, and Ad hoc Reporting.

Scheduled Reports

Scheduled reports are automatically generated based on a fixed schedule, finalized during requirements gathering. Users are notified via auto-generated emails once the report execution completes on a given schedule. Team CNSI's reporting solution contains several management and operational reports that are scheduled to run from the transaction OLTP, on a daily/weekly basis. These reports will also be made available through IBM Cognos BI Connection Portal for viewing and retrieval. The report outputs are archived and integrated into IBM Cognos BI Content Store and could be retained according to pre-defined retention policies. Figure 3.10.15-32 shows various scheduled report output versions in IBM Cognos BI Connection Portal.

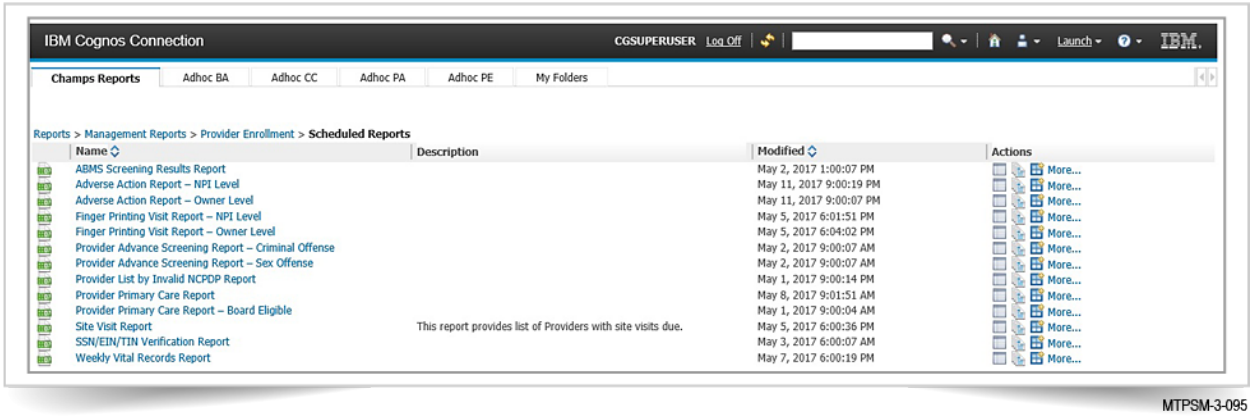


Figure 3.10.15-32. IBM Cognos Connection Portal. Screenshot showing different report outputs for scheduled reports in IBM Cognos Connection Portal.

On-Demand Reports

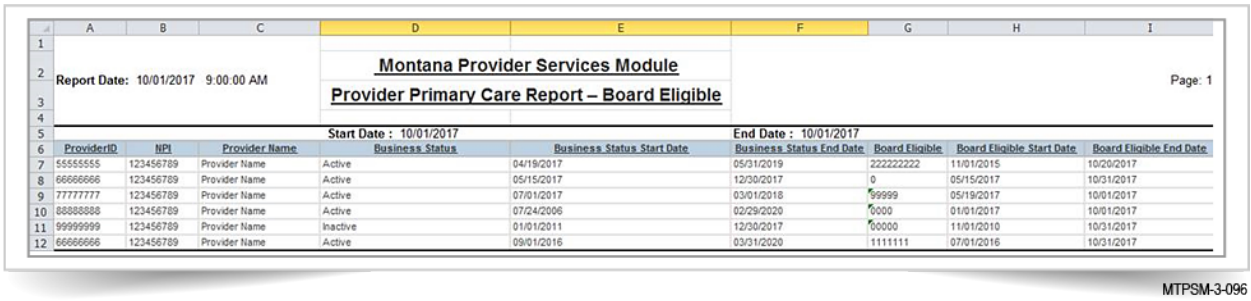
On-Demand Reports are generated based on user action. These reports are generally parameterized and will require some user input before they can be executed. The prompts may be based on dates, numbers or text. IBM Cognos BI validates user input values in the correct format. It will be up to the discretion of the user to save the reports locally, view, or discard them, as these outputs will not be available in the IBM Cognos BI Content Store repository. IBM Cognos BI Connection Portal allows users to access on-demand reports.

Ad Hoc Reports

In the context of MT PSM, ad hoc reporting is a frequent occurrence. Hence, it is important to have a tool that provides an easy interface to create and execute reports. IBM Cognos BI suite of tools offers Query Studio for analytical users to create, modify, view, and change the appearance and the distribution of ad hoc reports.

Team CNSI's ad hoc reporting for evoBrix PMIS is facilitated by OLTP, using IBM Cognos BI Query Studio. This is in turn integrated with evoBrix application. IBM Cognos BI Packages, a set of metadata objects, are designed to contain information relating specifically to one or multiple subsystems per business requirements. Packages contain data elements organized in a user-friendly way, which makes it easy to navigate and identify data elements. The complexity of the tables and relationships is hidden from the user for an enhanced self-service user experience.

Users can simply drag and drop the business elements required into their workspace to create their own customized ad hoc report. Due to the granular nature of data storage in OLTP, reports could be created at different aggregation levels (detail or summary) tied to various dimensions. Though this is applicable to pre-built reports as well, ad hoc reporting provides the user with the flexibility to create their own customized reports. They can also execute, generate the query or report, and can save in various formats including HTML, Excel, CSV, and PDF. Figure 3.10.15-33 shows a sample ad hoc report in Excel format.



Report Date: 10/01/2017 9:00:00 AM

Montana Provider Services Module

Provider Primary Care Report – Board Eligible

Page: 1

Start Date : 10/01/2017 End Date : 10/01/2017

ProviderID	NPI	Provider Name	Business Status	Business Status Start Date	Business Status End Date	Board Eligible	Board Eligible Start Date	Board Eligible End Date
55555555	123456789	Provider Name	Active	04/19/2017	05/31/2019	222222222	11/01/2015	10/20/2017
66666666	123456789	Provider Name	Active	05/15/2017	12/30/2017	0	05/15/2017	10/31/2017
77777777	123456789	Provider Name	Active	07/01/2017	03/01/2018	99999	05/19/2017	10/01/2017
88888888	123456789	Provider Name	Active	07/24/2006	02/29/2020	0000	01/01/2017	10/01/2017
99999999	123456789	Provider Name	Inactive	01/01/2011	12/30/2017	00000	11/01/2010	10/31/2017
66666666	123456789	Provider Name	Active	09/01/2016	03/31/2020	1111111	07/01/2016	10/31/2017

MTPSM-3-096

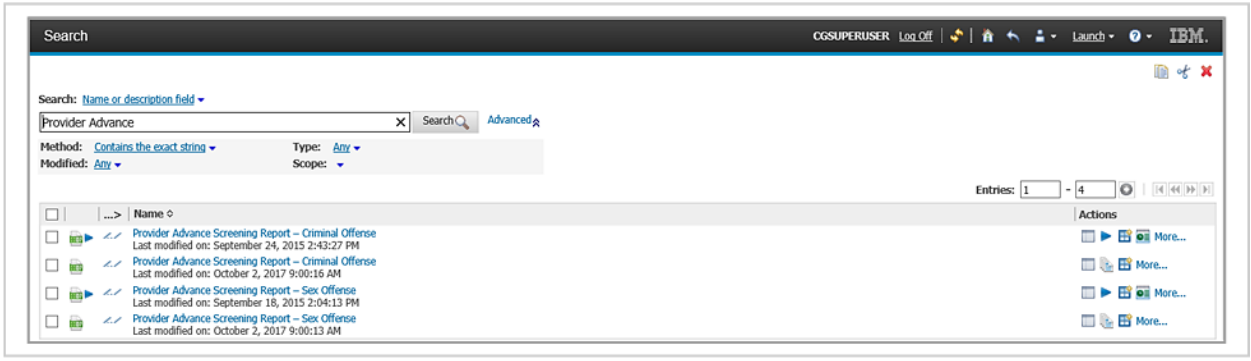
Figure 3.10.15-33. Excel Format Output. Screenshot showing a sample ad hoc report in Excel format.

REP32

The Contractor's reporting solution shall allow users to search on criteria including report names, report filters, and data elements included in the report in a library or repository of reports.

Team CNSI's reporting solution leverages IBM Cognos BI connection search feature that will enable users to search by report name and description. Users could refer to the Detail System Design Document (DSDD) to further explore the complete definition of the report such as prompt definitions, special

requirements, report filters, and data elements present in the report. Figure 3.10.15-34 shows how search criteria are used in IBM Cognos BI Connection Portal to list relevant reports.



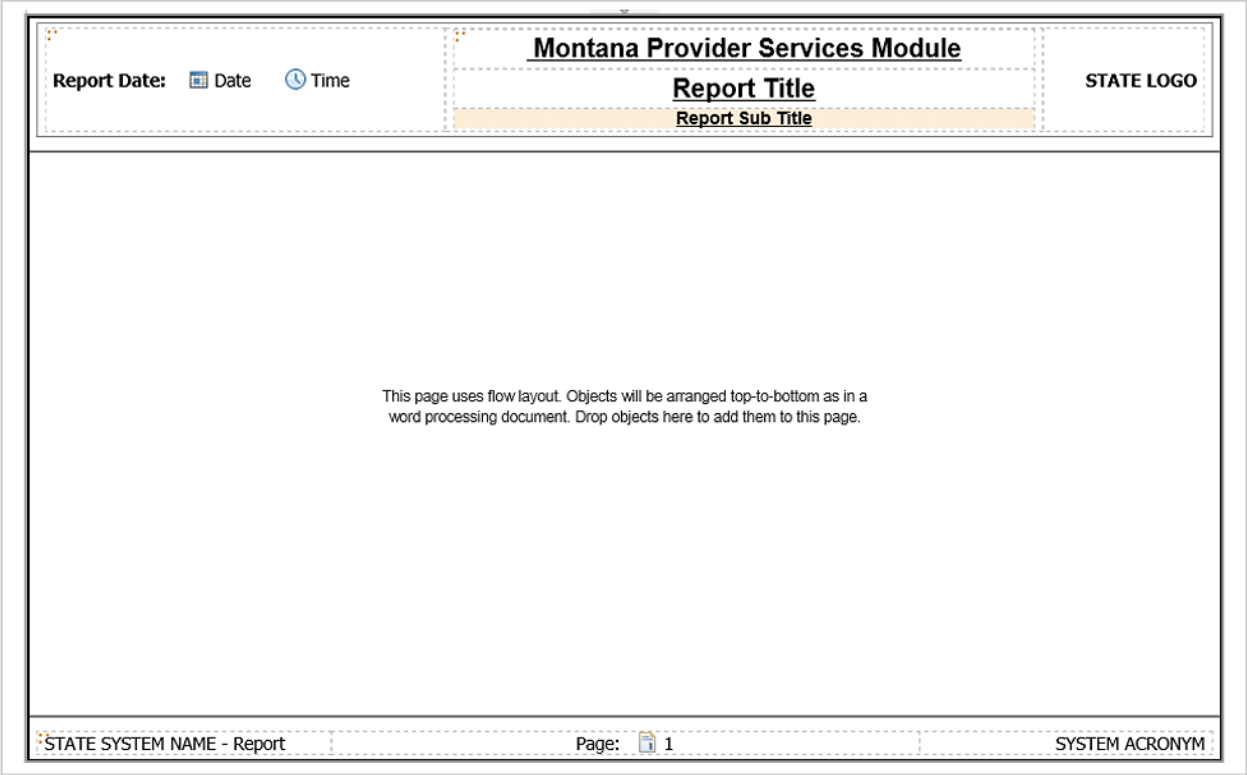
MTPSM-3-368

Figure 3.10.15-34. IBM Cognos BI Connection Portal Search. A sample shows how search criteria are used in IBM Cognos BI Connection Portal to list relevant reports.

REP36

The Contractor's reporting solution must display standard report header and footer information (e.g., report number, report title, page number, date) on all reports.

Team CNSI's reporting solution uses IBM Cognos BI Report Studio to design pre-built reports that are scheduled or on demand. All Report Studio reports including the list of system included reports follow header and footer standards defined by DPHHS business requirements including, but not limited to report number, report title, page number, and report date. Figure 3.10.15-35 shows a sample report template with all the header and footer fields available in on-demand or scheduled reporting.



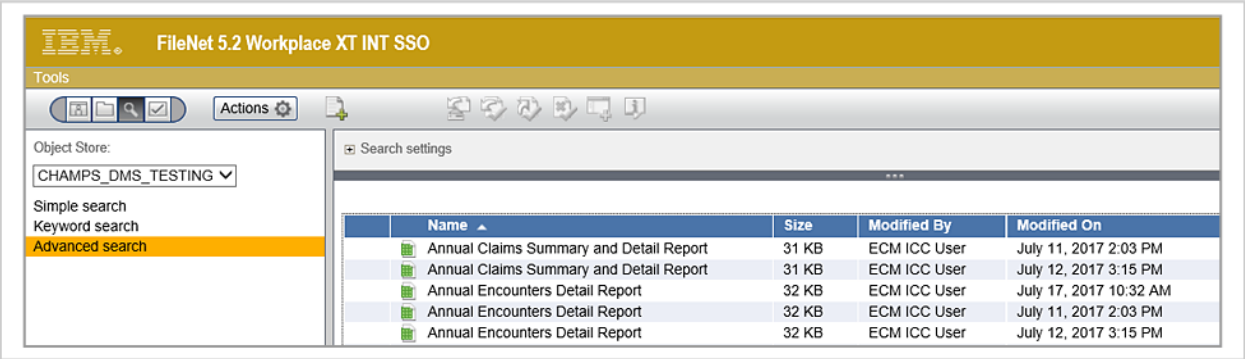
MTPSM-3-367

Figure 3.10.15-35. Standard Report Template. A sample report template with all the header and footer fields available in on-demand or scheduled reporting.

REP37

The Contractor's reporting solution shall provide the ability to store system generated reports in the Enterprise Content Management (ECM).

Team CNSI's reporting solution using IBM Cognos Content Archival, provides the capability to configure an enterprise content management (ECM) storage that is outside of IBM Cognos BI to store scheduled report outputs. Cognos Archival decides the archival criteria based on retention criteria in Content Store and uses background jobs to move the files to ECM automatically. Access to the report outputs will be the same as it is in IBM Cognos BI content store. These report outputs can be archived based on DPHHS defined retention policies. The report outputs can be shared with external applications or users who don't have access to Team CNSI's reporting solution. Figure 3.10.15-36 shows the list of reports output saved in ECM.



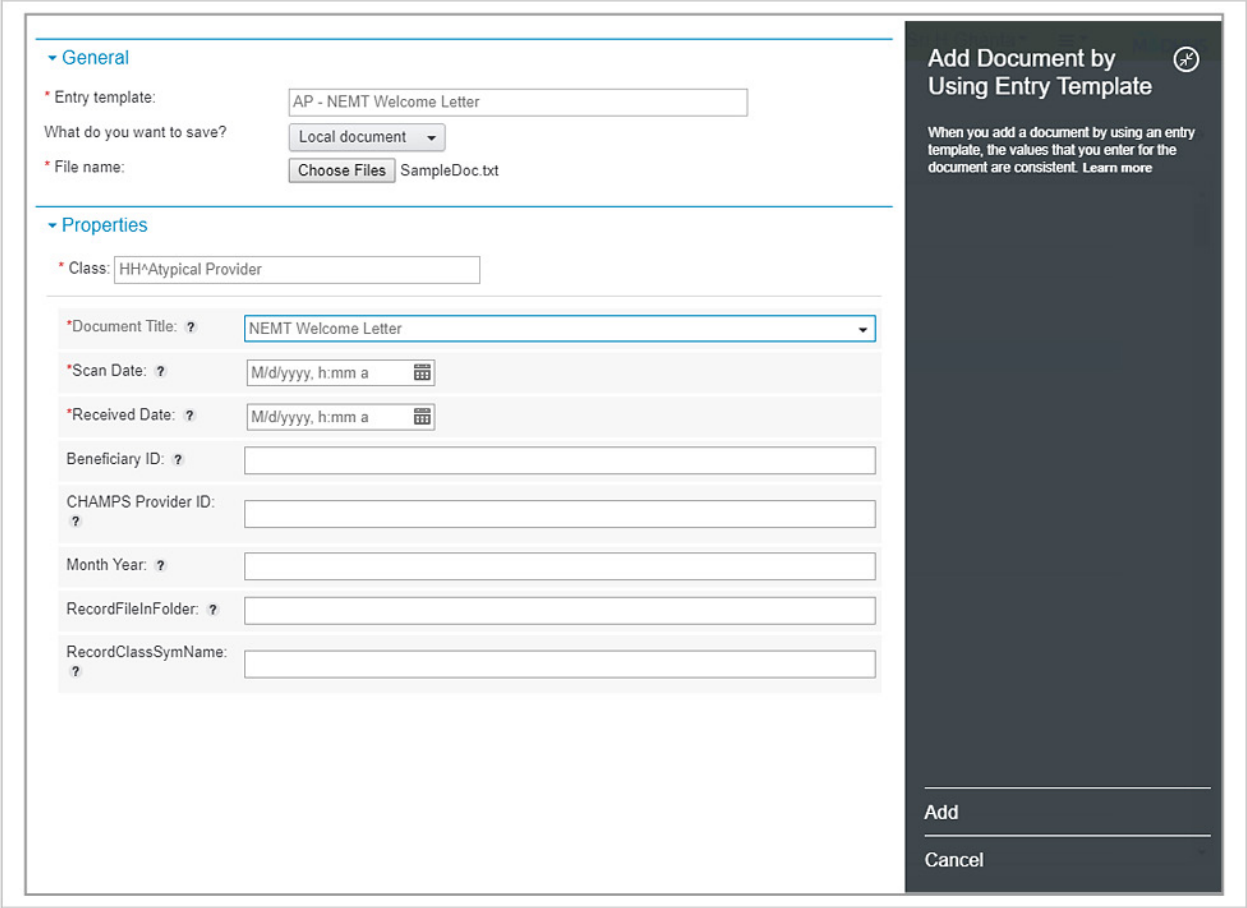
MTPSM-3-433

Figure 3.10.15-36. Report Output Stored in ECM. A screenshot showing the list of report output saved in ECM.

REP38

The Contractor's reporting solution shall allow a user to manually save report output to the ECM.

Team CNSI's reporting solution using IBM Cognos BI, provides the capability to configure ECM that is outside of IBM Cognos BI to save the individual report output files. This feature will enable both on demand and scheduled report outputs to be saved to the ECM. While the scheduled reports automatically save the output using IBM Cognos BI Content Archival, the on-demand report output can be manually saved to a desired location in the ECM. Figure 3.10.15-37 shows the upload screen for evoBrix ECM to manually upload reports into ECM.



MTPSM-3-434

Figure 3.10.15-37. ECM Upload Screen. A screenshot shows the upload screen for evoBrix ECM to manually upload reports into ECM.

REP39

The Contractor's solution shall provide efficient navigation (e.g., the ability to move forward and backward in the solution).

Team CNSI's reporting solution allows user access through a secure profile setup to IBM Cognos BI Connection Portal. The portal is accessed from the "External Links" tab within evoBrix and displays several attributes of reports such as Report Name, Run Frequency, Output Format, and Restricted Flag (based on user security and access privileges). The Connection Portal offers a single point of access for all reports including on demand reports, Scheduled Report output and Ad-hoc queries. Users will be able to seamlessly navigate forward and backward to access the Report folders within Cognos Connection Portal Page. The content (Reports) of the portal page is based on the Security Matrix User Profiles, and will vary with user profiles. Figure 3.10.15-38 shows the home page of the IBM Cognos BI Connection Portal.



Figure 3.10.15-38. Reports Navigation in IBM Cognos Connection Portal. Screenshot showing IBM Cognos BI Connection Portal from which reports can be accessed.

REP42

The Contractor's reporting solution shall allow authorized users to view, sort, export and print dashboard and report data in a variety of formats (e.g., HTML, Excel, TXT, CSV, PDF, or character delimited).

Team CNSI's reporting solution includes IBM Cognos BI Viewer that allows the user to export reports into various formats, such as HTML, Excel, CSV, or PDF. Figure 3.10.15-39 shows a sample report in IBM Cognos BI Viewer. The user can change output formats using the option in IBM Cognos BI Viewer.

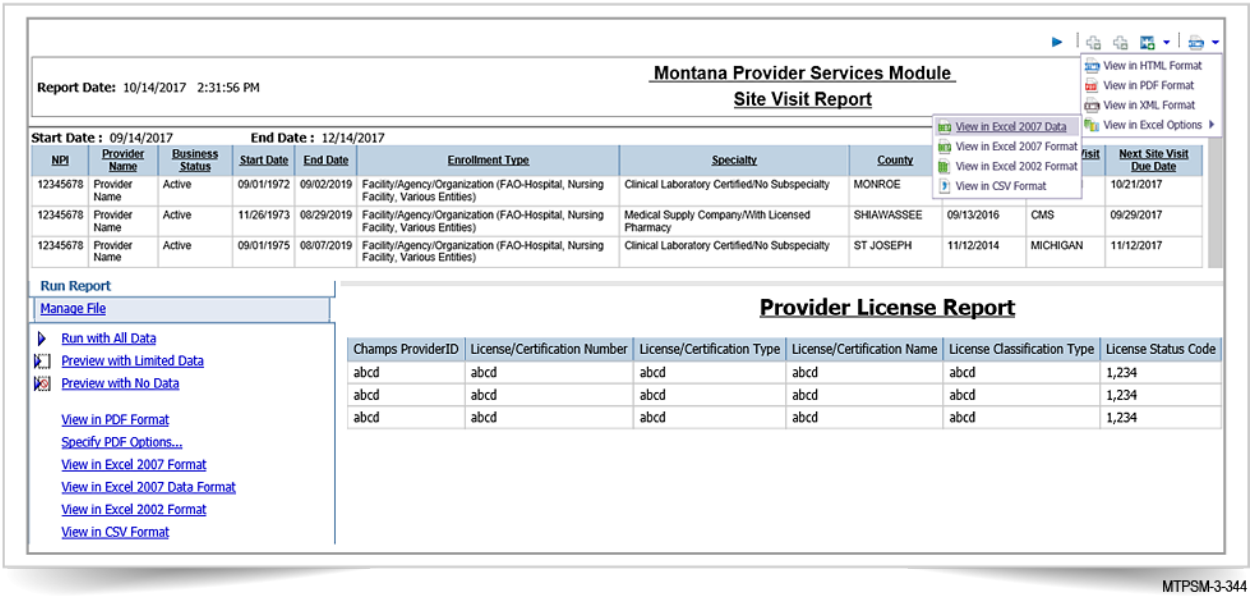


Figure 3.10.15-39. Report Export Formats. A sample of a pre-built IBM Cognos BI Report Studio report that shows how to view or export a standard report in different formats.

REP64

The Contractor's solution shall provide the ability to access and use all current and historical data for reporting purposes.

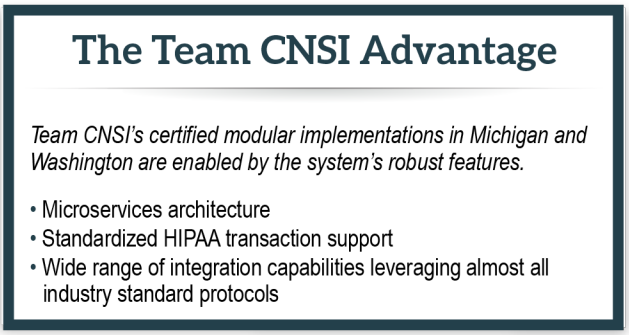
All current and historical provider information is retained in evoBrix OLTP, according to DPHHS defined data retention policies. Team CNSI's reporting solution uses On Demand, Ad hoc, and Scheduled Reporting to access all current and historical data on provider related information stored in evoBrix

OLTP. The reports could be designed to be queried using user specified parameters such as dates or active status that allow tracing the oldest information stored in evoBrix OLTP.

3.10.13 Option A Provider Services

In addition to the primary scope of the Provider Services module, states may procure additional provider self-service portal components and services for activities not categorized in Section 3.10.1 through 3.10.12. These services are integral to the provider's ability to complete necessary activities in order to participate in one or more of State healthcare programs. Option A Provider Services requirements provide flexibility to State's or Agencies who may desire to procure the components or services outlined in Option A as a part of this procurement versus a separate procurement. The Offeror is not required to include Option A in their proposal. If the Offeror chooses to include these services in their proposal the Offeror must describe in their response, their approach to meet the Option A requirements detailed Attachment F, Requirements Matrix.

Team CNSI's innovative approach for Option A Provider Services includes leveraging the evoBrix platform's modular capabilities along with using industry standard HIPAA transactions.

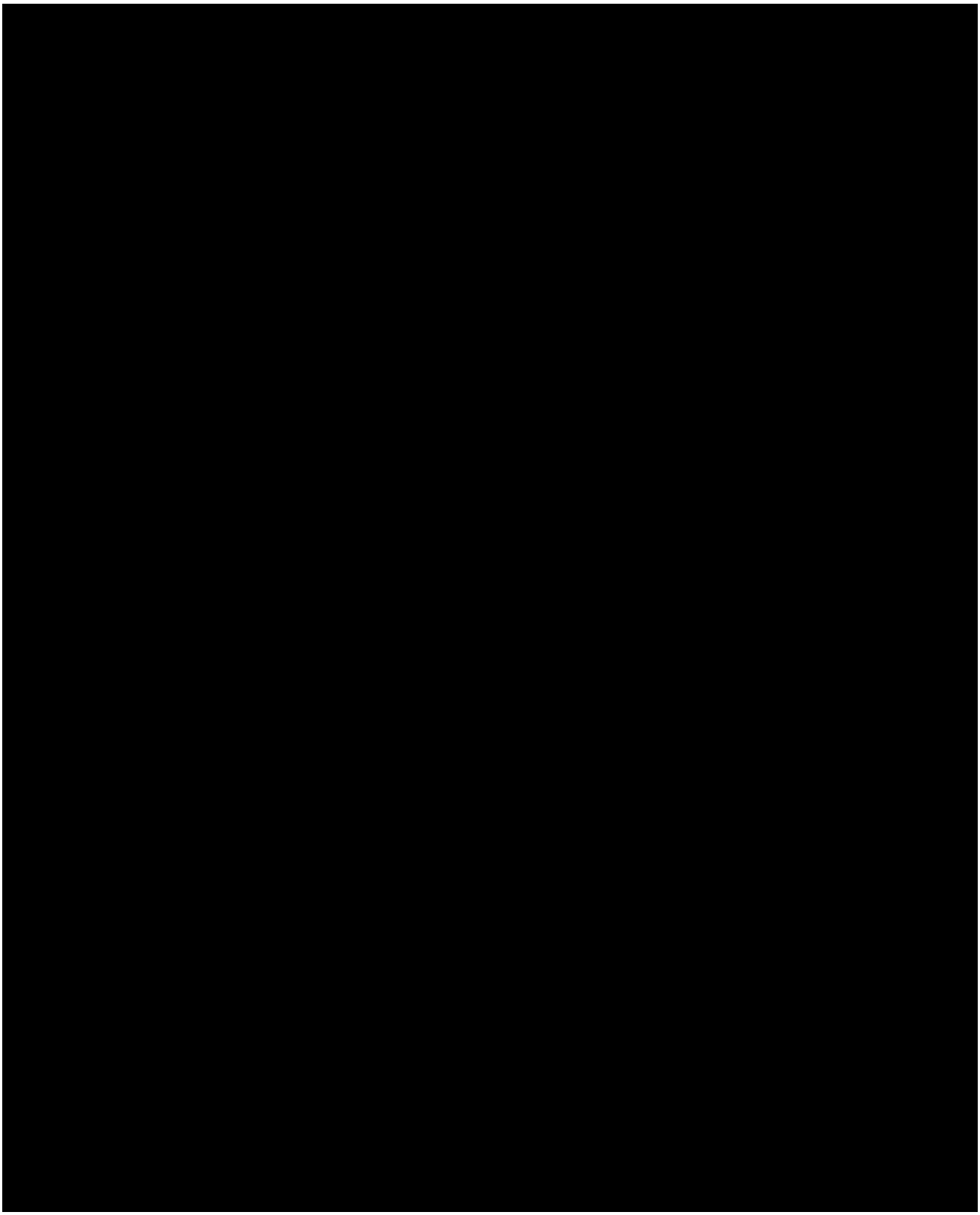


MTPSM-3-458

Team CNSI is working across states and with CMS to define a comprehensive, reusable, open-source technical architecture to support Medicaid Information Technology Architecture (MITA) business categories. The goal of this work is to provide a Medicaid-specific reference architecture that can be leveraged across State Medicaid Agencies (SMAs) to implement commutable, interoperable Medicaid Management Information Systems (MMIS). Through engagement with industry stakeholders to create a MITA reference architecture, Team CNSI is helping to create standard definitions for application services to combine business processes into standard objects to be packaged into modules. The development of a modular reference architecture across MITA business categories progresses the concept of modular design and reinforces the Medicaid Enterprise commitment to the Seven Standards and Conditions.

Team CNSI's evoBrix platform's configurable and modular design and standard transaction capabilities are engineered to implement the Option A Provider Services that NASPO participating states may procure.

Figure 3.10.13-1 illustrates evoBrix's high-level solution architecture supporting the Option A Provider Services requirements and how it will achieve integration with other DPHHS MMIS modules.



©2017 CNSI | Option A-2

Option A – High Level Solution Components

- evoBrix Self-service Portal follows responsive web design principles allowing users to securely inquire about eligibility, claims, and remittance advice data, and allow for Direct Data Entry (DDE) of claims.
- evoBrix Translator converts the web-based form data accumulated as business objects to standard HIPAA transactions by leveraging the Edifecs translation engine.
- evoBrix Integrator allows for audit capability and SOA-based integrations with the MPATH Integration Hub. evoBrix Integrator allows providers to directly submit HIPAA transaction files wherever applicable.
- The MPATH Integration Hub will receive HIPAA files, as shown in Figure 3.10.13-1, and, wherever applicable, will return valid HIPAA responses for evoBrix to consume.

evoBrix Solution Components Details

Self-service Portal

As depicted in Figure 3.10.13-1, the Option A solution provides secure access to providers and other authorized business users. evoBrix integrates with the Access and Identity Management infrastructure in the DPHHS environment and provides secure access to the self-service portal.

evoBrix's self-service features provide users access to business information and communication via a web portal. Accessibility services are integrated with security services to ensure that only authorized users are provided with access to secured information. Accessibility layer services leverage the evoBrix user interface components.

evoBrix Translator

evoBrix leverages industry leading Edifecs XEngine capabilities to achieve validations and translations to HIPAA standard transactions.

Edifecs XEngine Server delivers unparalleled performance to validate transactions for syntax, semantics, and custom business rules, thereby ensuring operational integrity of information exchange with trading partners. As shown in Figure 3.10.13-1, Edifecs XEngine Server's enterprise-strength throughput capabilities enable fast and accurate validation of transactions at the edge of the enterprise. By catching errors early, XEngine Server can separate good data from bad data, thus allowing organizations to comply with legislative and company mandates for streamlined processes, real-time access, and faster processing times. Good data can be further split into smaller logical units for efficient processing, and routed to multiple downstream systems based on the contents of the transaction. XEngine Server's translation capabilities allow data conversion between industry-standard HIPAA formats and downstream system formats.

XEngine Capabilities:

- Visually model and control the flow of transaction messages using an integrated, business process orchestration tool.
- Achieve high-speed, high-quality transaction performance by integrating data from all channels into a unified front-end system that uses a single-pass data processing approach to achieve highly scalable performance, while providing for clean error recovery and improved manageability.
- Validate inbound and outbound transactions against defined guidelines to eliminate bad transactions at the edge of the enterprise; generate acknowledgements and easy-to-read reports.

- Translate data using sophisticated pattern recognition technology that automatically determines the format of incoming data and then directly translates into a target format using maps that can be selected based on trading partner and/or industry standard transaction type including HIPAA and HL7.
- Split and route transaction data by breaking data into logical groups based on error status, and then routing to the appropriate destination based on data content or user-defined splitting rules.
- Customize front-end transaction processing by modifying data using rules specified in guidelines, or by using the Translator module to implement more complex data translations.
- Integrate with core systems and third-party applications, using various adapters and connectors that streamline transaction flow and reduce custom development.
- Rapidly achieve Operating Rules compliance by leveraging pre-defined system routes and Edifecs XEngine Server's superior performance.
- Route bad data to work queues or send alerts to users for exception management in near real time.

evoBrix Integrator

Team CNSI's evoBrix Integrator is comprised of the Oracle Fusion SOA middleware. Team CNSI's evoBrix Integrator can handle DPHHS integration for transmittal of data to align with the conceptual solution architecture. The solution can be configured to meet the data transfer needs per DPHHS' requirements.

Team CNSI's evoBrix Integrator offers batch and near real-time data trading of interfaces with MMIS modules. The solution supports inbound and outbound interfaces, service mediation, and pass-through with MMIS modules.

Team CNSI also supports data trading with MMIS modules in real-time via evoBrix Oracle Service Bus (OSB) web services. The evoBrix architecture uses an enterprise class service bus (Oracle Fusion SOA) as the core orchestration tool of business processes across the different applications that support Medicaid operations. evoBrix supports robust authorization, authentication, and validation features using OSB. The solution is capable of handling common industry standard service requests, such as SOAP and REST. Also, evoBrix can change the various attributes of the service without impacting existing clients. The Oracle Fusion SOA infrastructure will allow the Option A Provider Services solution to avoid point-to-point communication between system components and will streamline the flow of all information across modules.

evoBrix will transmit Statement of Record (SOR) data needed to support business operational functions of the legacy MMIS via the Integration Hub. During the SCI phase, Team CNSI and DPHHS will create the specifications for each of the interfaces that will need to be implemented. To support Option A requirements, a custom specification will be created for those interactions for which no HIPAA transaction exists.

DPHHS will provide Interface Control Documents (ICDs) in the procurement library for the legacy system interfaces. Team CNSI will follow the technical processes documented in our Systems Engineering Management Plan (SEMP) to implement the integration.

Following are the salient features of the evoBrix platform that will help provide DPHHS achieve desired integration with their as-is and to-be DPHHS MMIS modules:

- Standardized HIPAA transaction support. The evoBrix solution provides support for standard HIPAA X12 transactions by leveraging the Edifecs translation engine.

- Microservices architecture enables plug-and-play features that will help integrate evoBrix with the SI's ESB.
- In-flight Transaction Translation. Standard transactions wherever applicable, and custom transactions where standard transactions support is not available.
- evoBrix Integrator. Provides auditing framework for logging all requests and responses, thereby meeting all auditing requirements.
- evoBrix's Integrator. Supports integration protocols as requested in the INT86 (Attachment F requirement).
- evoBrix Responsive Web Design. Provides all the capabilities to support web-based queries and allow for DDE.

Key Capabilities of the Technical Solution

Modularity

evoBrix's modularity capability includes:

- Security components and infrastructure that facilitate information exchange, data sharing, and data access in a distributed environment
- Alignment to technology and data standards
- Interoperability and accessibility for information access, ease of integration, and information exchange aligned to service-oriented principles
- Business agility driven by a flexible, extensible platform for rapid adoption of changes
- Performance and system monitoring of the modular components at business and technology levels

Interoperability

The key interoperability capabilities of the Option A solution are as follows:

- SOA/Standards-based integration approaches using protocols, including REST, SOAP, and COTS APIs.
- Support for standard content formats such as documents, XML, JSON, EDI for user, and machine-readable and -understandable content.
- EDI gateway support for standards-based information exchange for EDI transactions (e.g., HIPAA ANSI X12 standards), and support for secure FTP gateway.

Accessibility

Self-service Portal provides access to business information for user access and communication through web portals. Accessibility services are integrated with security services to ensure that only authorized users are provided with access to secured information. Accessibility layer services leverage the evoBrix UI responsive layout for creating an engaging user experience.

Security

evoBrix platform security framework will be responsible for ensuring secure access to information, information exchange, secure communication, protection of privacy, and data security. Key security capabilities of evoBrix security framework include:

- Protection of health information – Controlled access to data and secure communication. Adequate security controls for existing and emerging threats and vulnerabilities.

- Application Security – Authentication controls including single sign on, identity proofing, two-factor authentication, separation of web layer and application layer via secure deployment, and data security in transit via validation and encryption. Authorization controls including role-based access control (RBAC) up to data element level, user account audit, audit trail, and history.
- Data Security – Data at rest and in-transit encryption and SAN encryption.
- Infrastructure Security – Hardware separation by secured zone-based architecture. Multi-zone architecture to protect application from vulnerabilities. Optimized resource utilization and expandable infrastructure on demand.

Alignment to Industry Standards

Team CNSI continues to participate in MITA, HL7 standards, and other standards-related forums to promote and adopt standards. The evoBrix solution is aligned to industry standards, including the following data standards:

- HIPAA X12 standards for EDI transactions and code sets, such as ICD10
- MITA standards
- CMS' Seven Standards and Conditions

Figure 3.10.13-2 summarizes how the evoBrix solution will address the Option A specific requirements, which are presented in the "Requirement" column.

Requirement	evoBrix Capability	evoBrix Technology Component
3.10.13.1 Self-Service Member Eligibility Inquiry	Allow providers to: ■ enter query via the evoBrix User Interface screen ■ view query results	Self-service portal's DDE web forms, translation services converting request to a HIPAA 270 transaction. Self-service portal capability to consume a 271 response HIPAA transaction from the SI.
3.10.13.2 Self-Service Claim Status Inquiry	Allow providers to: ■ enter query via evoBrix User Interface screen ■ view query results	DDE inquiry from the user interface, translation services converting request to a HIPAA 276 transaction. Self-service portal capability to consume a 277 response HIPAA transaction from the SI.
3.10.13.3 Self-Service Warrant and Remittance Advice Inquiry	Allow providers to: ■ enter query via evoBrix User Interface screen ■ view query results	DDE inquiry from the user interface, translation services converting request to a custom web service transaction. Self-service portals capability to consume an 835 response HIPAA transaction from the SI.
3.10.13.4 Self-Service Claims Based Medical History	Allow providers to: ■ enter query via evoBrix User Interface screen ■ view query results	DDE inquiry from the user interface, translation services converting request to a 276 HIPAA transaction. Self-service portal capability to consume a 277 response HIPAA transaction from the SI.
3.10.13.5 View, Upload and Download HIPAA Compliant Healthcare Transactions	Allow providers to: ■ submit HIPAA batch transaction requests ■ perform Web service batch HIPAA transaction submission ■ have HIPAA data download capability	Self-service portal HTML file upload capability. Self-service portal web service batch file submissions. Self-service portal evoBrix standard data translation controls, such as like Excel, pdf, and csv download features
3.10.13.6 Self-Service Online Provider Appeal Request	Allow providers to: ■ request appeals ■ route the request to the appropriate user/unit ■ view status of appeals	DDE from the user interface request translated to a custom web service request. Self-service portal workflow capability leveraging configurability. Self-service portal web form to display status of appeals.

Requirement	evoBrix Capability	evoBrix Technology Component
3.10.13.7 Self-Service PCCM Member Inquiry	Allow PCCM providers to: ■ query PCCM members ■ download and view PCCM member registries	DDE inquiry from the user interface, translation services converting request to a custom web service transaction. Self-service portal web form capability to view PCCM member data.
3.10.13.8 Self-Service Online Claims Entry	Allow providers to: ■ submit claims via user interface	DDE using web forms, translation services converting to a custom web service transaction.

Figure 3.10.13-2. Addressing Option A Specific Requirements. Highlighting how evoBrix technology components will address Option A specific requirements.

Team CNSI's modular out-of-the-box evoBrix solution, with loosely coupled microservices architecture, standardized HIPAA transaction support, and SOA based integration support capabilities, meets all of the Option A self-service portal requirements.

The following requirements are part of the Option A Provider Services requirements, but are not aligned with any specific Requirement Section of Attachment F. In accordance with the Q&A responses, we are including them with our introduction to our Option A Provider Services responses. These requirements and their respective responses address training, the self-service portal, and operations and maintenance, all as they relate to the Option A Provider Services.

TRN16

The Contractor's solution shall provide web-based video instruction.

Team CNSI will provide an **eLearning module** that provides learners with an overview and instruction on performing the functions offered through the provider self-service portal. The course material will be pre-recorded and available 24 hours a day, 7 days a week as a download from the provider self-service portal. This flexibility will allow learners to choose when they want to take the training and allow them to take it at their own pace.

PSER23

The Contractor's solution shall provide an online self-service Frequently Asked Questions (FAQ) tool that is easily navigable and searchable. The FAQ shall be updated quarterly or as directed by the State.

Team CNSI's online Frequently Asked Questions (FAQ) page provides instant help to State staff and providers, reducing customer care support time. The solution provides easy-to-navigate and searchable pages, articles, sections, and categories. FAQ content will be updated quarterly or as directed by DPHHS.

PSER24

The Contractor's solution shall allow users to view, download and/or print current and historical provider information (e.g., manuals, instructions, bulletins, program descriptions, eligibility criteria and forms).

The evoBrix PMIS solution allows authorized users to view, download, and/or print both current and historical enrollment information through the self-service portal.

PSER27

The Contractor's solution shall provide access for users to view current and historical fee schedules.

The evoBrix PMIS solution maintains a history of fee schedules, and allows authorized users to view current and historical fee information.

OMC22

The Contractor shall provide 500 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 500 system enhancement pool hours are included in the offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.

The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

Team CNSI will accommodate the request to provide 500 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 500 system enhancement pool hours are included in Team CNSI's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.

Team CNSI agrees that the unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

OMC23

The Contractor will provide 100 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 100 system enhancement pool hours are included in the Offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G Pricing Schedule, Schedule D-Enhancement Pool Hours. The cost of the

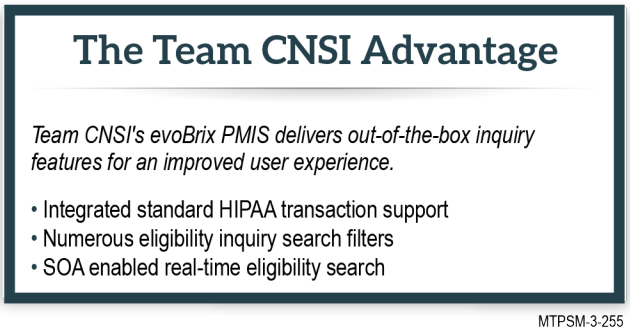
contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours.

Team CNSI will accommodate the request to provide 100 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 100 system enhancement pool hours are included in the Team CNSI's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

Team CNSI agrees that the unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G Pricing Schedule, Schedule D-Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours.

3.10.13.1 Self-Service Member Eligibility Inquiry

This section outlines the requirements for Self-Service Member Eligibility Inquiry. The Offeror's proposed Option A solutions and services shall include real time verification of eligibility through the Self-Service Portal and provide eligibility information including benefit plan enrollment, care management enrollment, waiver program information, program limits, service limits, and TPL information on the self-service portal to providers and other users authorized by the State. The Offeror must describe their approach to meet each of the self-service eligibility requirements defined in Attachment F, Requirements Matrix.



The evoBrix Option A proposed solution has a robust out-of-the-box member real-time eligibility inquiry and response capability. The member eligibility inquiry functionality has integrated HIPAA transaction support, as highlighted in Section 3.10.13 of the proposal. Eligibility inquiry in the self-service portal provides multiple search options, the details of which are highlighted in response to the PSER04 requirement. Through the self-service portal, a member's eligibility request/response can display data elements from various eligibility response segments, as required of PSER38; and authorized users of the system can submit, view and download eligibility transaction data. Please refer to the specific requirements (PSER04 and PSER38) responses below for system capability details.

PSER04

The Contractor's solution shall provide an online self-service tool for authorized users to perform real-time member eligibility inquiries. Eligibility inquiry responses will include at a minimum, eligibility dates, eligibility for one or more benefit plans, care management enrollment information, waiver program information, program limits, TPL information, and other member information necessary for the provider to determine if the member is eligible for services.

The evoBrix Self-service Portal allows authorized State staff and Medicaid providers to perform member eligibility inquiries for Medicaid beneficiaries. The Self-service Portal provides a Direct Data Entry (DDE) inquiry screen for authorized providers to submit eligibility inquiries and receive real-time results. The required response data elements identified in the PSER04 requirement are standard 271 transaction elements. These data elements have been mapped and will be appropriately displayed in the self-service portal of our Option A solution.

Authorized providers will be able to access the evoBrix Provider Portal for the inquiry based on security access levels assigned to each user profile. Figure 3.10.13-3 exhibits the login page for the provider to log in to the system with the "Eligibility Inquiry" profile.

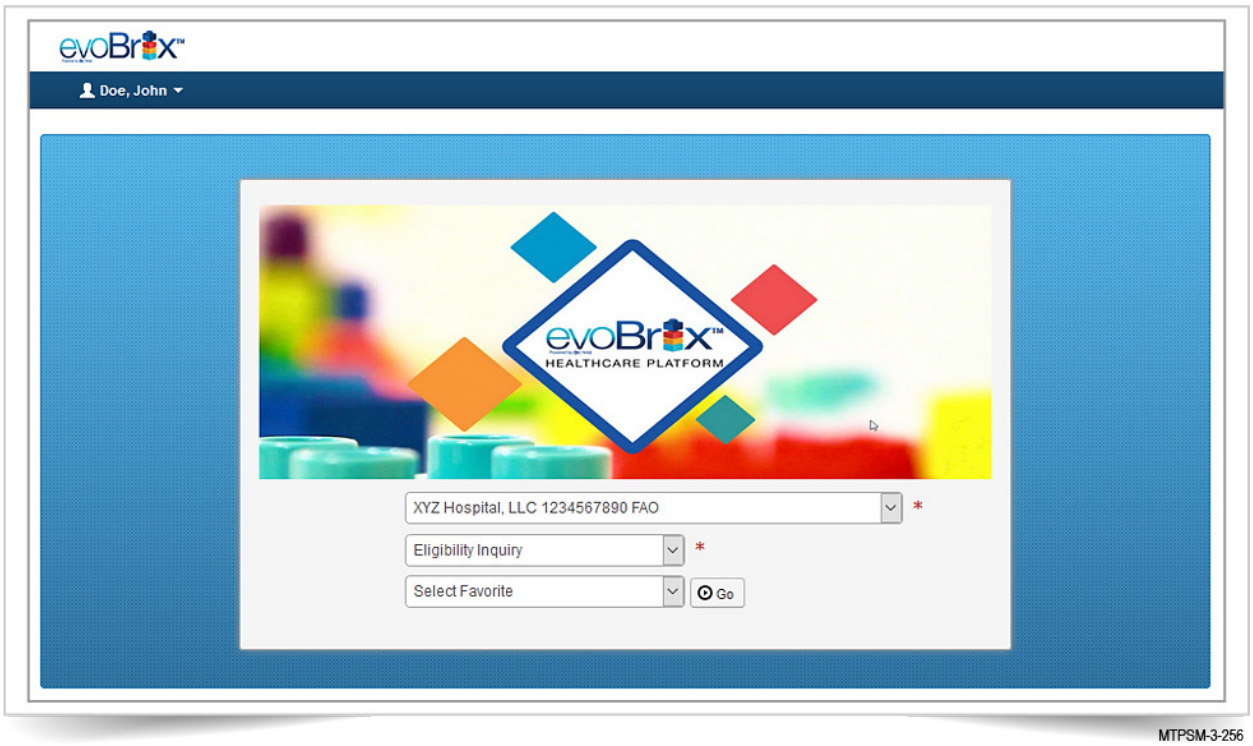


Figure 3.10.13-3. evoBrix Login Screen. Displays the login screen for authorized access.

Once logged in to the system, providers will be able to conduct eligibility inquiry through the Eligibility Inquiry functionality present under the Member sub-system in evoBrix, as shown in Figure 3.10.13-4.

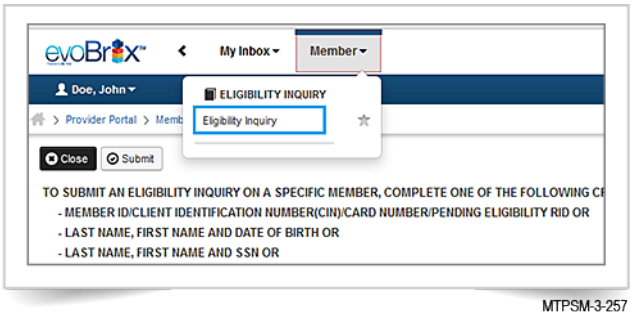


Figure 3.10.13-4. Eligibility Inquiry Location. Eligibility inquiry URLs location in the member sub-system.

Providers will be able to search for a member's eligibility through the various search criteria. Figure 3.10.13-5 displays the multiple search parameters present for the eligibility inquiry.

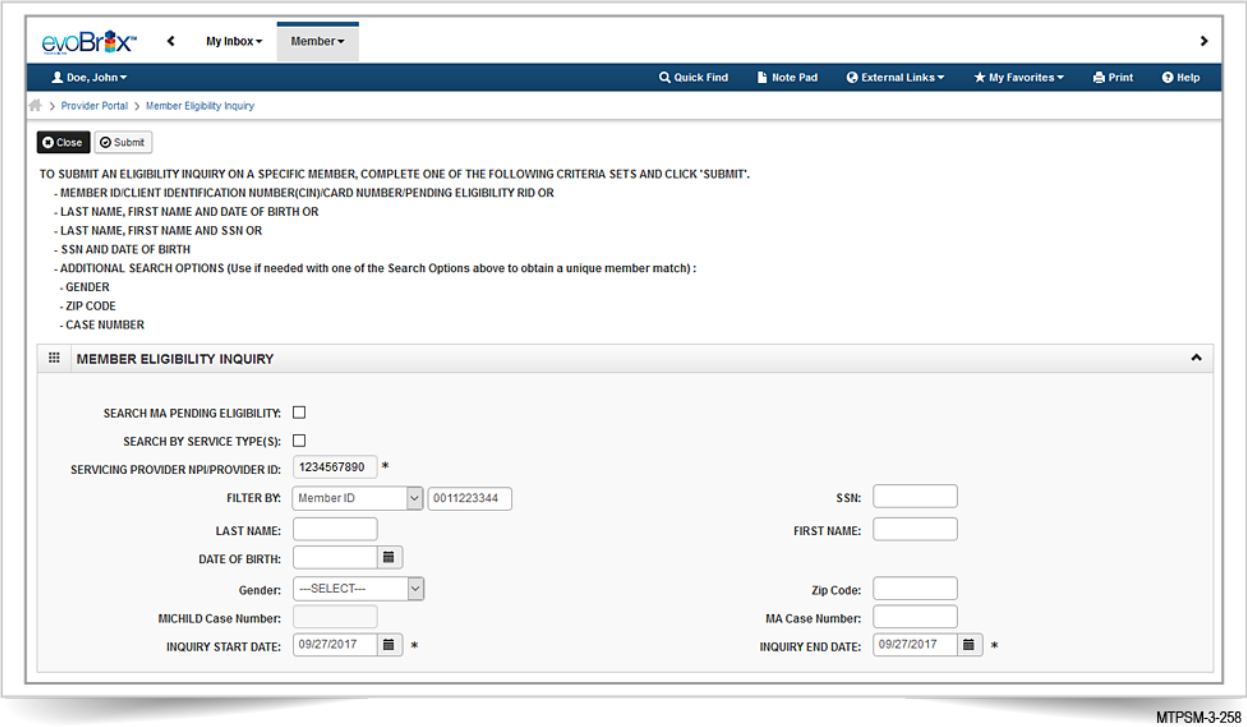


Figure 3.10.13-5. Eligibility Inquiry Search Parameters. Screenshot highlighting the eligibility inquiry search capability. Search elements are configurable.

Providers can submit an eligibility inquiry based on a combination of parameters for either a single date or for a range of dates. The time period or the duration of the search criteria for the eligibility inquiry is configurable in the system.

evoBrix PMIS also provides additional search options, along with the basic parameters, for distinct identification of a member.

evoBrix PMIS provides a real-time eligibility response based on the eligibility inquiry criteria submitted by the provider. Figure 3.10.13-6 shows the eligibility and enrollment data reported in the response.

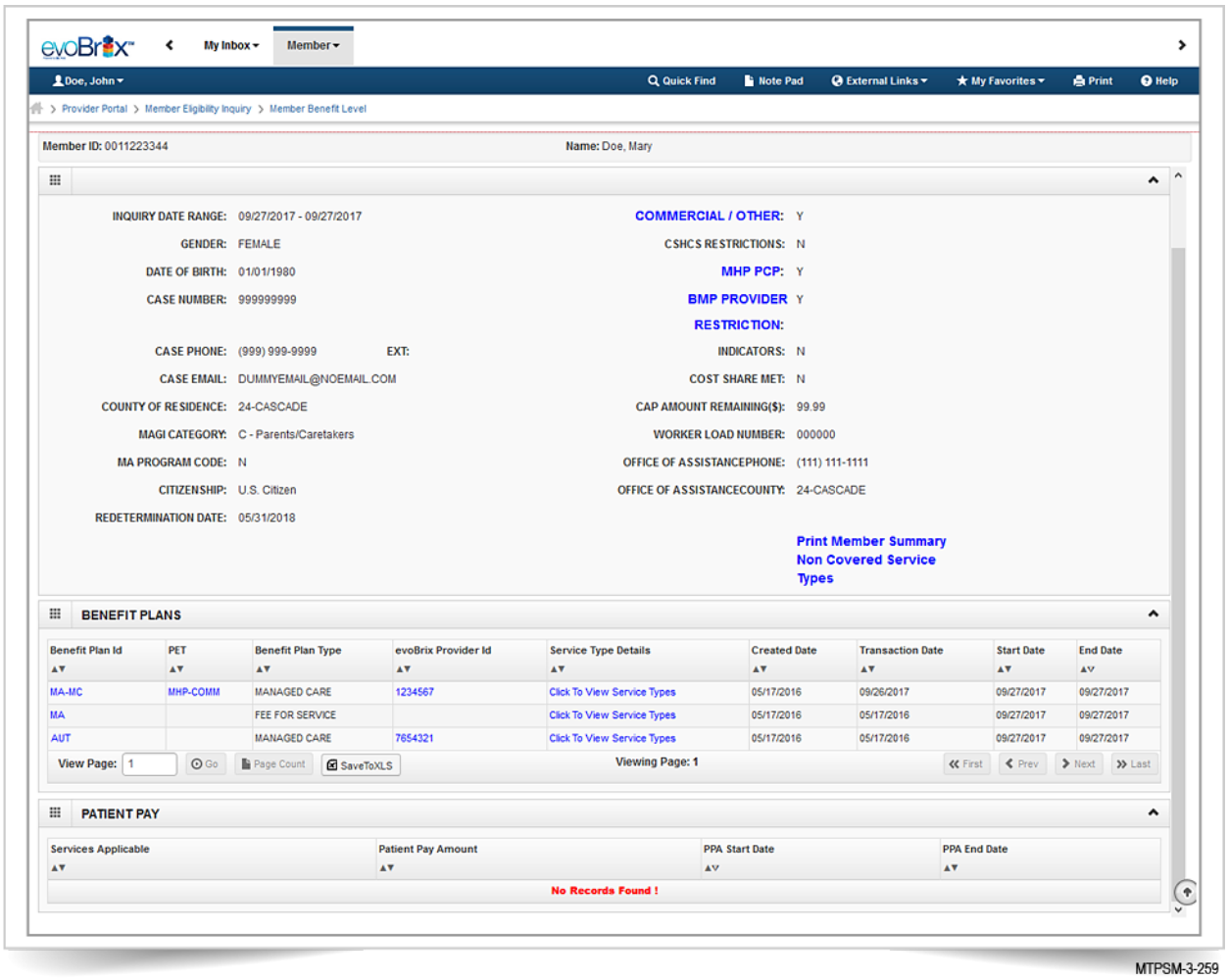


Figure 3.10.13-6. Eligibility Response. The eligibility response screen presents easily configurable elements to capture the needed member data.

The response for the eligibility inquiry is categorized in three segments. The first segment contains the basic demographic and other member specific information. The information reported under this segment is configurable.

The second segment – the Benefit Plan (BP) segment – reports the applicable benefit plan information for the member. This section entails the Benefit Plan ID, along with the applicable dates and the associated provider. A detailed benefit plan description and provider ID details are also provided to the providers under the Benefit Plan ID and the provider ID hyperlinks, respectively. Figure 3.10.13-7 shows the BP description and Figure 3.10.13-8 shows the provider summary information.

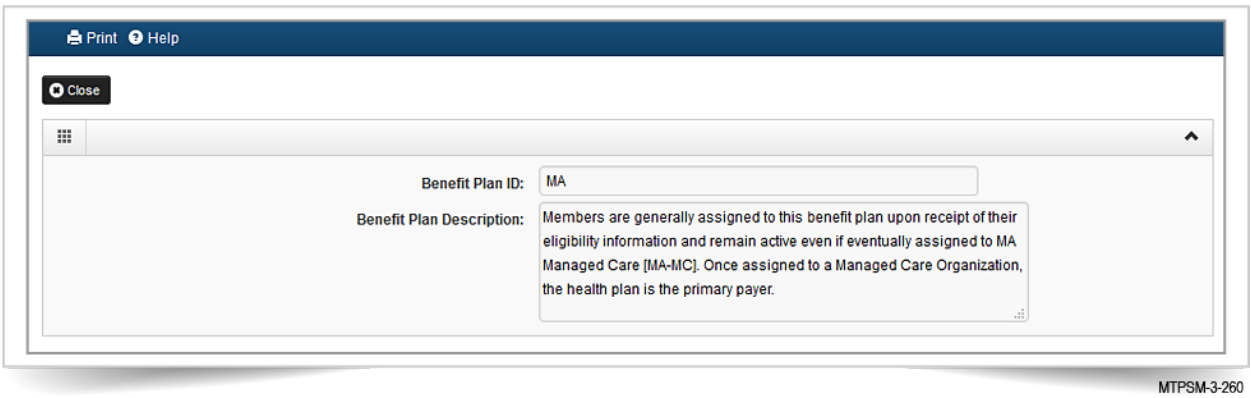


Figure 3.10.13-7.Benefit Plan Data. The Benefit Plan screen provides specific data regarding that specific Benefit Plan.

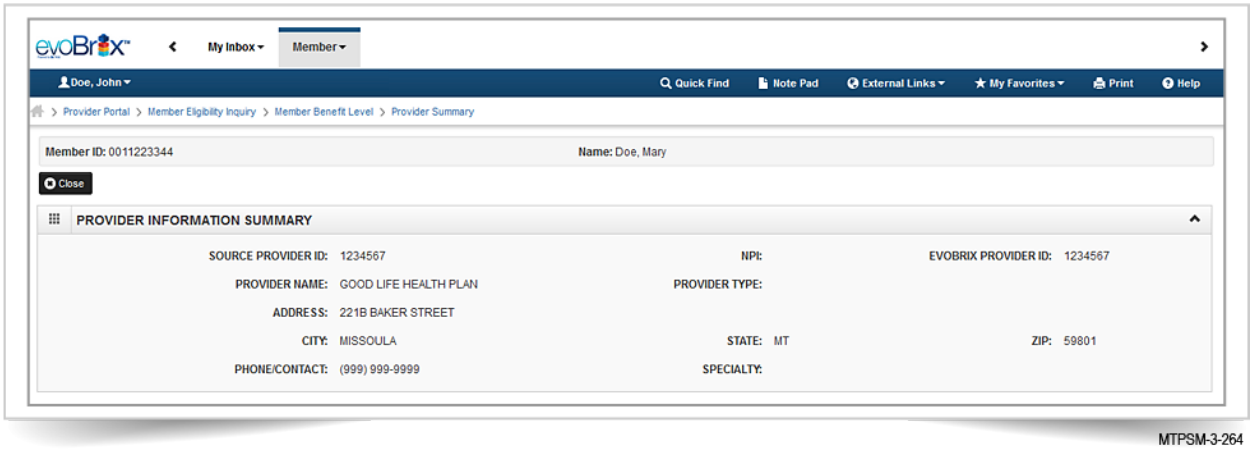


Figure 3.10.13-8. Provider Data. The Provider Information Summary screen presents specific data regarding a particular provider.

Providers also can view the service type limits information by clicking the hyperlink under the Service Type Details in the BP segment. Figure 3.10.13-9 displays the service type details shown to providers.

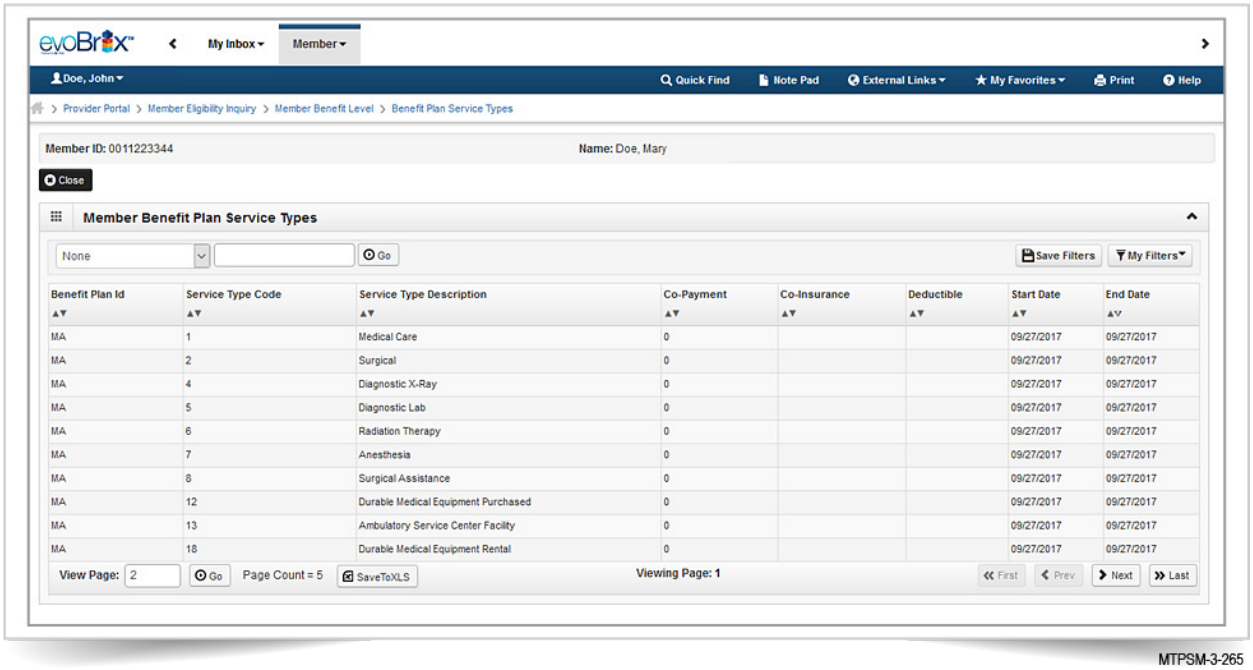


Figure 3.10.13-9. Service Type Data. The Member Benefit Plan Service Types page provides significant detail regarding the service types.

The third segment on the eligibility inquiry response is for reporting the Patient Pay Amount, as applicable for the member.

Waiver information is abstracted from the eligibility response and displayed. Figure 3.10.13-10 highlights the data elements associated with waivers.

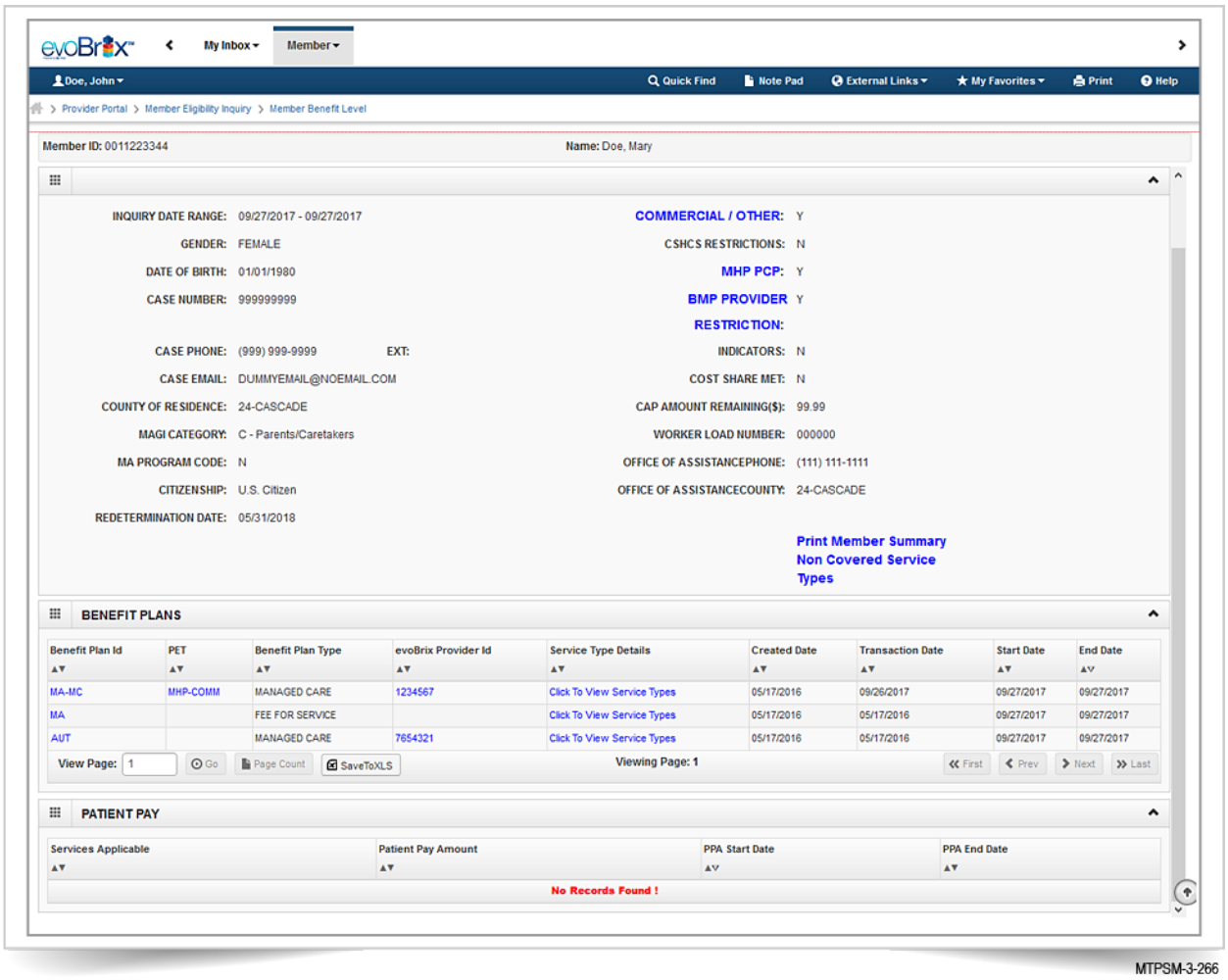


Figure 3.10.13-10. Waiver Information. Users can easily search on data elements associated with member benefit level waivers.

Third-Party Liability (TPL) information is reported as “Y” when the member has commercial insurance present in the system. The details of the TPL information are provided once the provider clicks the hyperlink for the “Commercial/Other” displayed in Figure 3.10.13-11.

©2017 CNSI | Option A-16

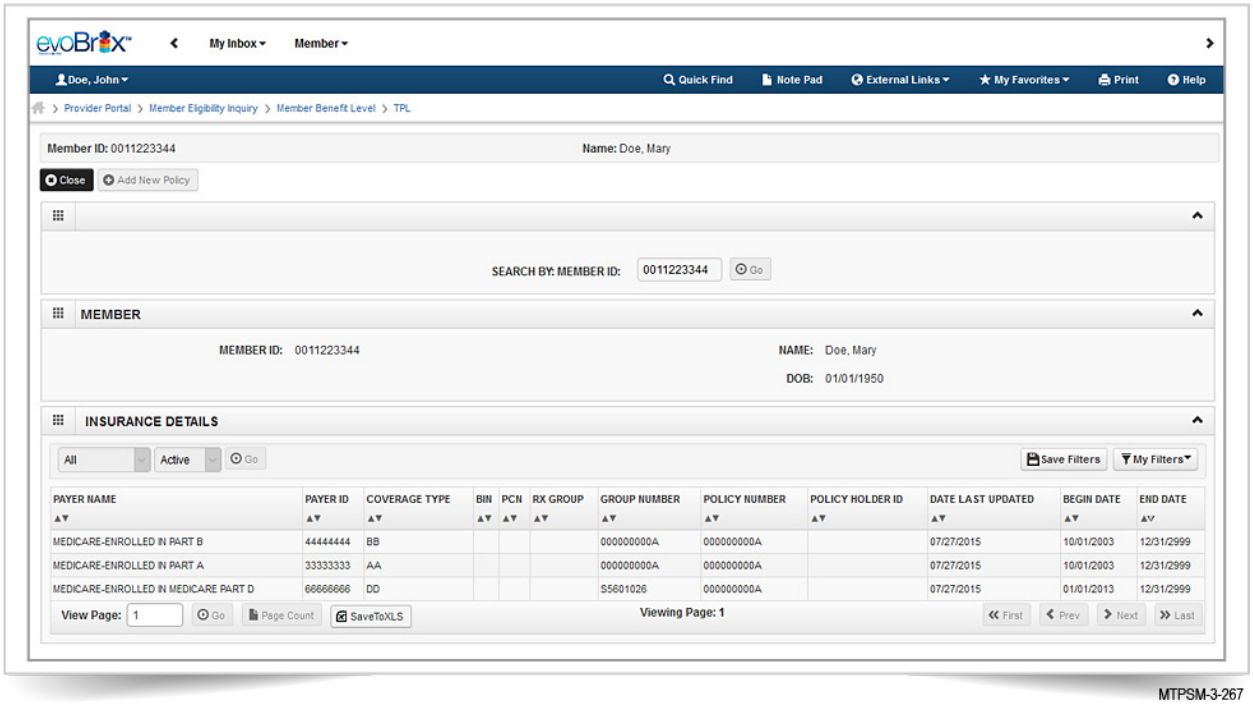


Figure 3.10.13-11. TPL Data. By clicking the TPL link, authorized users have immediate access to the TPL details.

PSER38

The Contractor's solution shall allow an external user to print member eligibility responses or download in PDF format.

The evoBrix Option A solution has enhanced capability for the authorized users to view the eligibility response and to print or download the eligibility response in .pdf format. The field “Print Member Summary” displayed in Figure 3.10.13-12, enables the user to print the eligibility response reported for a member.

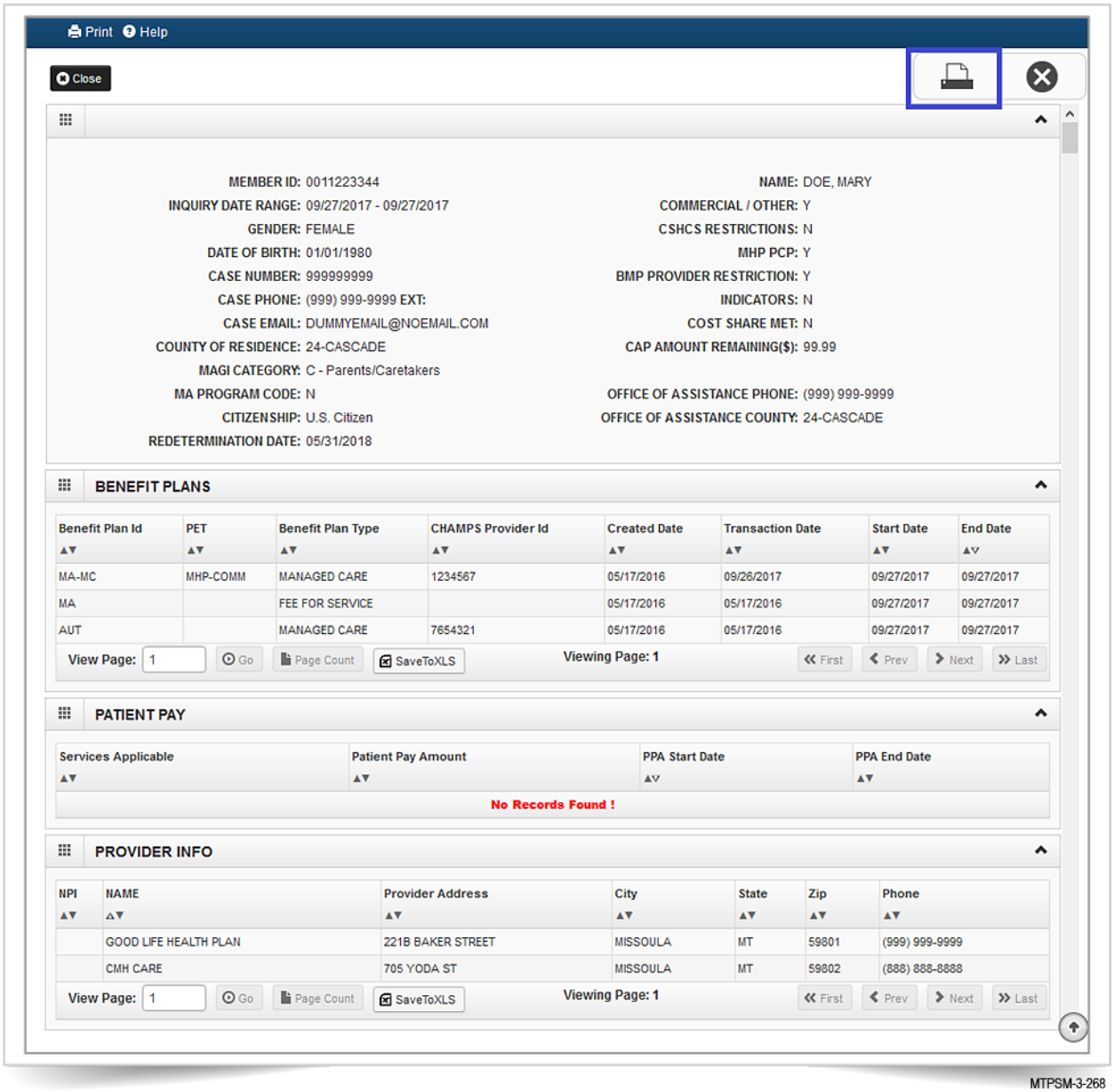


Figure 3.10.13-12. Print Capability. By clicking the print icon, authorized users can print the eligibility response summary.

3.10.13.2 Self-Service Claim Status Inquiry

This section outlines the requirements for Self-Service Claim Status Inquiry. The Offeror's proposed Option A solutions and services shall include real time claims status inquiry to allow providers to check the status of their claims. The Offeror must describe their approach to meet each of the self-service claim status inquiry requirements defined in Attachment F, Requirements Matrix.

The evoBrix Self-Service Option A solution offers robust support for real-time claims status inquiries. The claim inquiry functionality allows providers to securely query the status of their claims in near real-time using integrated HIPAA 276/277 transactions.

Authorized providers can enter claim inquiry parameters into a configurable user interface. The request is translated into a real-time HIPAA 276 transaction in the evoBrix Translator and then re-directed via evoBrix Integrator to the SI. The Integration Hub communicates with the MMIS or other appropriate system and returns a HIPAA 277 response via the same channels of the request. The response will be parsed and displayed to the provider via configurable user interface (UI) components.

The Team CNSI Advantage

Team CNSI's evoBrix PMIS delivers easy to use features for inquiries regarding a claim's status.

- Easy to use real-time Claim Status Inquiry option using HIPAA 276/277 transactions.
- Option to save the results to Excel or Print to PDF

MTPSM-3-278

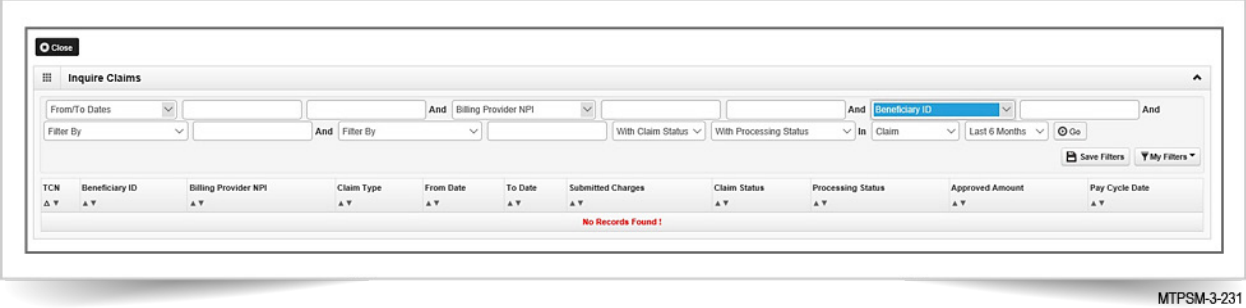
Please refer to Section 3.10.13 of the proposal for details on the overall solution approach.

PSER06

The Contractor's solution shall provide an online self-service tool for providers to view claim status.

The evoBrix Claim Status Inquiry screen gathers search criteria information from authorized users. The evoBrix Data Translator converts the gathered inquiry data into a HIPAA 276 transaction.

After receiving the 276 transaction, the MPATH Integration Hub returns the HIPAA 277 response transaction to evoBrix PMIS. The evoBrix Data Translator will translate the information from the 277 transaction to display it on the Claim Status Inquiry screen, as shown in Figure 3.10.13-13.



MTPSM-3-231

Figure 3.10.13-13. Claim Inquiries. Claim search criteria values are sent to the Integration Hub as a HIPAA 276 transaction.

The filter criteria values and the result set fields are configurable.

Upon receiving a response from MPATH Integration Hub in 277 transaction format, the evoBrix Translator converts the data to display the search results with information about the claim's status, as shown in Figure 3.10.13-14.

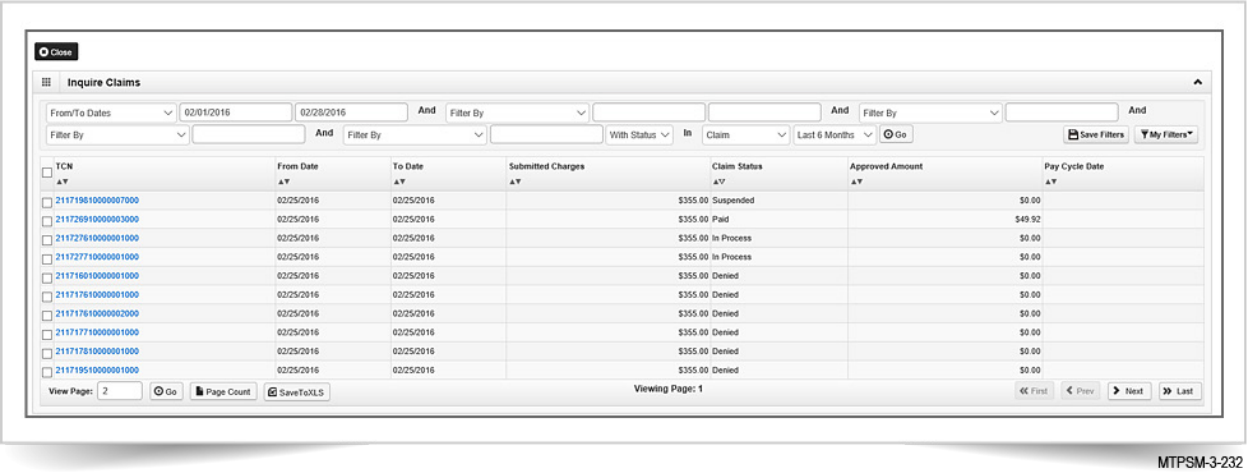


Figure 3.10.13-14. Inquire Claims Results. The result set displaying the claim status for the requested claims per the search criteria entered in the Inquire Claims screen.

PSER43

The Contractor's solution shall allow authenticated users to download or print a claim status report in Excel and PDF.

The evoBrix Claim Inquiry screen allows authorized users to save the result set in Excel format. The result set can also be printed to PDF with a pdf plug-in.

The "SaveToXLS" HTML button located at the bottom of the inquiry screen allows users to save the search results into an Excel file, as shown in Figure 3.10.13-14. Upon clicking the SaveToXLS button, a dialog box opens to provide the status of the download and the save process, as shown in Figure 3.10.13-15.

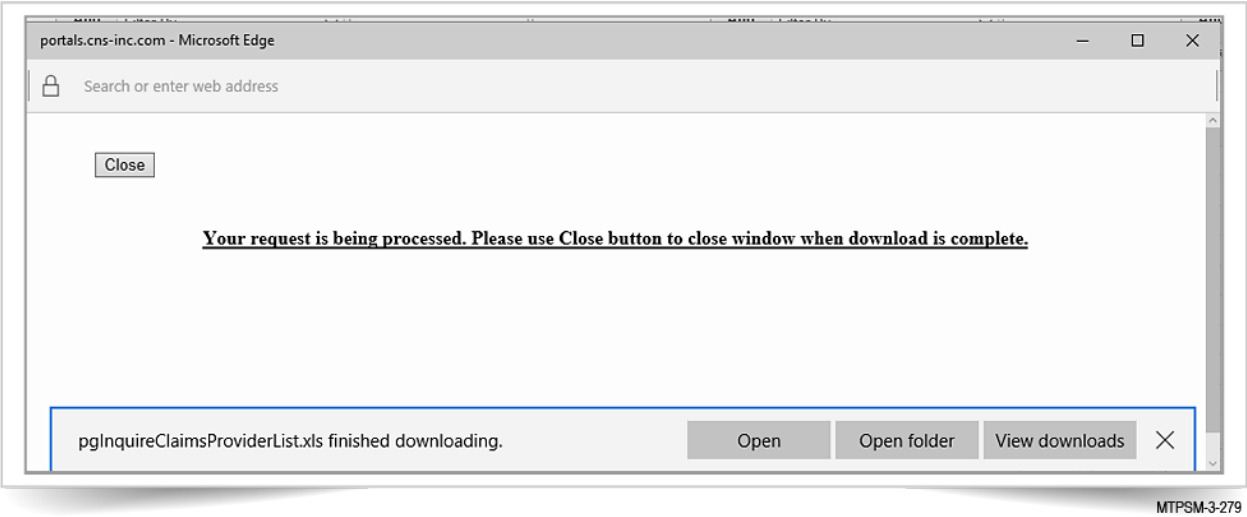


Figure 3.10.13-15. Save To Excel Dialog Box. The screen displaying "Save To Excel" dialog box functionality available after clicking the SaveToXLS button.

Once the Excel document is opened, then the user can leverage the Excel functionality to save the document to any other format of choice, including PDF ("Print to PDF"), as shown in Figure 3.10.13-16.

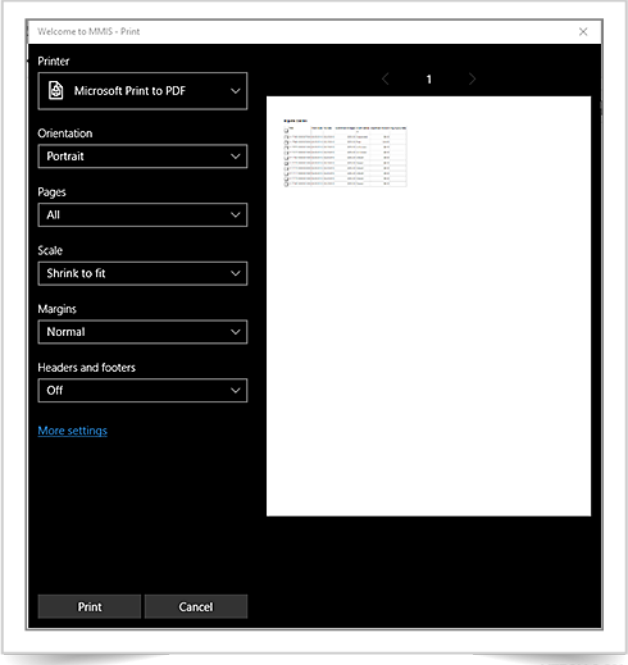


Figure 3.10.13-16. Print to PDF. Using the Print to PDF option while printing, the result set can be saved as PDF.

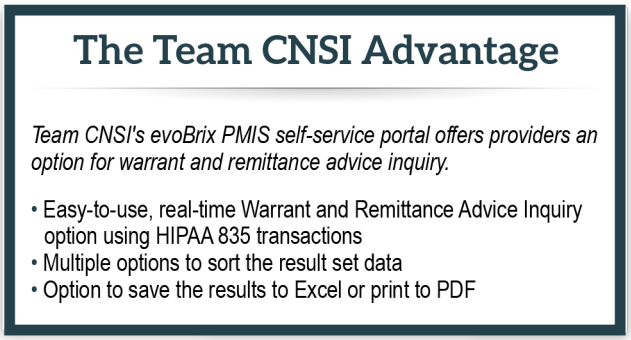
3.10.13.3 Self-Service Warrant and Remittance Advice Inquiry

This section outlines the requirements for self-service warrant and remittance advice access. The Offeror's proposed Option A solutions and services shall provide access to remittance advice and warrant information through self-service portal for the provider and other users authorized by the State. The Offeror must describe their approach to meet each of the requirements for self-service warrant and remittance advice access defined in Attachment F, Requirements Matrix.

Team CNSI's evoBrix Option A solution for self-service warrant and remittance advice inquiry allows providers to securely query the warrant and remittance advice information in real time.

Authorized providers can enter warrant and remittance inquiry parameters into a configurable user interface. The request is translated into a real-time custom transaction in the evoBrix Translator and then routed by evoBrix Integrator to the MPATH Integration Hub. The Integration Hub transmits the data to the MMIS, and returns an 835 HIPAA response via the same channels of the request. The response will be parsed and displayed to the provider via configurable user interface components.

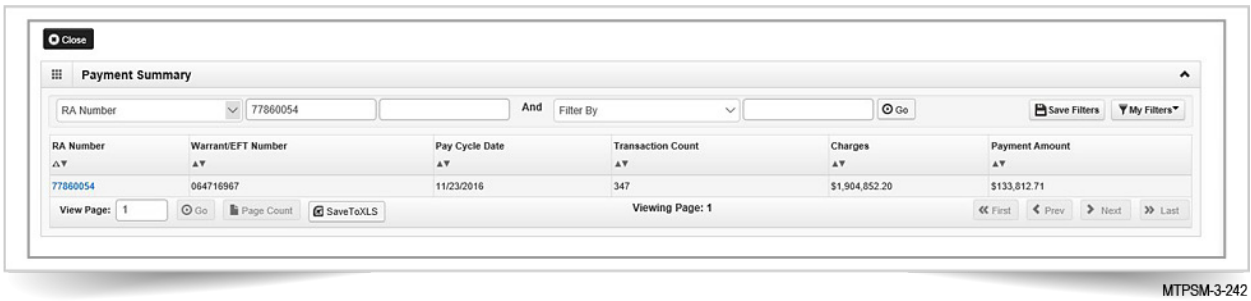
Please refer to Section 3.10.13 of our proposal for details on the overall solution approach.



PSER02

The Contractor's solution shall include an online self-service tool allowing authenticated users to view current and all previous warrants.

The evoBrix Payment Summary screen allows authorized users to enter search criteria to submit a warrant and remittance advice inquiry. The evoBrix Data Translator converts the data into a custom web service transaction. The evoBrix Integrator forwards the request to the MPATH Integration Hub for processing by the claims system. The Hub returns responses using the HIPAA 835 transaction for evoBrix to consume. The evoBrix Data Translator translates the information to an 835 transaction to display it on the Payment Summary Inquiry screen, as shown in Figure 3.10.13-17.



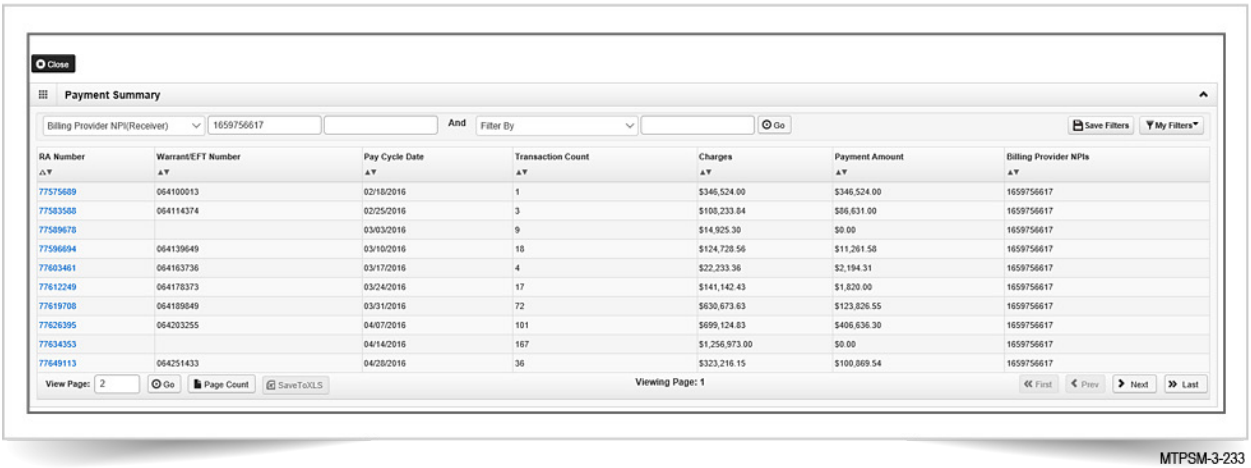
MTPSM-3-242

Figure 3.10.13-17. Payment Summary. The evoBrix screen provides multiple search options to view the payment summary for a warrant and remittance advice inquiry.

PSER07

The Contractor's solution shall provide an online self-service tool that allows authenticated users to access and view current and previous remittance advice that can be sorted by various parameters (EFT, date, NPI, etc.).

The evoBrix Payment Summary screen allows authorized users to access and view current and previous remittance advice that can be sorted by such fields as RA Number, Warrant/EFT Number, Pay Cycle Date, Payment Amount, and NPI. Figure 3.10.13-18 shows the Payment Summary information for a billing provider.



MTPSM-3-233

Figure 3.10.13-18. Payment Summary Information. The Remittance Advice information is displayed based on the search criteria entered. Information can be sorted by any field on the screen.

PSER40

The Contractor's solution shall allow authenticated users to download warrants and remittance advice in multiple formats (e.g., Excel or PDF) as directed by the State.

The evoBrix Payment Summary screen allows authorized users to save the result set data in Excel format. The result set can also be printed to PDF with a pdf plug-in.

The "SaveToXLS" button on the Payment Summary screen, as shown in the Figure 3.10.13-18, allows users to save the search results in an Excel file. Figure 3.10.13-19 shows a dialog window that opens after the SaveToXLS button has been selected.

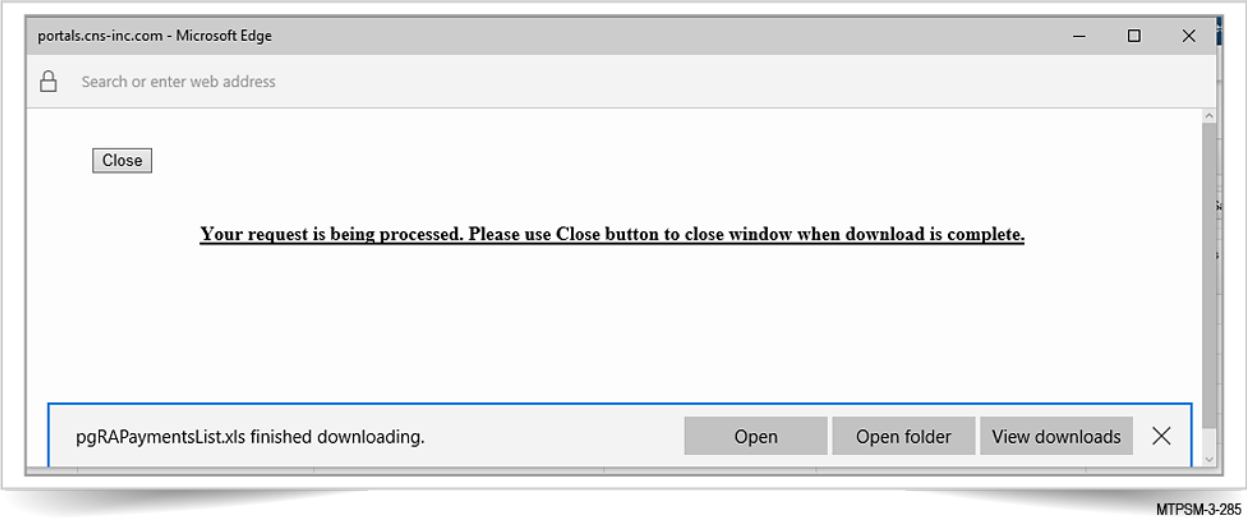
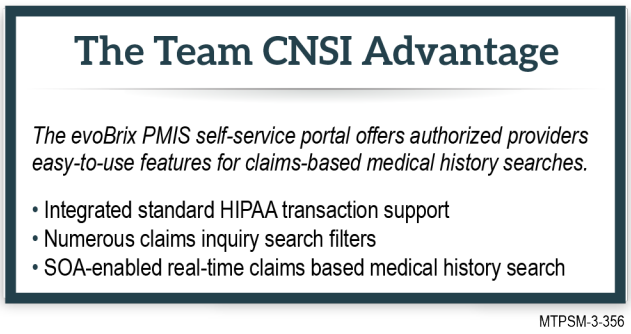


Figure 3.10.13-19. Save To Excel. This screen displays after the SaveToXLS button has been clicked to show the user the status of the download and the option to open the newly created Excel file.

Once the file is opened in Excel, the user can print the file in PDF format using the same approach as shown in Figure 3.10.13-16 in the earlier response to requirement PSER43, thereby allowing the result set to be saved as a PDF document.

3.10.13.4 Self-Service Claims Based Medical History

This section outlines the requirements for Claims Based Medical History. The Offeror's proposed Option A solutions and services shall include member medical history access on the Self-Service Portal to allow providers with the authorized roles to access a member's medical histories interactively. The Offeror must describe their approach to meet each of the claims based medical history requirements defined in Attachment F, Requirements Matrix.



The evoBrix PMIS self-service claims-based medical history option will leverage the solution's claims status inquiry capability, as described in Section 3.10.13.2 of our proposal. The claims status inquiry screen will be configured to allow searches based on claim attributes, such as procedure codes, revenue codes, and associated diagnosis codes, thereby providing insights into a member's medical history. A chronological member claims list, which includes a history of dates of service, procedure codes, revenue codes, and diagnosis codes, will be generated as an output to the Claims Based Medical History inquiry.

PSER21

The Contractor's solution shall allow authorized users to search and view Claims Based Medical History.

Team CNSI's evoBrix PMIS collects claims-based medical history data based on information from providers that have submitted bills for member's care (e.g., the different doctors, hospitals, laboratories, imaging centers, pharmacies). The claims data has information about the procedure codes, revenue codes, and associated diagnosis codes. This data can help providers determine what medical care has been provided.

The evoBrix Claims Inquire screen allows authorized providers to gather specific data based on the search criteria they enter. Providers can specify the member ID, with additional parameters such as date span, to inquire about the claims-based medical history. Providers will only be able to search the claims data submitted by them. evoBrix PMIS can be configured to accommodate additional search criteria.

The evoBrix Data Translator converts the search criteria data into a custom web service request. The request is sent to the MPATH Integration Hub using evoBrix Integrator. After receiving the request, the Hub returns a response to evoBrix PMIS using a custom web service response. The evoBrix Data Translator translates the information in the response and displays it on the Inquire Claims screen, which, based on the search parameters, could include the claims-based medical history. Please refer to the narrative response provided in Section 3.10.13 of our proposal for additional details on the evoBrix Translator and evoBrix Integrator solution components.

Figure 3.10.13-20 show a sample Inquire Claims screen depicting claims-based medical history.

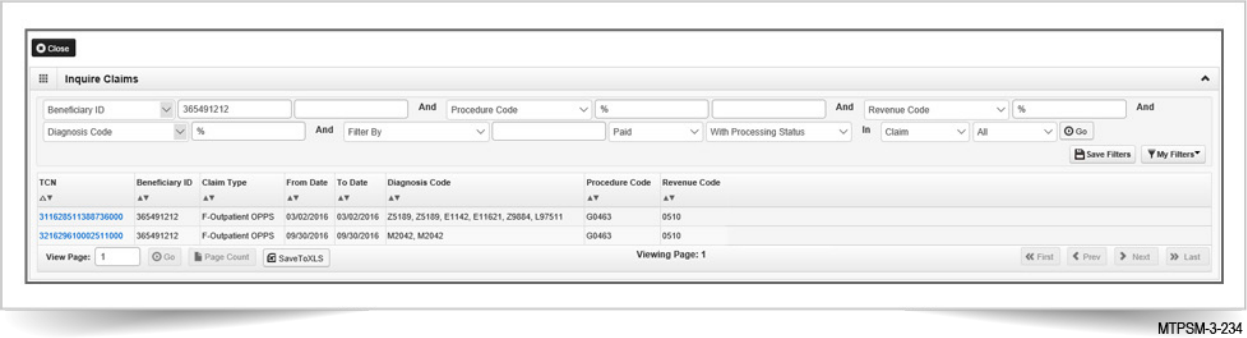


Figure 3.10.13-20. Inquire Claims Screen. evoBrix PMIS screen displays a member's claims-based medical history.

3.10.13.5 View, Upload and Download HIPAA Compliant Healthcare Transactions

This section outlines the requirements to View, Upload and Download HIPAA Compliant Healthcare Transactions. The Offeror's proposed Option A solutions and services shall allow authorized users to view, upload and download HIPAA compliant healthcare transactions (e.g., 270/271batch eligibility status inquiry and response, 837 batch claims submission, and 276/277 Claim Status request and response) on the Self-Service Portal. The Offeror must describe their approach to meet each of the requirements to view, upload and download HIPAA compliant healthcare transaction requirements defined in Attachment F, Requirements Matrix.

The evoBrix Option A proposed solution provides a streamlined upload process for the inbound HIPAA transactions and download process for the outbound transactions via the provider portal. Team CNSI will work with DPHHS to define the metadata that will be configured to retrieve the responses/ acknowledgements.

The Team CNSI Advantage

evoBrix PMIS is fully HIPAA-compliant for all required healthcare transactions, and provides users with the options to view, upload, and download these transactions.

- EDI framework that is easily integrated with state-specific gateways, based on years of industry experience
- Easy-to-use file upload and download functionality for HIPAA inbound and outbound transactions

MTPSM-3-332

Authorized users who have been established as valid trading partners by the DPHHS are able upload the following HIPAA batch transactions:

- 270 Eligibility inquiry
- 837 Claims submission
- 276 Claims status inquiry

In real time, the submitted batch files are routed to the appropriate drop-box location pre-configured in the evoBrix Integrator. The MPATH Integration Hub's process monitoring the drop-box location sends acknowledgement citing successful receipt of the batch files back to the users.

The submitted files are picked up from the drop-box location by a recurring or scheduled back-end job in the DPHHS environment for processing by the appropriate MMIS vendor system.

Once processed by the MMIS, the files are available in the drop-box location to be downloaded by authorized users via the evoBrix user interface in the following HIPAA-compliant formats:

- 271 Eligibility Response
- 277 Claims Status Response

Please refer to the narrative response in Section 3.10.13 of our proposal for additional details on the high-level solution approach.

PSER39

The Contractor's solution shall allow authorized user to view, upload and download HIPAA compliant healthcare transactions (e.g., 270/271batch eligibility status inquiry and response, 837 batch claims submission, and 276/277 Claim Status request and response) on the Self-Service Portal.

The evoBrix PMIS solution provides authorized users easy-to-use functionality for uploading, downloading, and viewing HIPAA-compliant files through the Self-Service Portal.

File Upload

The file upload option allows authorized providers the ability to upload 837 - Batch Claim Submission files, 270 - Eligibility Status Inquiry files, and 276 - Claim Status Request files in X12 5010 format using the Self-Service Portal.

The web portal screen interface allows authorized users to select a file to upload using the standard naming convention. The file naming rules are listed on the screen for easy reference.

Figure 3.10.13-21 displays the File Upload functionality offered in evoBrix as a claim intake option.



Figure 3.10.13-21. Upload File. evoBrix offers easy-to-use screens for authorized providers to upload X12 5010 files.

The uploaded file is then sent to an appropriate drop-box location using evoBrix Integrator.

File Download and View

The evoBrix solution provides an option for authorized providers to retrieve and download various HIPAA transaction files. Using the MPATH Integration Hub and evoBrix Integrator, the files are made available for the providers to download and view. Figure 3.10.13-21 displays the File Download functionality offered in evoBrix.

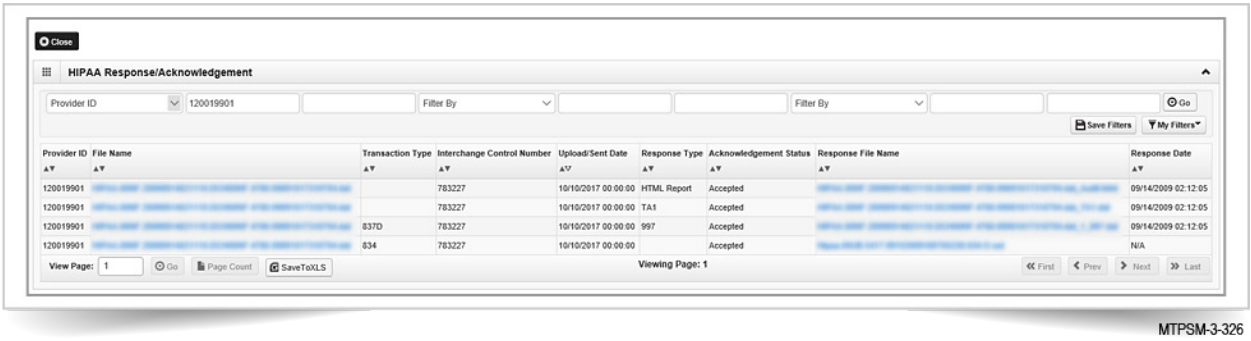


Figure 3.10.13-2. Downloading Files. evoBrix's HIPAA Response/Acknowledgement screen allows authorized providers to download X12 5010 files by clicking the hyperlinks for the request file name and response file name.

3.10.13.6 Self-Service Online Provider Appeal Request

This section outlines the requirements for Online Provider Appeal Requests. The Offeror's proposed Option A solutions and services shall provide the functionality for providers to request appeals. Automated workflow integration will route appeals to the appropriate work unit or user. The Offeror must describe their approach to meet each of the online provider appeal request requirements defined in Attachment F, Requirements Matrix.

The evoBrix proposed solution for Option A has a self-service module that allows providers to request an appeal and to check its status. The online appeal requests will be routed to the appropriate business unit in DPHHS.

Team CNSI understands appeals can be characterized by different appeal types. For example, appeals could relate to an amount on paid claims, provider re-enrollment, or re-certification. Different business units within DPHHS may be receiving different kinds of appeals and providing resolution. Team CNSI will work with DPHHS stakeholders to identify appeal types, data elements to be collected for an appeal type, and where the appeal needs to be sent. evoBrix will be configured and customized to address the unique appeal request requirement. Appeal requests will be submitted as a custom real-time web service request to the MPATH Integration Hub.

Please refer to Section 3.10.13 of our proposal, which describes our Option A solution, highlighting the automated web service integration with DPHHS agencies using the evoBrix Integrator.

PSER03

The Contractor's solution shall support on-line self-service tool for all providers to request an appeal.

The evoBrix self-service capability for appeals is highlighted in Figure 3.10.13-22. This self-service capability allows providers to request different types of appeals. Appeal requests are routed to the appropriate DPHHS agency based on the Appeal Type. The self-service portal also captures notes pertaining to the request, assigns a case number to the appeal, and captures the date the appeal was initiated. Additional data elements can be configured and/or customized based on DPHHS' specific needs. Figure 3.10.13-22 shows a sample Appeal Request screen.

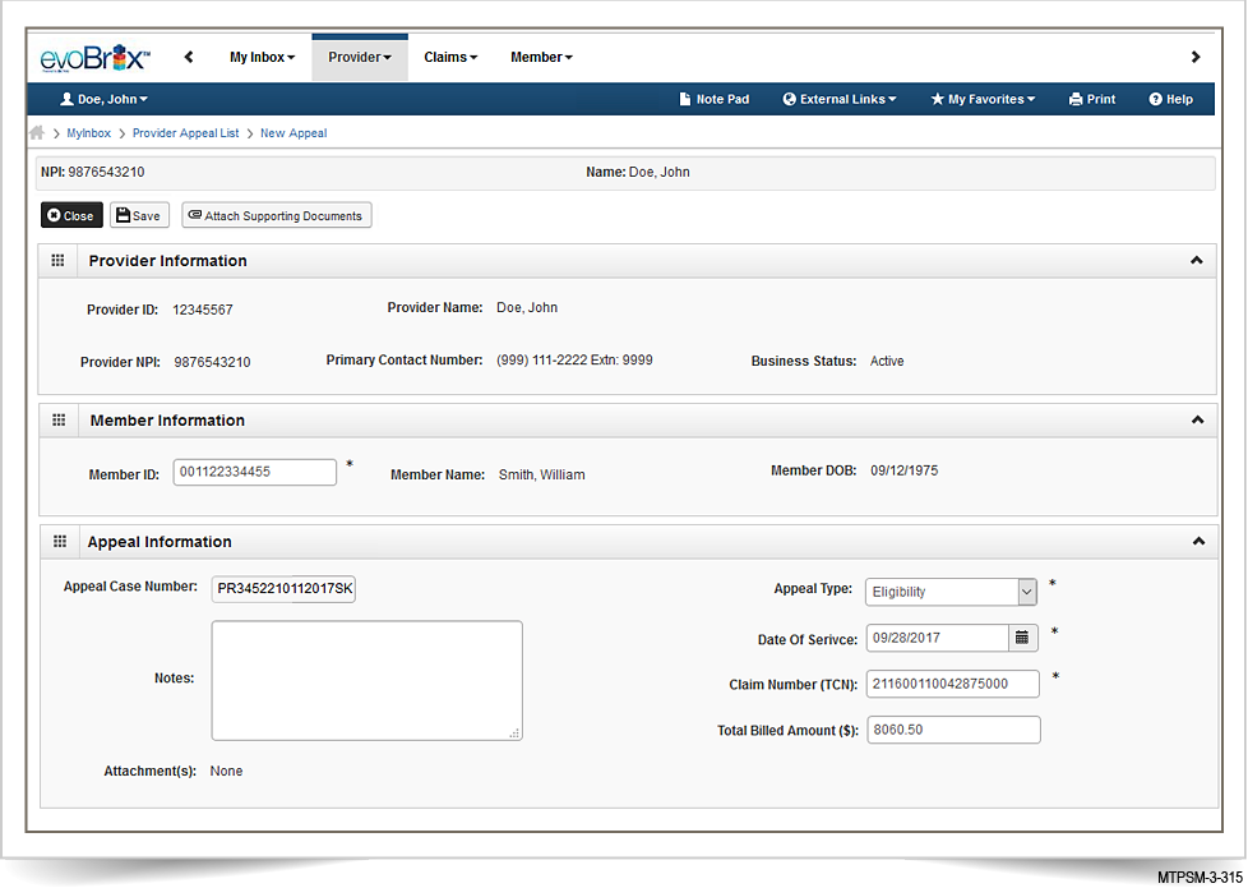


Figure 3.10.13-22. Self-service Appeal Request Screen. Providers can easily submit a new appeal request online.

PSER41

The Contractor's solution shall allow users to view the status of their appeal request.

The evoBrix self-service capability for appeal requests allows providers to search requested appeals and report on their status. Please see Figure 3.10.13-23, which shows a sample Appeal Status screen. The self-service portal allows providers to search by case number, appeal status, and submitted date. Additional search criteria can be configured and/or customized based on the DPHHS specific needs.

The appeals will be routed to the appropriate vendor in the DPHHS environment in real-time as a custom web service. The custom web service response will be parsed by evoBrix Translator and the appeal request status will be displayed on the self-service portal.

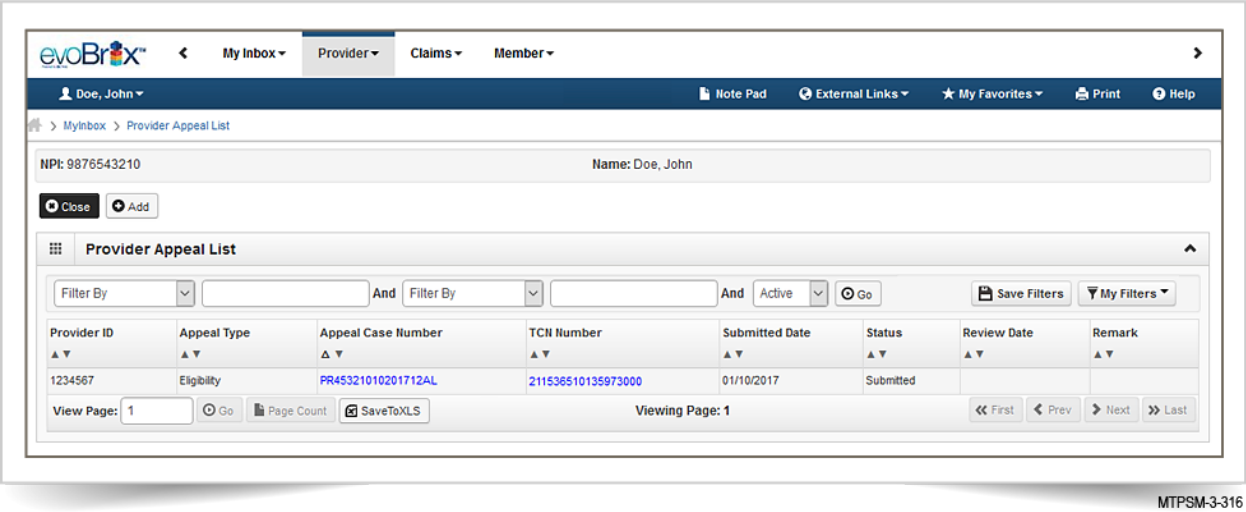


Figure 3.10.13-23. Sample Appeal Status Screen. Once created, appeal requests can be tracked, allowing providers to check status on the Provider Appeal List screen.

3.10.13.7 Self-Service PCCM Member Inquiry

This section outlines the requirements for Self-Service PCCM Member Display. The Offeror's proposed Option A solutions and services shall include display and download functionality to allow providers enrolled in care management programs to view their caseload and download their member registries. The Offeror must describe their approach to meet each of the self-service PCCM member inquiry requirements defined in Attachment F, Requirements Matrix.

evoBrix PMIS allows authorized providers, who are enrolled in the care management programs, to log into the system through the Provider Portal to view their respective members.

Team CNSI will work with DPHHS and the SI to identify the source system and data elements required to meet the unique PCCM Member Inquiry requirement. evoBrix will be configured and customized to meet the requirements of the PCCM member inquiry. PCCM member inquiry will leverage the integrated SOA-based, real-time web service call to the appropriate DPHHS solution module to display member registries.

Please refer to Section 3.10.13, where the proposed Option A solution is described, highlighting the modular integrated approach.

PSER14

The Contractor's solution shall allow authorized users to view registries for PCCM and other care management programs.

Team CNSI will work with DPHHS to identify search parameters. evoBrix will be configured and/or customized to meet the unique PCCM view registries and other care management programs.

Through the profile configuration, providers are able to access their Member Roster screen, which displays the active members associated with the provider under the case management program for the current month. The provider can view the members for any given period based on selected dates in the Filter By values field.

Figure 3.10.13-24 shows the navigation path to the sample Member Roster.

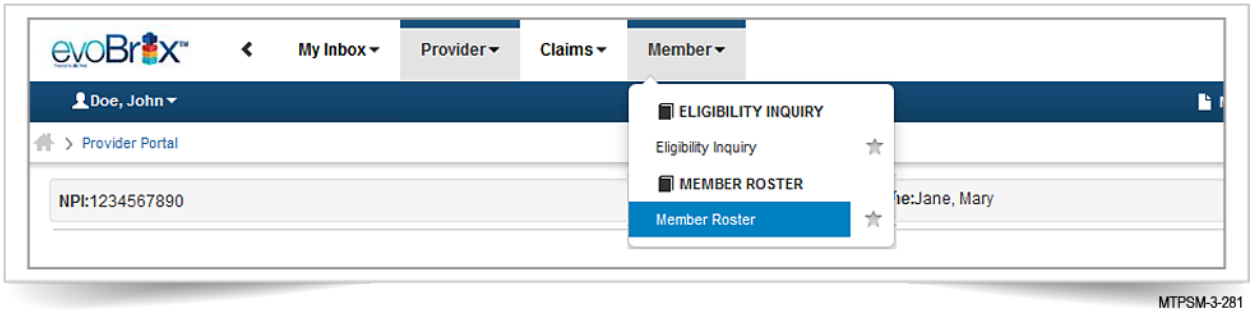


Figure 3.10.13-24. Member Roster. Using pulldowns, authorized providers are easily able to navigate to the Member Roster to view their member registry.

After providing the appropriate filter criteria, a real-time web service request is sent to the appropriate DPHHS solution module. Figure 3.10.13-25 shows the sample PCCM member registry web service response data elements.

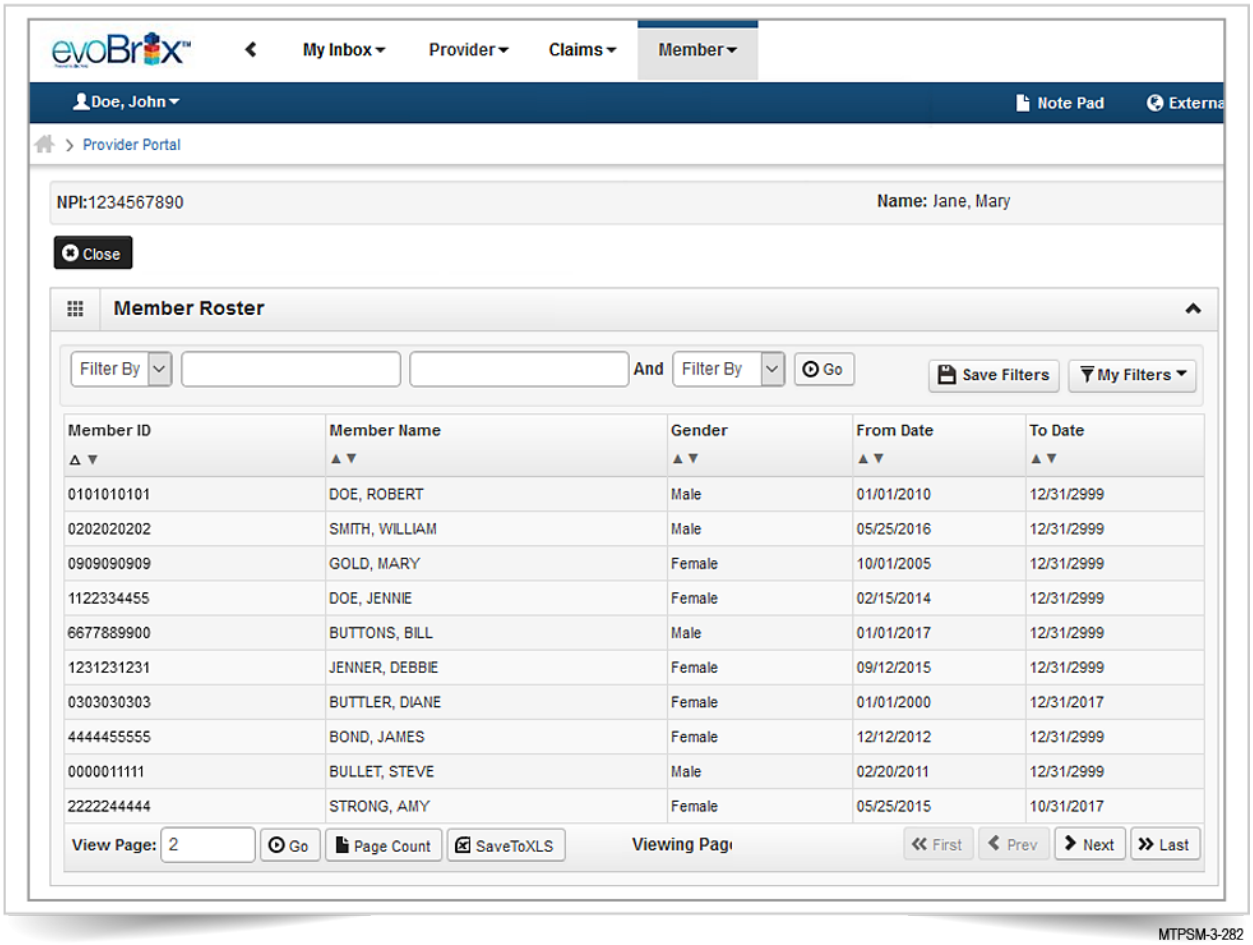


Figure 3.10.13-25. Member Registries. Authorized providers can use the evoBrix Member Roster screen view their member registries.

©2017 CNSI | Option A-30

PSER44

The Contractor's solution shall allow authenticated users to download or print member registries in Excel and PDF.

Figure 3.10.13-25 also shows the "SaveToXLS" button, which allows providers to save the member registries into Excel. From within Excel, users can leverage the application functionality to save the document to PDF.

3.10.13.8 Self-Service Online Claims Entry

This section outlines the requirements for Online Claims Entry. The Offeror's proposed Option A solutions and services shall include a real-time direct data entry claims solution for all claim types, corrections, void and replacement claims via the self-service portal and reject claims that fail front-end edits. The Offeror must describe their approach to meet each of the online claims entry requirements defined in Attachment F, Requirements Matrix.

Team CNSI knows that effective and timely claims processing is dependent upon accurate and reliable receipt of claims. We also understand that providers have differing needs and technical abilities. To support the provider community, the Team CNSI Option A solution provides user-friendly claims submission via the provider portal through DDE. evoBrix's innovative DDE solution will work in tandem with the payor claims adjudicating system.

The Team CNSI Advantage

Team CNSI's claims administration expertise is based on intake and adjudication of over 300 million claims every year.

- Experience supporting 25,000 unique trading partners representing roughly 290,000 providers
- Template-based claims to ease data entry for providers

MTPSM-3-244

The following process describes the role of evoBrix and the role of DPHHS' claims adjudicating system in real-time during and after the claim DDE process:

1. Claim information is entered in evoBrix using DDE screens
2. On-screen validations are performed during DDE in evoBrix
3. Data reference validations (e.g., verifying valid procedure code, diagnosis code) is performed via real-time service integration. Team CNSI will work with the SI to identify the services required for performing the required validations.
4. After DDE is complete in evoBrix, the claim is submitted as an 837 transaction to the claims adjudicating system in the payor environment. The Transaction Control Number (TCN) is generated in evoBrix.
5. Acknowledgement is sent back to the provider upon successful submission of the claim.

Real-time direct data entry claims for all claim types, corrections, void, and replacement claims are described in response to requirement PSER29.

Front-end claim edits are addressed in response to requirement PSER30.

Team CNSI's effective claims intake solution has been operational in the states of Michigan and Washington for more than a decade, and has been optimally designed to receive Medicaid Claims.

PSER13

The Contractor's solution shall include a self-service tool for providers to directly and efficiently enter claims.

The evoBrix Claim Processing Service offers easy to use screens, as shown in Figure 3.10.13-26, for authorized users to directly enter professional, institutional, and dental claims data into the system. The screens comply with HIPAA 5010 standards.

The main features of the DDE service include:

- Validation of claims data as it is entered. The validation requests will be routed via the evoBrix Integrator using real-time services.
- On-screen error messages are displayed when error conditions are encountered, thereby giving the user an opportunity to correct the data at the point of entry to prevent incorrect data from entering the system.
- Ease of claims entry due to informative messages that provide guidance and instruction.
- Reduction in claims suspension because of immediate data validation, ensuring quality claims data enters the system.

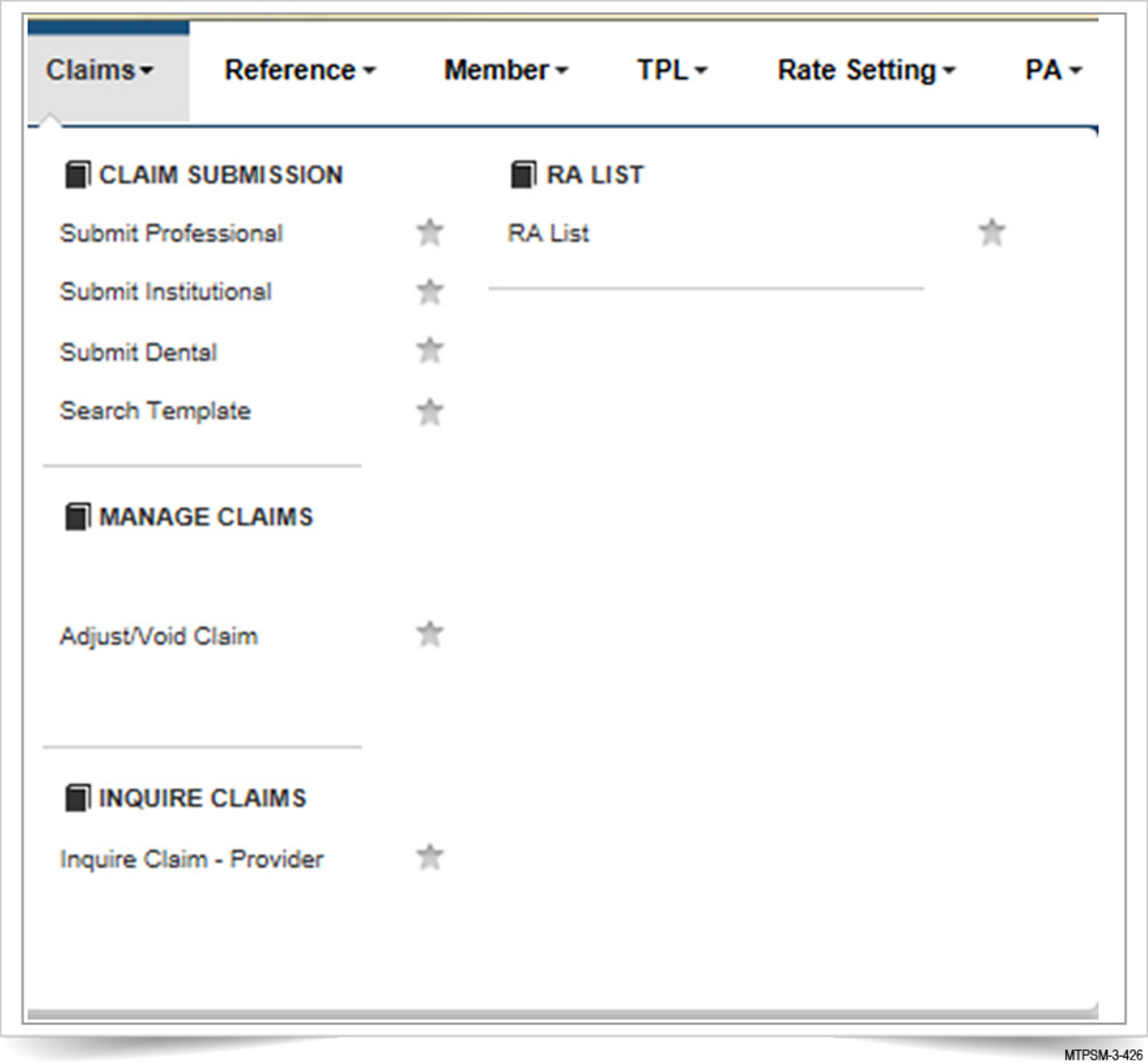


Figure 3.10.13-26. Claims Masthead. evoBrix is configured to allow the user to quickly select the web portal options offered by the evoBrix Core Claims Module.

Please refer to the introduction to Section 3.10.13.8 for additional details on the Option A solution approach.

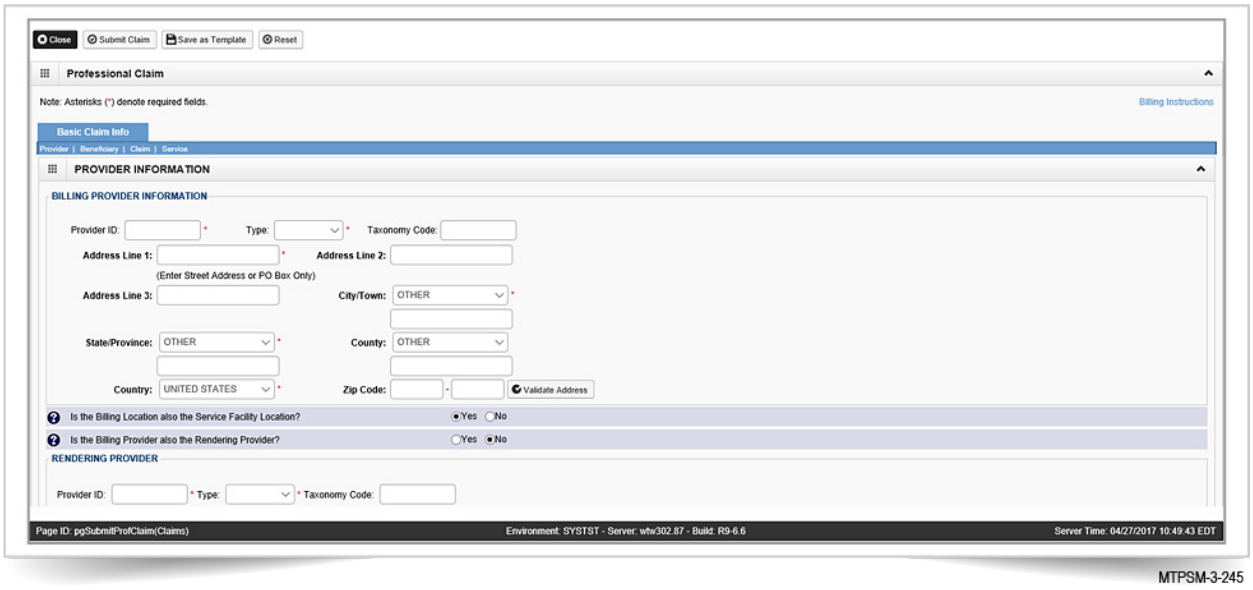
PSER29

The Contractor's online self-service claims entry tool shall accommodate and accept all claim types including Professional, Institutional, Dental, Encounter claims, Adjustments, Roster billing, claim corrections, and the ability to void and replace claims.

The evoBrix Option A solution offers authorized providers an ability to directly key in Professional, Institutional, or Dental claims from the portal using the DDE screen, as shown in Figure 3.10.13-27, Figure 3.10.13-28, and Figure 3.10.13-29. To ease the task of entering a claim into evoBrix directly, the

system provides screens that look like the corresponding claim forms. The data captured using the web screens is validated for data integrity, including the procedure codes, revenue codes, and Healthcare Common Procedure Coding System (HCPCS) codes, before being accepted into the DPHHS claims adjudicating system. Please see our response to requirement PSER13, which highlights the role and responsibility of evoBrix as the online self-service claims entry tool in relation to the claims adjudicating vendor.

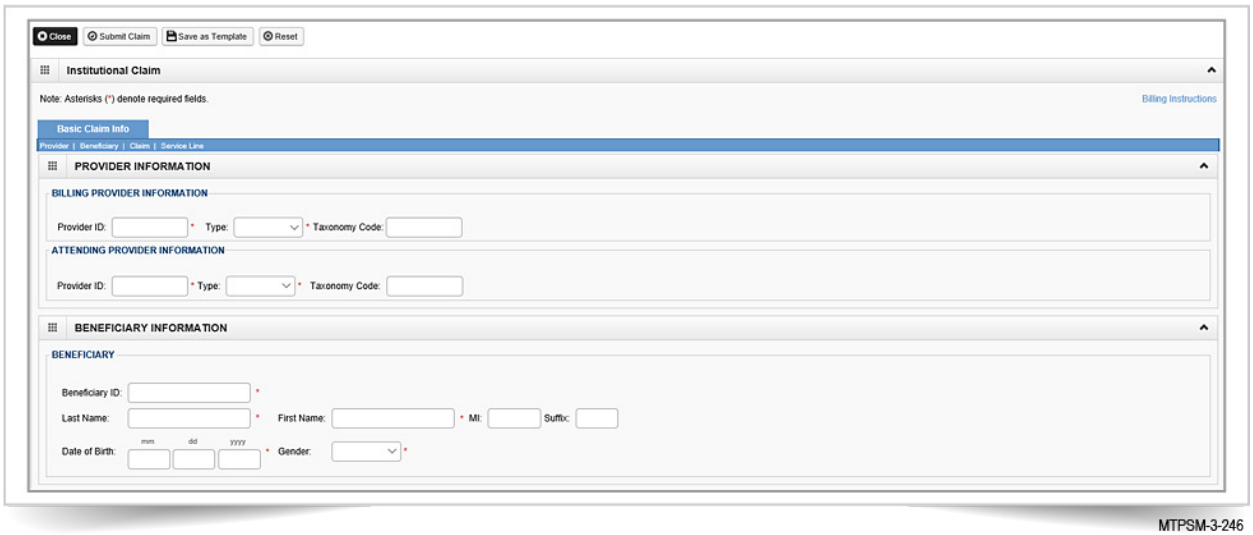
Figure 3.10.13-27 shows the DDE screen for a Professional claim.



MTPSM-3-245

Figure 3.10.13-27. Submit Professional Claim. evoBrix offers an easy-to-use screen for Professional Claim direct data entry. These screens enable providers with lower volume claims to expedite claim adjudication by direct claim entry.

Figure 3.10.13-28 shows the DDE screen for an Institutional claim.



MTPSM-3-246

Figure 3.10.13-28. Submit Institutional Claim. The evoBrix solution offers an easy-to-use screen for Institutional Claim direct data entry. These screens enable institutions with lower volume claims to expedite claim adjudication by direct claim entry.

©2017 CNSI | Option A-34

Figure 3.10.13-29 shows the DDE screen for a Dental claim.

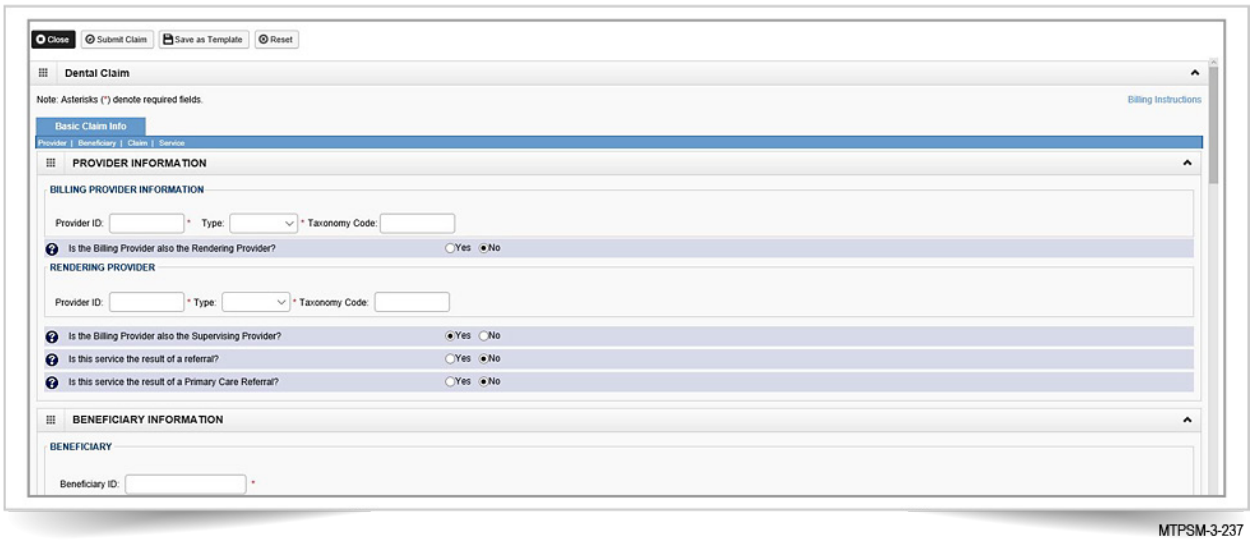


Figure 3.10.13-29. Submit Dental Claim. The evoBrix solution offers an easy-to-use screen for Dental Claim direct data entry. These screens enable providers with lower volume claims to expedite claim adjudication by direct claim entry.

Claims Adjustment and Void:

The evoBrix solution provides a user interface to adjust or void a paid claim. The Adjust Claims Document Billing List screen provides authorized providers access to search for paid claims. Various filter options on the List screen help the provider to specify precise search criteria to request the required claims. The search criteria information is converted into a custom web service request. The custom web service response will bring in a list of claims, as shown in Figure 3.10.13-30.

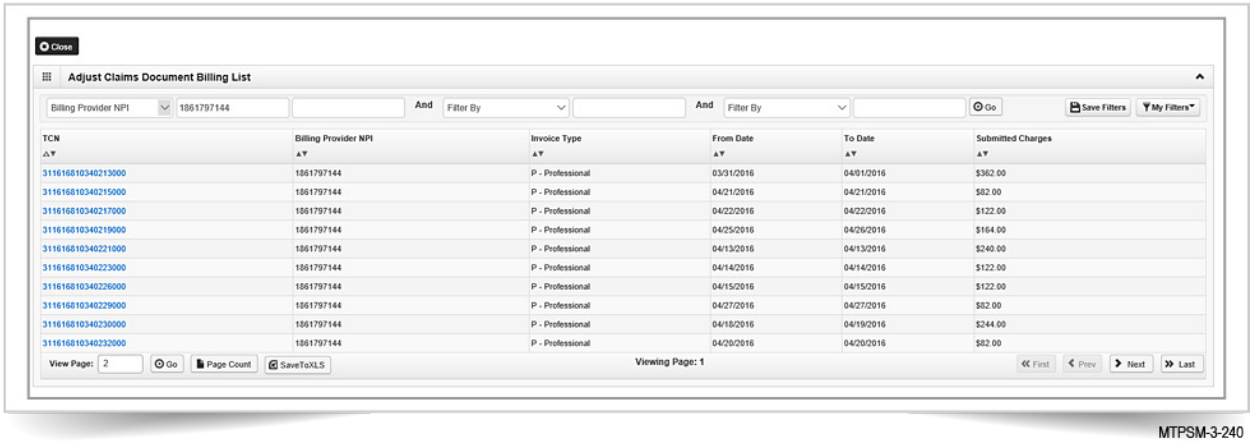


Figure 3.10.13-30. Claims List Screen. The screen provides a list of Paid claims based on the requested search criteria using EDI 276 and 277 transactions.

After selecting a paid claim for correction, evoBrix sends a 276 transaction request to gather the selected claim details. The MPATH Integration Hub sends the TCN details back to evoBrix using a 277 EDI transaction. The evoBrix Translator displays the transaction control number (TCN) details on the screen for the providers to either void or adjust the claim, as shown in Figure 3.10.13-31. The saved data on the screen is transferred to DPHHS via a HIPAA 837 transaction.

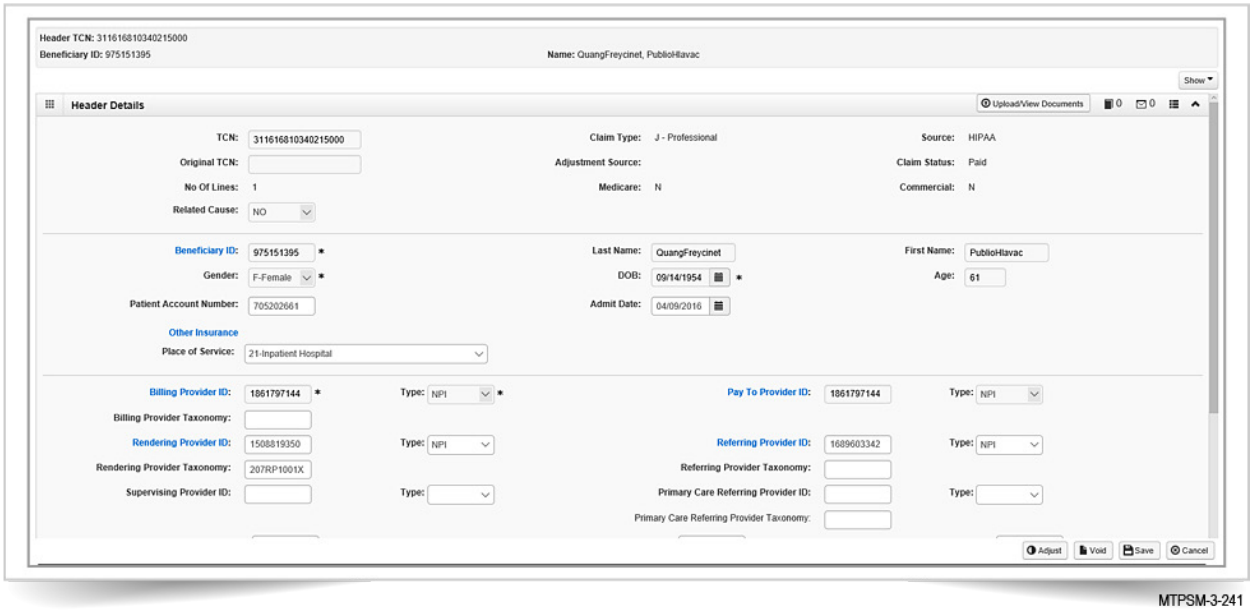


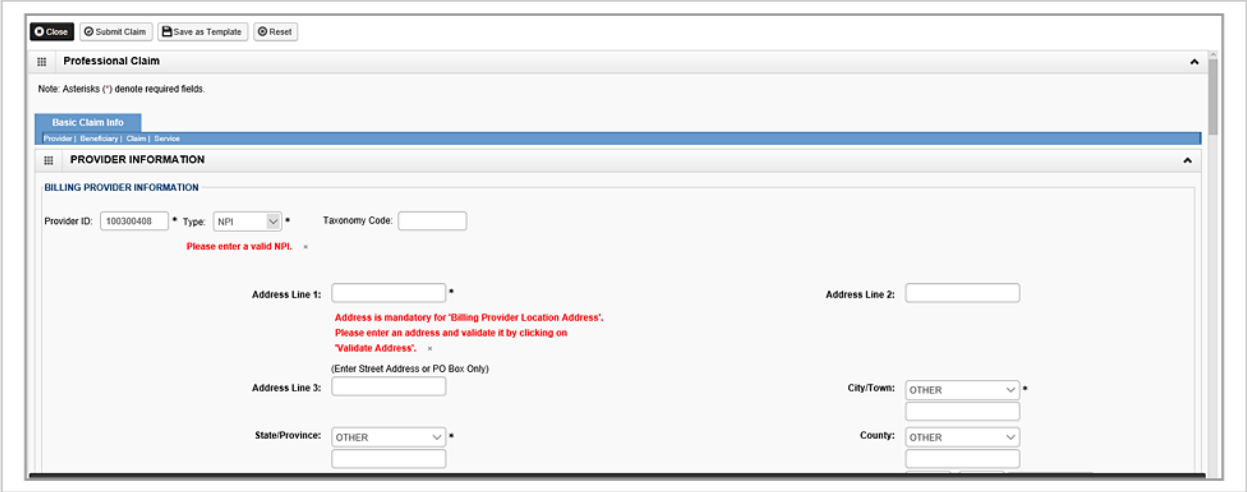
Figure 3.10.13-31. Adjust Claim Screen. The screen displays the transaction details to the user to void the claim or adjust the claim by updating the information.

PSER30

The Contractor's online self-service claims entry tool shall include a validation feature that performs real-time front end editing prior to claim submission, not allowing submission of claims that fail the front end edits. Edits will include, but are not limited to, active provider enrollment, member eligibility, valid revenue codes, procedure codes, and diagnosis codes. Front end edit(s) shall be displayed to the user for review and correction. The validation feature will not display pricing information.

The claims DDE screens perform various validations in real time before accepting the claim. Validation includes checking that a provider is active in the system, member's eligibility to receive a service, and validity of the reference data, such as revenue codes, procedures codes, and diagnosis codes. The system also performs various date validations.

When the error conditions are encountered, informative messages are displayed, thereby giving the user an opportunity to correct the data at the point of entry and prevent incorrect data from entering the system, as shown in Figure 3.10.13-32.



MTPSM-3-427

Figure 3.10.13-32. DDE Data Validation. The evoBrix DDE screens validate the data while submitting a claim and display informative messages on the screen for guidance.

The reference data validations are performed using real-time custom web service call to the Hub for routing. The actual request is eventually routed to and serviced by the appropriate claims adjudication vendor in the DPHHS environment.

evoBrix performs the following edits when a provider submits a Professional, Institutional, or Dental claim using the DDE screen:

- Admission Date must be equal to or less than From Date.
- Accident Date, Remittance Date, Statement Date From, Occurrence Date, Occurrence Span From Date, Accident Date, Appliance Placement Date validation against Date of Birth. These dates cannot precede member Date of Birth.
- Discharge Date cannot precede Admission Date.
- Service To Date cannot precede Service From Date.
- Duplicate check for Diagnosis Codes, Condition Codes, Related Causes
- Remittance Date can't be future date
- Invalid entry in various date fields
- Amounts must be numeric
- Valid entry check for reference data – Procedure Code, National Drug Code, Rendering Provider, Taxonomy Code, Anesthesia Procedure Codes, Billing Provider Taxonomy, Rendering Provider Taxonomy, Modifier, Beneficiary ID, Prior Authorization Number(s), Rendering Provider, Billing Provider
- Required fields check for the mandatory information
- Service Line entry check
- Field dependency validation checks – e.g. Supervising Provider ID cannot be the same as Referring Provider ID

PSER31

The Contractor's online self-service claims entry tool shall allow an authenticated user to upload an attachment to associate with a specific claim or multiple claims.

The DDE screen allows users to submit a claim via the self-service web portal. A TCN is generated for a submitted claim after successful data validation. The TCN is displayed on the screen and the solution allows the user to upload supporting documents. The uploaded documents are associated with the claim using the TCN. The documents are added to the DPHHS document repository or drop box location using a custom web service. Figure 3.10.13-33 shows a sample screen of successfully accepted claim details, along with a button highlighting document upload capability. Current functionality allows the users to submit multiple attachments to the same claim.

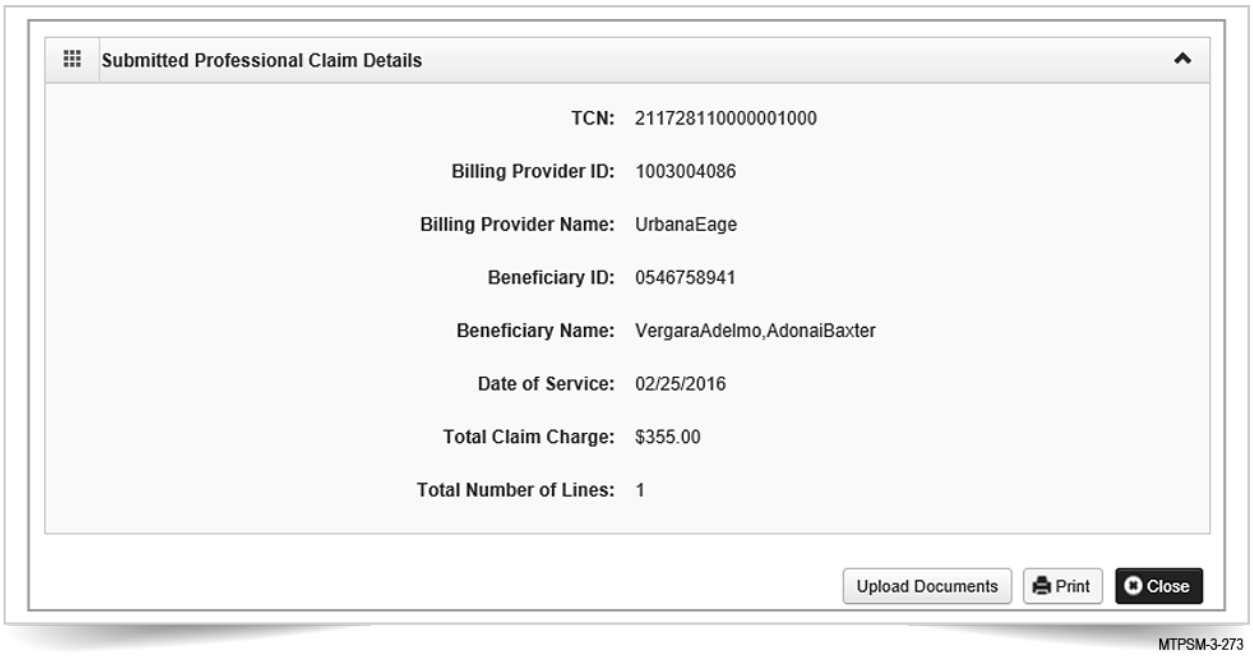


Figure 3.10.13-33. Upload Documents for a Claim. The evoBrix Upload Documents option allows users to upload documents while submitting a claim using DDE screen. Attachments are linked to the correct claim using the TCN.

PSER32

The Contractor's online self-service claims entry tool shall instruct users to include a claim confirmation number on any paper attachment when users indicate that an attachment is being mailed or faxed in order to allow for efficient association between a claim and an attachment.

When a claim is successfully submitted, the evoBrix solution generates unique TCN for the claim and displays it on the screen. The providers are required to use the TCN number while sending the attachments via paper or fax. That allows the DPHHS system to subsequently link the incoming document to an existing claim.

PSER33

The Contractor's online self-service claims entry tool shall allow users to indicate paper attachments will be mailed and/or faxed.

The evoBrix solution allows users to add a note to the claim submission. Using the Claim Note screen, providers can indicate on the claim that attachments will be mailed or faxed. Figure 3.10.13-34 shows the Claim Note screen highlighting this capability.



Figure 3.10.13-34. Claim Note. Users can add a note on a claim to indicate that supporting documents will be mailed or faxed.

PSER34

The Contractor's online self-service claims entry tool shall provide an tracking or control number to the user upon successful completion of the transaction.

Every claim entering the system through DDE is assigned a unique TCN. The TCN is used to track and maintain a claim in the system. The taxonomy of the TCN includes specific data that identifies the mode of entry of the claim, invoice type information, and the date it was received. Every TCN is 18 characters long.

Figure 3.10.13-35 shows the taxonomy of an evoBrix TCN.

Field	Length	Type	Description
Input Medium Indicator	1	Numeric	0 – Reserved 1 – Paper – Assigned by the Imaging System when the Claim is received in paper format. 2 – Direct Data Entry (DDE) (Web Submission) – Assigned by the System when the Claim is submitted through the DDE Screens 3 – Electronic (HIPAA) – Assigned by the System when the Claim or Encounter is submitted as an electronic batch. 4 – CE System-generated – Assigned by the System when the transaction is generated by the Core Claims Module. 5 – CM System-generated – Assigned by the System when the transaction is generated by the Managed Care Module. 6-7 – Reserved 8 – Paper – with Attachments 9 – Reserved
TCN Category	1	Numeric	0 – Reserved 1 – FFS – Assigned to any claim that is submitted directly to the system including Institutional, Professional and Dental Claims. 2 – Crossover – Assigned to any Claim received from the national Medicare intermediary.

Field	Length	Type	Description
			3 – Encounters – Assigned by the loading routine when the indicator on the X12 Claim is set as an Encounter including Institutional, Professional and Dental. 4 – Capitation Claims – System-generated claims created by the Contracts Management Module. 5 – Gross Adjustments – System-generated by Core Claims and Contracts Management Modules. 6 – Pharmacy Encounters – Stored and assigned TCN in the operation data store. 7 – Recurring Payments – System-generated by Core Claims and Contracts Management Modules. 8-9 – Reserved
Batch Date	5	Numeric	YYDDD – Year + 3-digit Julian date
Adjustment Indicator	1	Numeric	0 – Original Claim 7 – Replacement Claim 8 – Void All valid NUBC Frequency Type Codes are mapped to one of these values for internal processing. Note: Original Claim is 1 in HIPAA.
Sequence Number	7	Numeric	Sequence Number is by Input Medium and TCN Category, starting with 0000001 at the beginning of each Julian Date.
Line Number	3	Numeric	Line Number will begin with 001 for every new Claim. The header has the line number as 000.

Figure 3.10.13-35. Transaction Control Number Composition. The evoBrix TCN allows providers to uniquely identify a claim. The TCN is used to support claims inquiry, track the claim, and to ensure that attachments are linked to the correct claim.

Upon submitting a claim after entering valid data, evoBrix generates a TCN that is displayed on the screen.

PSER35

The Contractor's online self-service claims entry tool shall provide a configurable auto populate feature for appropriate fields for each claim type (e.g., provider information, submission date, member associated information).

The evoBrix DDE screens auto populate multiple fields by retrieving information from the system. Once the provider NPI information is entered, the solution validates that the provider is actively enrolled in the system and auto populates the address information. Similarly, after validating the member, the associated information, such as name, gender, date of birth, and age is auto populated. This functionality is achieved using a custom web service to the Hub. Please refer to Figure 3.10.13-36 and Figure 3.10.13-37, which highlight the auto populate capability.

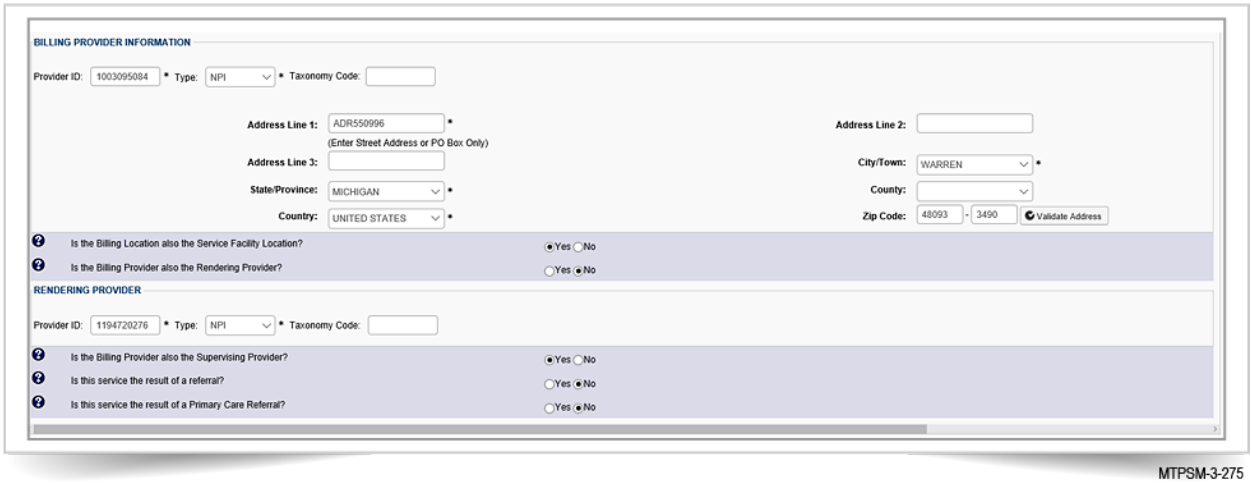


Figure 3.10.13-36. Provider Information. The provider information is auto populated based on the Provider ID and Type entered.

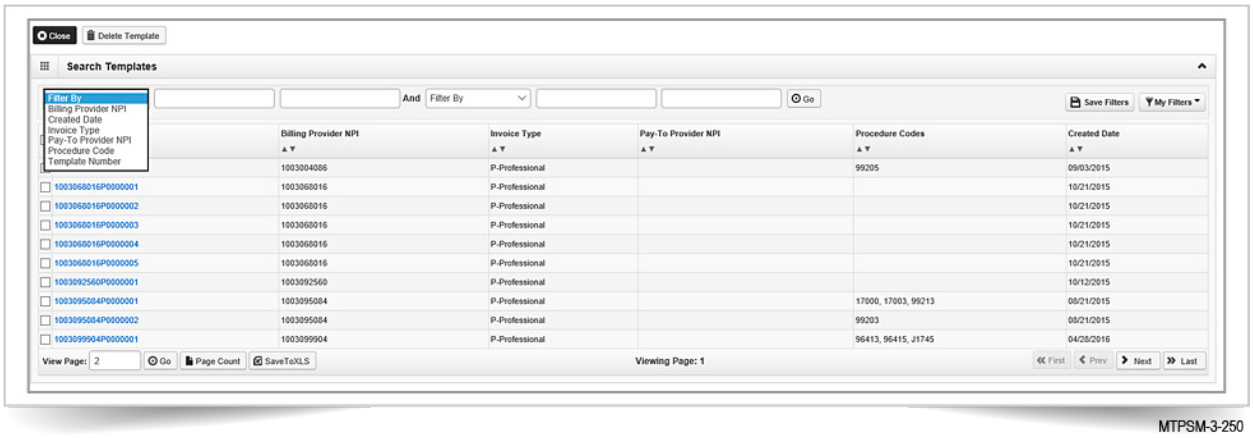


Figure 3.10.13-37. Member Information. The member information is auto populated based on the Beneficiary ID (Member ID) entered.

PSER36

The Contractor's online self-service claims entry tool shall include a claim template feature that allows users to create templates to be stored and used in the online claims entry tool.

As a service to the provider community, evoBrix offers a feature to remove the labor-intensive task of re-entering the same data on similar claims. evoBrix provides a Claim Template feature that enables the provider to save reusable claim data as a template. The saved claim templates are searchable using various options, as shown in Figure 3.10.13-38. Often, a provider submits very similar claims, and the Search Template feature allows the provider to select the most appropriate template to reduce data entry work.



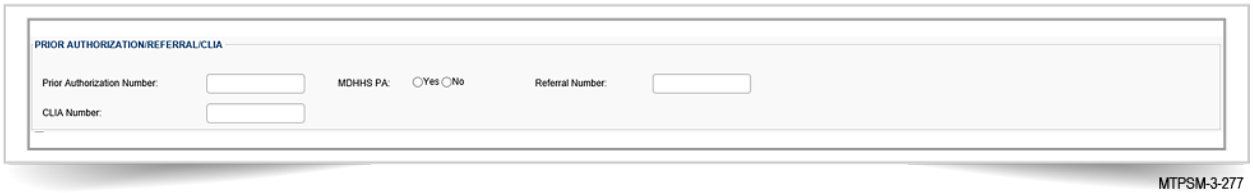
MTPSM-3-250

Figure 3.10.13-38. Search Templates. An evoBrix screen displays the saved templates and the various options to filter the search results. Saved templates help providers and Team CNSI personnel quickly select an appropriate template to enter a claim.

PSER37

The Contractor's solution shall provide search capabilities for users entering data in the online claims entry tool. The search tool will include provider information and provider associated service authorization information.

The evoBrix solution features a DDE screen with fields for entering the service authorization information, such as the prior authorization number and referral number, while accepting the claims data (as shown in Figure 3.10.13-39). The information entered is validated against the service authorization information available in the DPHHS claims adjudicating system using a custom web service.



MTPSM-3-277

Figure 3.10.13-39. Prior Authorization Information. evoBrix provides the fields for entering prior authorization number or referral number on the claims DDE screen.

PSER42

The Contractor's online self-service claims entry tool shall convert all entered claims into an X12 837 format.

All of the DDE claims are converted into standard HIPAA 837 transactions using evoBrix Data Translator. These claims are then added to the DPHHS claims adjudicating system using evoBrix Integrator and the MPATH Integration Hub.

Please see our response to Section 3.10.13 of the proposal for additional details on the evoBrix Translator and how it leverages the industry standard Edifecs translation engine.

3.10.14 Option B Provider Services

In addition to the primary scope of the Provider Services module, states may procure components and services not categorized in Section 3.10.1 through 3.10.13. Option B Provider Services requirements provide flexibility to States or Agencies who may desire to procure the components or services outlined in Option B as a part of this procurement versus a separate procurement. The Offeror is not required to include Option B in their proposal. If the Contractor chooses to include these services in their proposal the Contractor must describe in their response, their approach to meet the Option B requirements detailed in Attachment F, Requirements Matrix.

Team CNSI's collective experience with provider services and solutions spans over five decades and covers thirty-three states and territories. All our proposed services are based on best practices and lessons learned honed from actual experience providing similar services for other states and for Medicare.

The Team CNSI Advantage

Team CNSI has over 50 years of experience and the capability to deliver innovative provider services.

- Team CNSI's prior operations experience will facilitate successful provider services operations
- Proven call center services with a focus on provider satisfaction
- Mobile technologies support efficient site visit services using real-time system, eliminating paper

MTPSM-3-071

Team CNSI has a track record of successful provider services technology implementations in the states of Utah, Washington, Michigan, and Illinois. In addition, Team CNSI team member, Noridian Healthcare Solutions, LLC (Noridian), brings experience in Federal and State health care services, including direct support of providers participating in these programs. Noridian supports Medicare providers in 28 states, with several of those states participating in the NASPO ValuePoint collaborative. Experience serving providers in the states of Montana, Wyoming, South Dakota, North Dakota, Hawaii, and Oregon sets Team CNSI apart and brings value to each state as we leverage existing relationships and knowledge of the challenges providers face in each state. Evidence of our success in delivering excellent provider services can be seen in Noridian twice being awarded the CMS Provider Customer Service Program (PCSP) of the Year award, in addition to consistent praise by the providers served. Noridian doesn't only bring experience, but also brings results. The effectiveness of our programs is demonstrated by the high scores shown in the 2017 survey of providers' satisfaction. Noridian's scores for its Medicare Jurisdiction F contract – the contract that includes the states of North Dakota, South Dakota, Montana, and Wyoming – was the highest in the nation.

We have the technology, business processes, and experience with the provider community for the multi-state cooperative members supported through the NASPO ValuePoint initiative. This unmatched geographic and operational experience is the foundation for the Option B Provider Services:

- Conduct Provider Site Visits
- Include Reference Documentation
- Customer Relationship Management (CRM)
- Provider Call Center
- Integrated Voice Response (IVR)
- Staffing
- Collect and Enter State Auditor's Office Financial Information
- Performance Requirements

Another unique aspect of Team CNSI's solution is that we have implemented solutions in a multi-state environment in the states of Michigan and Illinois. We understand the details of configuring multi-tenant, cloud-hosted, rules-based solutions specifically for Medicaid programs. In addition, the modular solutions of the future require vendors experienced in multi-vendor collaboration and capable of not only

interfacing technology seamlessly, but also interfacing business processes. Team CNSI members have the distinction of having over a decade of experience in the first Medicaid operation to fully embrace modularity in administrative services. Iowa's Medicaid program had struggled with a monolithic legacy vendor that provided Iowa very little visibility into the status of its Medicaid program. Iowa Medicaid Enterprise implemented its vision in 2005 by separating administrative services between eight vendors. This implementation had many parallels to the NASPO ValuePoint cooperative program vision, and the lessons we learned in 12 years of operating this system will be applied in providing the Option B Provider Services.

Figure 3.10.14-1 provides a graphical overview of our provider services and solutions that support Option B. Option B requirements include systems-based solutions, business services, technical services, staffing, and Service Level Agreement (SLA) monitoring and reporting. Figure 3.10.14-1 provides the context and high-level relationships of these solutions and services.

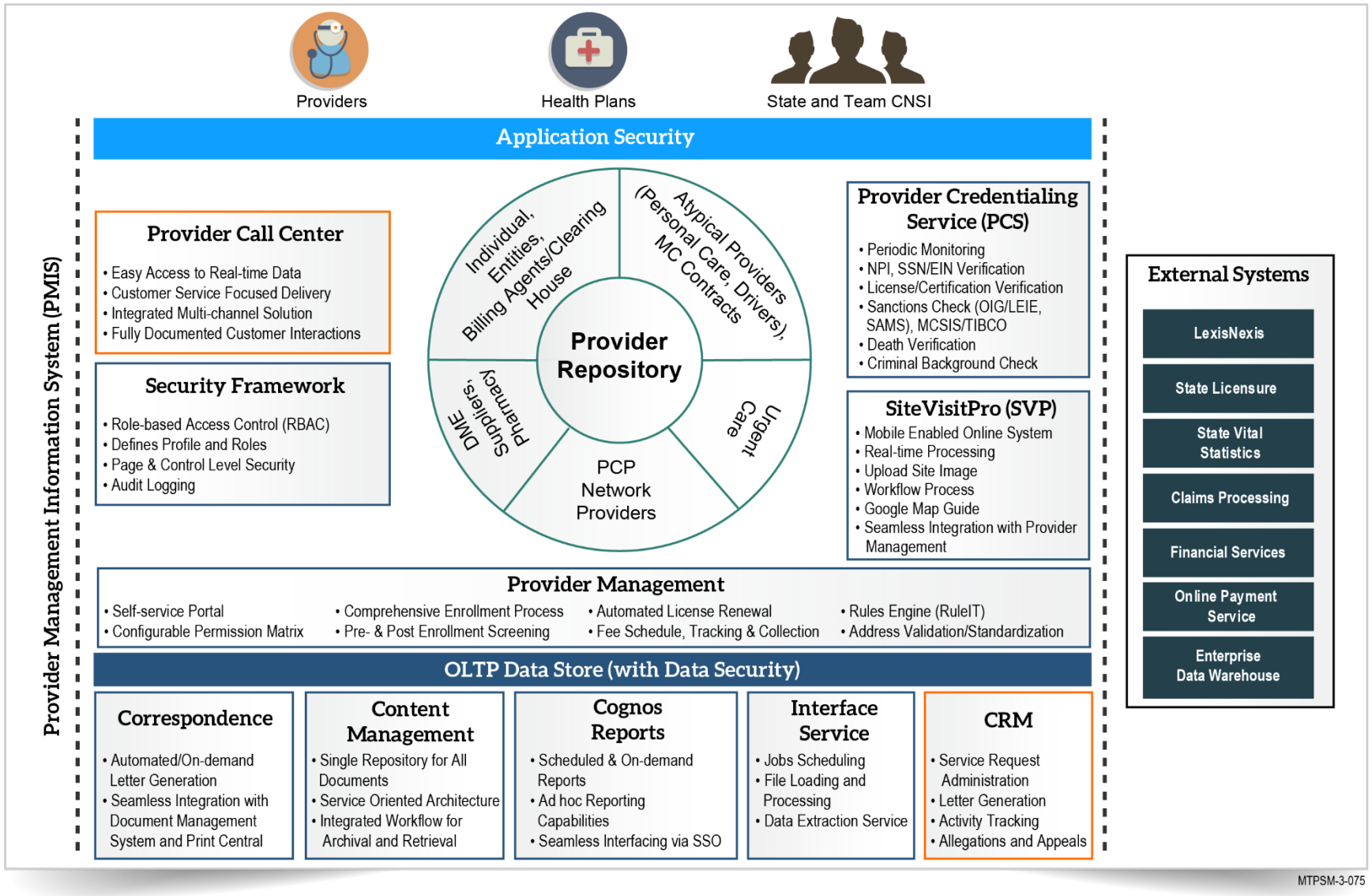


Figure 3.10.14-1. Team CNSI's Provider Services Overview. Team CNSI has a complete services and solution offering for provider services that promotes efficiency and customer service through automation.

©2017 CNSI | Option B-3

The core aspect of our solution is based on our evoBrix Provider Management Information System (PMIS), which provides a repository to enable our business operations staff to manage the full life cycle of provider services. A rich set of provider management capabilities enables self-service, provider enrollment, pre- and post-enrollment screening, license renewal, and address validation/standardization.

Figure 3.10.14-2 provides the key features and benefits of Team CNSI's Option B services.

Option B Provider Service	Key Features and Benefits	Proposal Location
Conduct Provider Site Visits	■ Mobile application, SiteVisitPro (SVP), and automation for efficiency and more responsive service ■ Production experience with SVP in the state of Michigan	3.10.14.1 Conduct Provider and Maintain Site Visits
Include Reference Documentation	■ Integrated with provider self-service capabilities	3.10.14.2 Include Reference Documents
Customer Relationship Management (CRM)	■ Scalable, configurable, robust solution that employs the principles of service oriented architecture (SOA) ■ Integrated and proven with evoBrix PMIS	3.10.14.3 Customer Relationship Management
Provider Call Center	■ Ready access to relevant information in real-time ■ Prompt answers to questions, supported by multiple technologies ■ Consistent and accurate information ■ Automated tracking and reporting of all contact types, from initiation through closure	3.10.14.4 Provider Call Center
Integrated Voice Response (IVR)	■ Skills-based routing ■ Integrated with CRM ■ Flexible call trees and scripts	3.10.14.5 Interactive Voice Response System
Staffing	■ Focus on customer service ■ Focus on provider satisfaction supported by receipt of satisfaction scores well above the national average ■ Lean staff management maximizes productivity and efficiency ■ Proactive and regular review of operational metrics support ability to monitor and adjust to assure SLAs are met	3.10.14.6 Staffing
Collect and Enter State Auditor's Office Financial Information	■ Online features of PMIS enables providers to update W-9 and provider information	3.10.14.7 Collect and Enter Provider Financial Information in State Financial Systems
Performance Requirements	■ Near real-time monitoring with HealthBeat ■ Focus on transparency of operations to provide states with meaningful insight ■ Proven business processes based on Lean principles ■ Business processes based on ISO 9001:2015	3.10.14.8 Performance Standards

Figure 3.10.14-2. Key Features and Benefits of Option B Services. Team CNSI's Option B services offer many features and benefits for NASPO ValuePoint state cooperative members.

The following requirement is part of the Option B Provider Services requirements, but is not aligned with any specific Requirement Section of Attachment F. In accordance with the Q&A responses, we are including them with our introduction to our Option B Provider Services responses. This requirement and its response addresses interfaces related to the Option B Provider Services.

INR13

The Contractor shall provide an extract of Agency defined data to the Agency data warehouse, at a minimum, weekly.

The evoBrix ISR solution is capable of sending the required extracts with the defined data sets to the data warehouse on a schedule basis. The ISR solution offers various batch schedule frequencies such as daily, weekly, monthly, yearly, on a specific day in a week, on a specific day in a month, only weekdays, only weekends, multiple times in a day, and other custom schedules. Batch frequencies of an interface are configured in the ISR solution, and any changes to schedules can be easily accommodated. For data exchange with external systems, the proposed platform provides a comprehensive data reconciliation framework that mirrors the same structural and data integrity with external systems.

The remaining sections provide detailed responses to each of the Option B requirements.

3.10.14.1 Conduct Provider and Maintain Site Visits

This section outlines the requirements necessary for conducting and maintaining provider site visit information. During the provider enrollment screening process for moderate and high-risk providers, there is a mandated requirement for the Agency to conduct an on-site evaluation of the provider. The Offeror's Proposed Option B solutions and services shall include providing staff to act on behalf of the Agency in order to conduct the on-site evaluation of the provider. The Contractor will upload the results of the site visit evaluation into the provider's profile within the Provider Services module. Site visits can include but are not limited to: verification that the information submitted to the Agency is accurate and in compliance with federal and state enrollment requirements, accurate business hours, checking personnel at the business location, etcetera. The Offeror must describe their approach to meet each of the Site Visit requirements defined in Attachment F, Requirements Matrix.

A key aspect of maintaining the integrity of Medicaid programs is to be judicious in enrolling providers. In accordance with § 42 CFR 455.432, the Affordable Care Act (ACA) requires a state Medicaid agency to conduct pre-enrollment and post-enrollment site visits of providers who are designated as "moderate" or "high" categorical risks to the Medicaid program. The purpose of the site visit is to verify that the information submitted to the state Medicaid agency is accurate, to determine compliance with federal and state enrollment requirements, and to prevent fraudulent practices.



Team CNSI will designate two business operations staff members to conduct site visits. These staff will telecommute from two separate locations in the state to provide coverage across Montana's significant geographic footprint. We will use a similar approach across other states as needed. Team CNSI identifies providers in each risk category and creates a schedule for site visits associated with pending new enrollments, revalidation, and other post-enrollment visits. We create a balanced stream of workload to best use staffing resources and minimize any "bubbles" of workload. For revalidations, we evaluate the provider's risk category, last validation date when applicable, and schedule the provider, assuring that providers are revalidated in the timeframe appropriate for their risk level.

Team CNSI staff use our innovative mobile enabled application, SiteVisitPro (SVP) to plan, conduct, and maintain site visits. SVP is designed for use with tablets to enable our business operations staff to provide site visit updates on a real-time basis to support the enrollment process. Eliminating the need to transfer data from paper forms greatly improves the accuracy and efficiency of our provider enrollment processes. This application uses real-time provider information directly from our PMIS, eliminating redundant data entry and increasing efficiency with the elimination of paper processing. SVP assists in the identification of fraudulent providers by capturing specific information about the provider's practice. SVP can be accessed from anywhere via a mobile 4G/cell wireless connection. In the event of mobile network outages and connectivity issues, Team CNSI staff will capture all necessary site visit information in paper form, and enter the information into the system once internet connectivity is reinstated or available. The MT PSM solution:

- Streamlines Site visit processing using a real-time system, reducing the need for paper
- Eliminates periods of no activity on the site visits through alerts to the appropriate business operations staff
- Decreases the time it takes to approve or reject a provider's application for enrollment
- Eliminates redundant data entry and manual updates to the Medicaid provider enrollment system
- Enables staff to upload any documents (e.g., PDF files created from scans) collected from the provider

Figure 3.10.14-3 provides an overview of Team CNSI's Site visit processes. It demonstrates the two primary solutions modules, PMIS and SiteVisitPro, used by our staff to manage and conduct provider enrollment and other site visits. The PMIS module provides the central provider enrollment and management capability supported by an attribute-rich data store. Key provider information such as demographics, locations, ownership, taxonomy, and risk category are shared with SVP for providers selected for site visits. SVP is used to manage all aspects of the site visit from scheduling to documenting the results. The site visit results are posted to the PMIS for reporting and record keeping. Site visit process steps and activities are logged for monitoring using Team CNSI's HealthBeat.

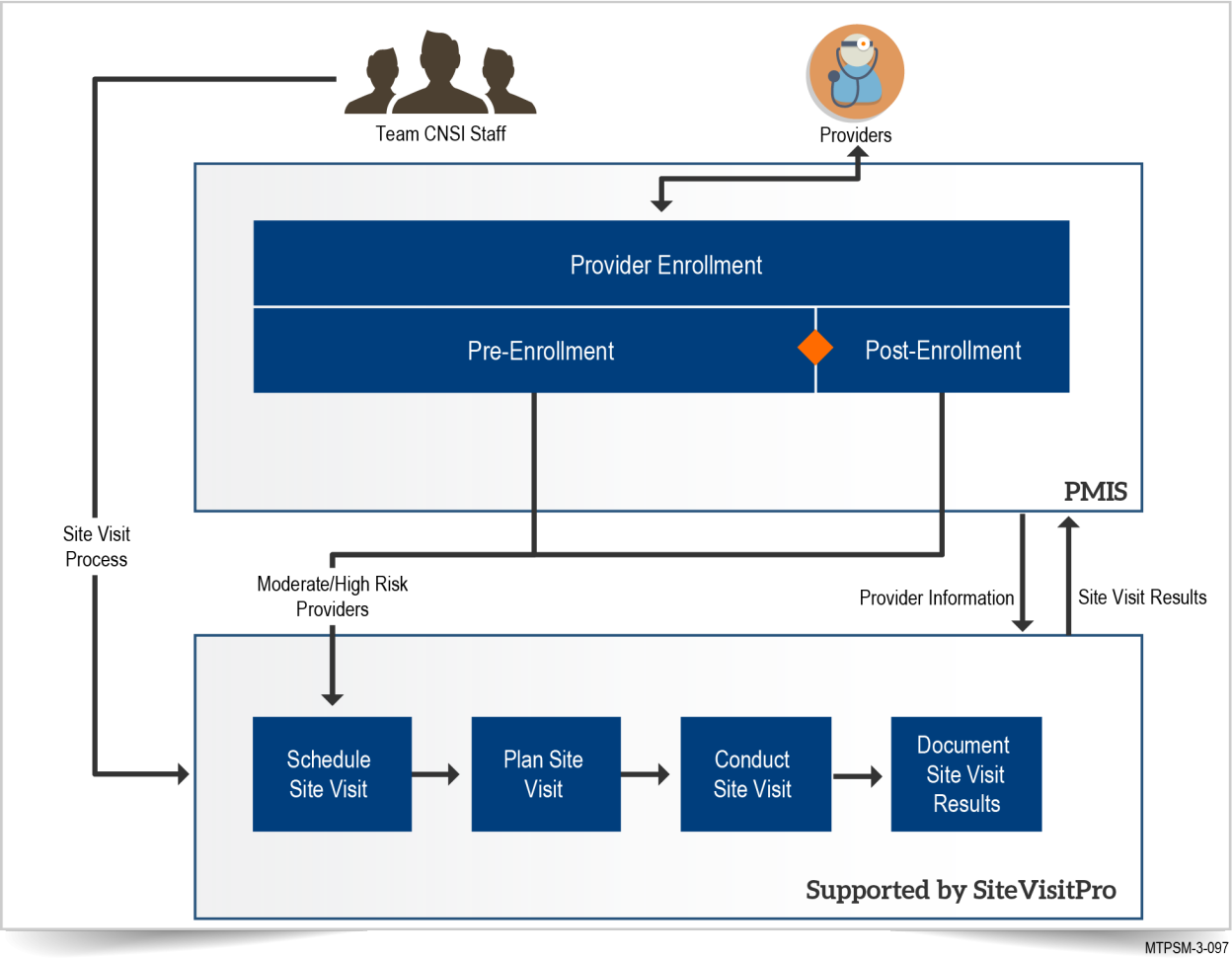


Figure 3.10.14-3. Team CNSI Site visit process Overview. Team CNSI staff use proven tools such as SiteVisitPro to schedule, plan, conduct, and track site visit information which increasing their efficiency and reducing the need for manual processes.

PSV01

The Contractor shall conduct pre- and post-enrollment onsite screening of moderate and high risk providers according to Agency onsite screening protocols and federal onsite screening regulations, including at a minimum:

-Conducting the initial assessment to verify the facility location, hours and personnel;

-Verifying operational status; and

-Confirming final determination of provider enrollment status.

During the implementation phase, Team CNSI will work with DPHHS to document DPHHS' screening protocols and criteria for site visits. This documentation will form the basis of the site visit services Team CNSI will conduct during operations. Screening protocols include specific data collection questions that are completed upon a site visit.

Team CNSI's business operations staff use checklists housed within SVP which provide a set of questions for each provider type. For example, a Durable Medical Equipment (DME) supplier would have a

different checklist from a clinical laboratory. The questions and protocol information are configured into the SVP during the implementation phase and updated as necessary during operations. The key point is that the screening process is standardized to ensure consistent results and automated to eliminate manual documentation. As shown in Figure 3.10.14-3, site visits have four major steps:

- Schedule site visit
- Plan site visit
- Conduct site visit
- Document site visit results

Schedule Site Visit

The site visit mobile-enabled application provides a user-friendly graphical user interface (GUI) for administering, scheduling, and collecting site visit information. Team CNSI's business operations manager, with the role of administrator for the SVP, can search, review site visit results, or view the site via Google Maps. Our business operations manager monitors enrollment processes for providers categorized as moderate or high risk using DPHHS' approved screening criteria. DPHHS may also identify providers for site visits.

The business operations manager schedules site visits using SVP by searching for a specific provider using provider national provider identifier (NPI), specialties, location, tax identifier, or risk level. Assignments are made to a designated Team CNSI staff member to conduct the site visit. Team CNSI anticipates most site visits as we monitor the moderate/high risk providers coming up for revalidation in a particular period. As we schedule moderate/high risk provider visits, we work to arrange visits for other providers in geographic proximity. Figure 3.10.14-4 shows the provider search screen used by our scheduler to find the targeted provider.

Our business operations manager can also search for already scheduled site visits to review workloads, reschedule, or reassign the site visit. Reassignment may be necessary to conduct a second site visit if the first site visit was not completed due to unavailability of the provider's office manager or other needed personnel. This is a likely occurrence given that site visits are often unannounced. The information presented for each site visit includes provider details, assigned business operations staff, site visit details, and additional information.

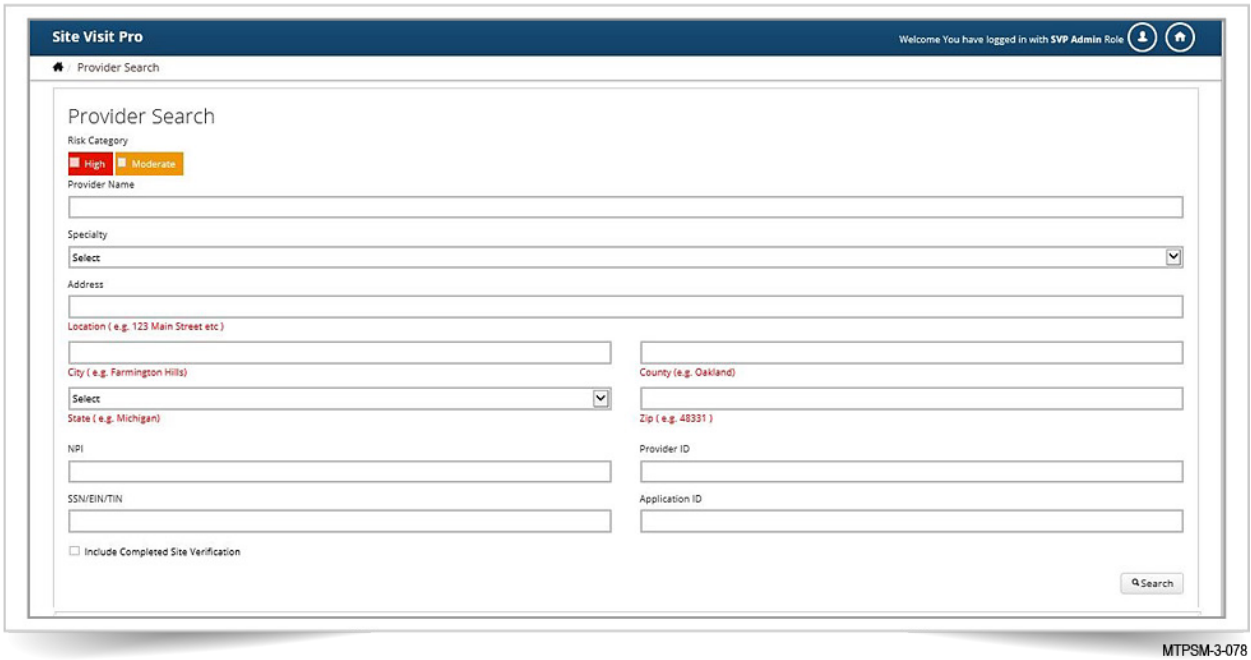


Figure 3.10.14-4. Provider Search Screen. Scheduling begins with finding the right provider(s) by provider NPI, specialties, location, tax identifier, or risk level.

Plan Site Visit

Once the site visit is assigned to a Team CNSI business operations staff member, planning for the site visit begins. Planning includes logistics for physical travel as well as preparation of data collection questions. When possible, multiple providers will be visited during the same trip for efficiency. Team CNSI will coordinate with the appropriate NASPO ValuePoint state, if needed, prior to conducting the site visit. Planning site visits includes the following activities:

- Review provider details including location, operating hours, and personnel
- Verify prior Medicare-based site visits using the CMS Provider Enrollment and Chain of Ownership (PECOS) system
- Plan travel
- Review site visit history (Figure 3.10.14-5 provides a sample screen showing site visit history for a provider)
- Plan data collection questions
- Review site visit calendar displayed in SVP
- Provide recommendations to the business operations manager after the completion of the site visit

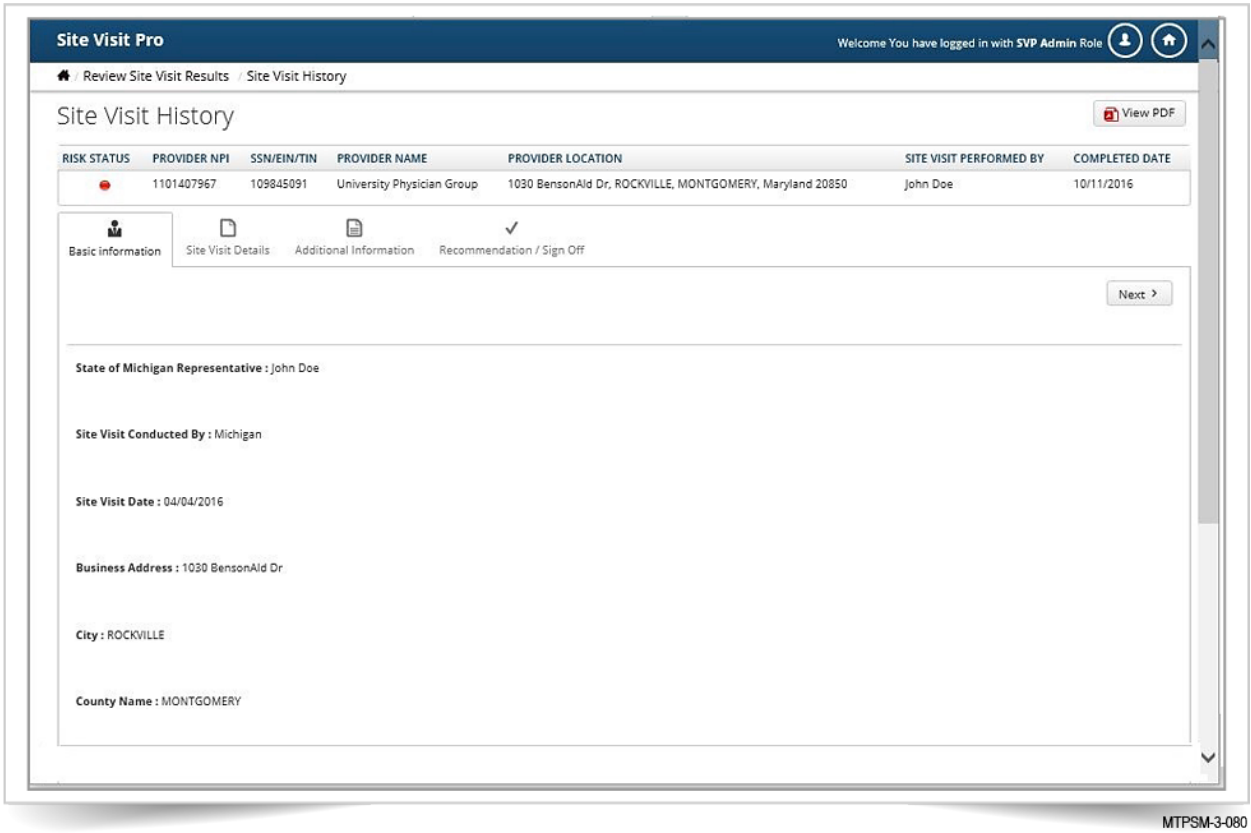


Figure 3.10.14-5. Site Visit History. SiteVisitPro shares information with data in the PMIS and provides the ability to review prior site visit information that may have been conducted by other states.

Conduct Site Visit - Verify Initial Assessment and Operational Status

Team CNSI's business operations staff member arrives at the provider site and discusses the site visit with appropriate provider staff. The provider's operational status is verified including:

- Verification of location
- Review of business hours
- Reviewing adequacy of staff
- Verifying patients are scheduled (when applicable depending on provider type)
- Verifying equipment is present and seems reasonable (depending on provider type)
- Confirming that patient or other necessary records are kept and available
- Review of questions (checklists), screening protocols defined for the provider type by DPHHS

Site visit information is captured in SVP in real-time during the visit. Figure 3.10.14-6 presents one of the views of SVP that is used to review and capture site visit information. Photos of the provider location are also taken using SVP to include as a part of the site visit record.

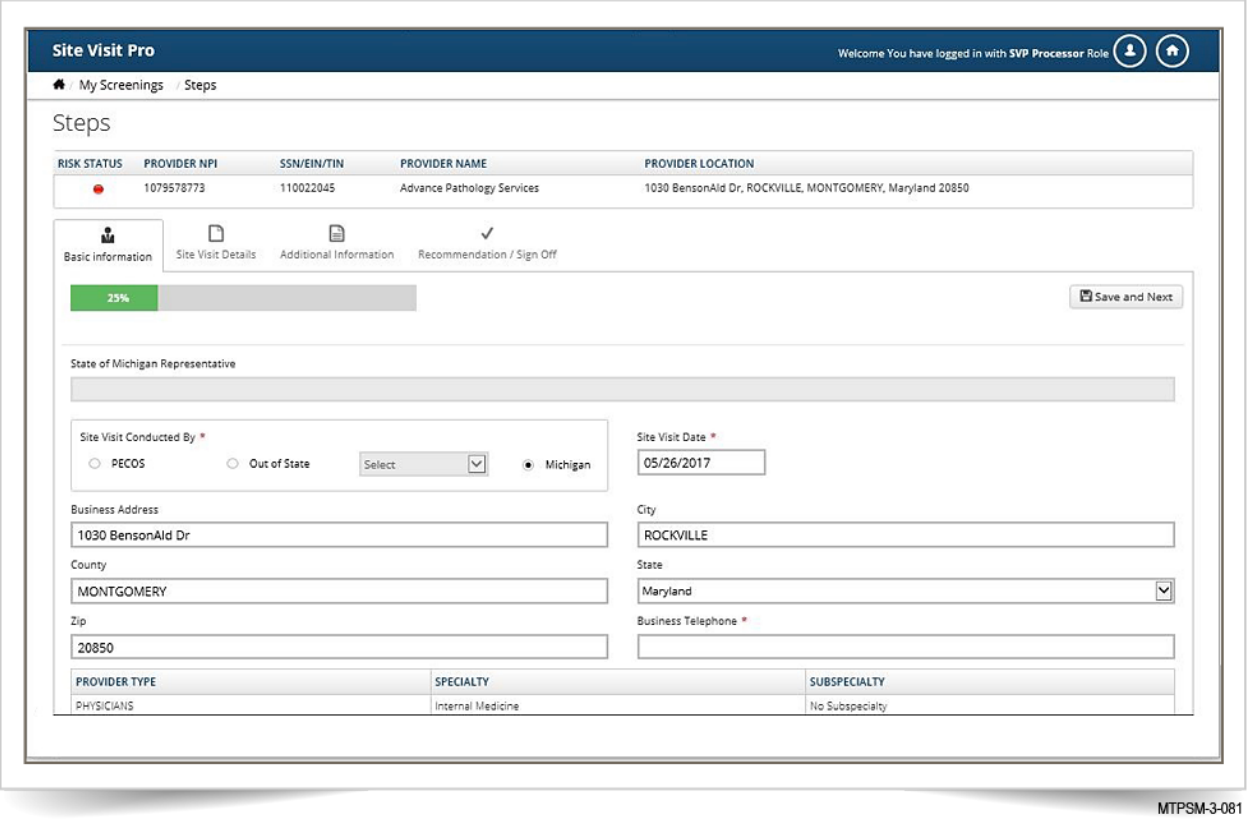


Figure 3.10.14-6. Site Visit Details. Team CNSI staff captures site visit details in real-time using SiteVisitPro.

Document Site Visit Results - Confirm Final Determination of Provider Enrollment Status

While onsite, Team CNSI's business operations staff member completes the site visit checklist along with a recommendation as to whether the provider "passed" or "failed" the site visit and submits the data using SVP. If necessary, the final site visit information is entered into the system when the business operations staff member returns to the office. Often any photos or other documentation collected from the provider are uploaded during this last stage of the site visit. Team CNSI staff use the site visit information along with all other enrollment screening results to make a final determination of the provider's enrollment approval. Figure 3.10.14-7 shows the screen from SVP used to capture site visit recommendations.

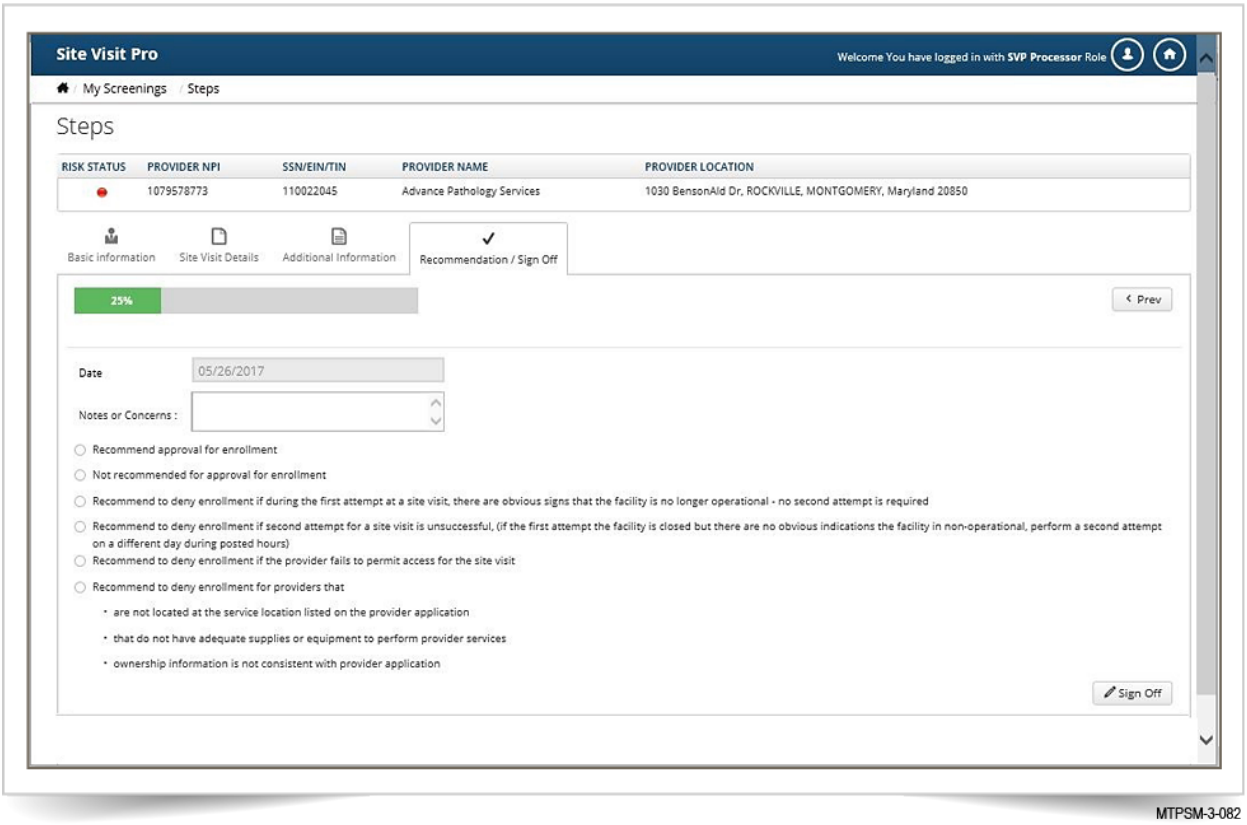


Figure 3.10.14-7. Site Visit Recommendation. Site visit results are published immediately after the site visit is completed and approved by the Team CNSI business operations manager.

3.10.14.2 Include Reference Documents

This section outlines the requirements necessary to include reference documents in the provider portal. The Offeror's Proposed Option B solutions and services shall include providing access to current and historical provider manuals and other reference documentation, as necessary, within the portal. The Contractor will not be responsible for creating or maintaining manuals. The Offeror must describe their approach to meet each of the Current and Historical Reference Document requirements defined in Attachment F, Requirements Matrix.

The evoBrix Provider Management Information System (PMIS) solution seamlessly integrates with IBM FileNet, which is Team CNSI's Document Management System (DMS) and will serve as our Enterprise Content Management (ECM) solution.

FileNet will be the repository for all provider support materials, State policies and procedures manuals, training materials, and system generated correspondences. Our ECM solution is high scalable. For example, we have generated and stored over 4 million correspondence documents in our Michigan operations.

FileNet supports high-speed ingestion of imaged and non-imaged content through a series of tuned processes. Unlike other document management solutions, electronic documents are

The Team CNSI Advantage

Team CNSI's evoBrix PMIS solution uses IBM FileNet as the Content Management solution.

- It supports a wide variety of document formats including, but not limited to Word, PDF, Visio, Excel, PowerPoint, TIFF, and JPEG
- Internal users can access integrated content from the FileNet content repository using a simplified easy-to-use interface through IBM Content Navigator
- External users can search for and view manuals through a menu option directly within the evoBrix PMIS portal

MTPSM-3-236

stored in their native formats, which reduces errors in transformation and supports future accessibility and migration to other platforms. FileNet is a configurable, integrated, and secure solution that provides the agility required to adapt to change, while assuring accuracy and timeliness of information. FileNet supports all facets of document management, including common and generic features like ingestion, storage, retrieval, filing, and retention. The integrated security features ensure that documents are accessible and distributed only to authorized users.

Solution Summary

State staff members are provided access to IBM Content Navigator, which is a versatile application that can deliver integrated content from the FileNet content repository using a simplified easy-to-use interface. They manage and administer the provider manuals through the IBM Content Navigator tool. They can also access the documents through the evoBrix PMIS portal. Providers, on the other hand, can only access the manuals and support materials through the evoBrix PMIS portal.

FileNet Security

Content Platform Engine is the core component of IBM FileNet, which an administrator can use to create and manage document classes, properties, storage, and metadata that form the foundation of the FileNet ECM solution. Content Engine does not implement its own authentication module but uses the application server's authentication mechanism. Before clients can log in to a Content Engine server, the application server's authentication providers must be configured to point to specified directory servers where security objects, such as realms, groups, and users, are stored.

A directory server is divided into partitions, each of which is called a naming context (or namespace). There are different types of naming contexts, such as the configuration naming context, which holds configuration information, and data naming contexts, which contain all directory data. Each data naming context is defined as a Content Engine realm and each realm contains groups and users.

A user object exists in the Content Engine realm as part of the security interface that allows a user access to a specific Content Engine resource. A group object maps to a set of users and access rights (permissions) are assigned to individual users and/or groups. FileNet implements role based security by mapping permissions to groups as opposed to individual users.

RFDC01

The Contractor's solution shall provide external and internal users access to current and historical provider manuals (e.g., CMS1500, Dental Claims Manual, Institutional Claims manual, Pharmacy Claims Manual and other Agency manuals or provider bulletins related to Medicaid policy and claims processing.

NOTE: Contractor shall not be responsible to create the content of the manuals.

The evoBrix PMIS seamlessly integrates with the FileNet content management solution by IBM, which is Team CNSI's DMS. FileNet will be the repository for all provider support materials, State policies and procedures manuals, training materials, and system generated correspondences. Providers and State staff members can access current and historical manuals through the evoBrix PMIS portal.

Internal Users

IBM FileNet comes with a Content Navigator tool that enables users to access, manage, and use enterprise content across platforms using a standard web browser. Authorized users will be able to upload the manuals into DMS using the Content Navigator tool. They can specify the effective dates for the manuals/documents during the upload process, along with other pertinent metadata that can be used for indexing the documents, as shown in Figure 3.10.14-8. They can define specific document classes that map to different kinds of manuals (e.g., CMS1500, Dental Claims Manual, Institutional Claims manual, Pharmacy Claims Manual and other Agency manuals or provider bulletins related to Medicaid policy and claims processing) with their own set of index parameters that can then be used to search for and retrieve specific types of manuals. They can also access the documents through the evoBrix PMIS portal through a menu option.

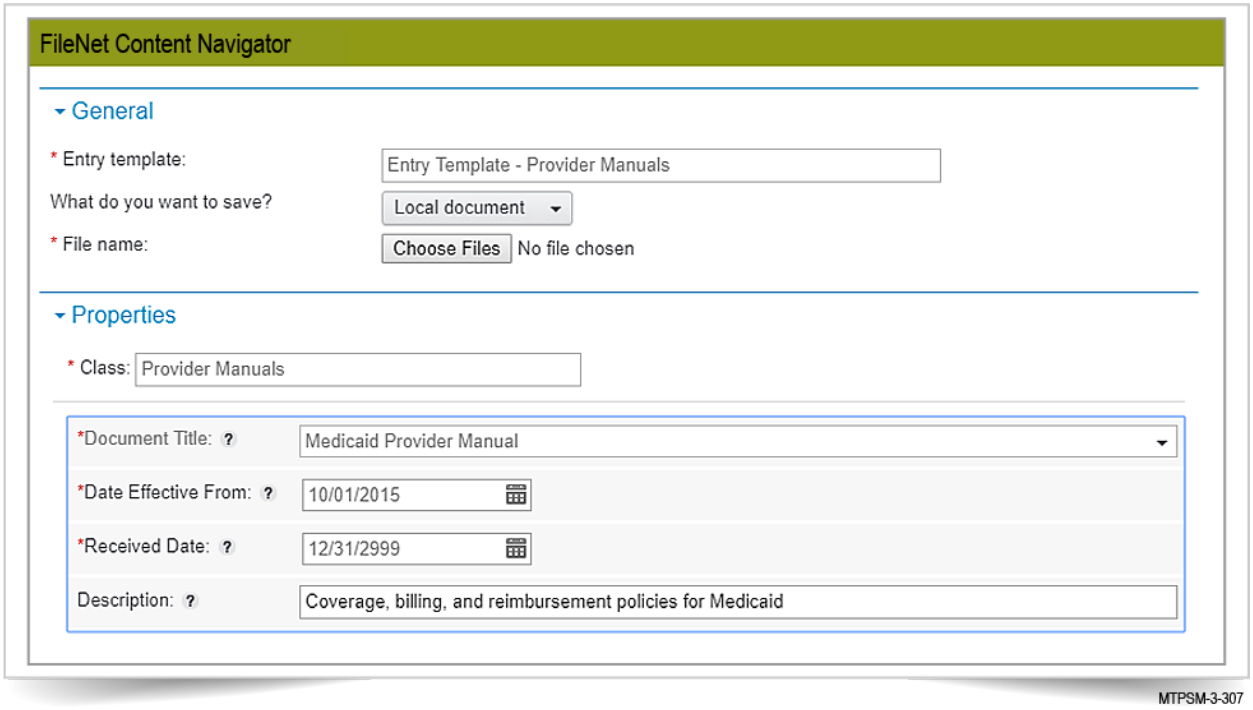


Figure 3.10.14-8. State/Business Operations Staff View Through IBM FileNet Content Navigator. Authorized users can upload provider manuals and specify effective dates for the same.

FileNet supports maintaining the history of changes to a document and helps control the access users have to change the content of a document at a particular point in time. The set of versions for a single document is maintained as a version series. Authorized users have the capability to check-out documents, perform revisions, and check them in, and the changes are maintained through version history. This feature can be leveraged to maintain the historical manuals.

External Users

The provider manuals are made accessible to providers and internal users through a menu option within the evoBrix PMIS portal. They can search for manuals using different criteria such as name, type, and effective dates, as shown in Figure 3.10.14-9.

©2017 CNSI | Option B-14

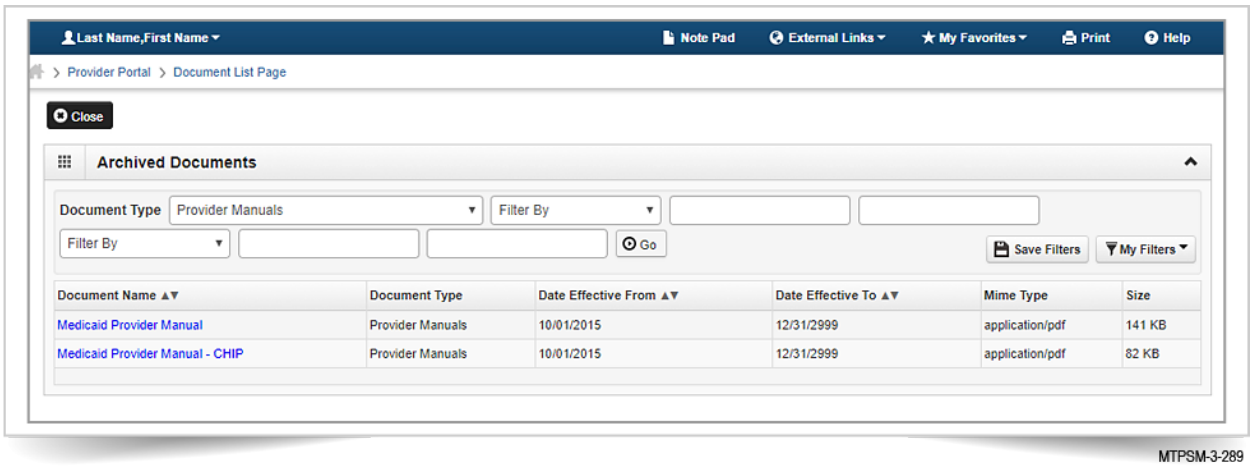


Figure 3.10.14-9. Provider View Through the evoBrix PMIS Portal. Authorized users can search for and view provider manuals from within the portal.

When the user(s) invoke the search functionality within the evoBrix PMIS, the system internally calls the FileNet API to search for the manual within FileNet. The FileNet Java API is an interface-based API that provides access to the full capabilities of the Content Engine. The FileNet P8 Platform also includes web services for the Content Engine, which are compliant with WS-I Basic Profile 1.0 and WS-Security. Using these web services allows us to optimally leverage the functionality of Content Engine APIs for effective document management.

3.10.14.3 Customer Relationship Management

This section outlines the requirements for a Customer Relationship Management Tool. The Offeror's Proposed Option B solutions and services will include providing and utilizing a Customer Relationship Management (CRM) tool in order to manage correspondence with providers. The CRM tool will be able to capture interactions with providers through free-form text, pre-defined data elements, and be capable of searching logged correspondence on command. The CRM tool will support attachments; linking of documents and information within the tool; and routing of correspondence and captured information through the workflow to specific individuals. The Offeror must describe their approach to meet each of the Customer Relationship Management tool requirements defined in Attachment F, Requirements Matrix.

Team CNSI's proposed Customer Relationship Management (CRM) tool enables team CNSI's business operations staff to deliver excellent service to providers as well as manage and analyze provider interactions and data. It consolidates customer information and documents it in a single CRM database so business users can more easily access and manage it. Team CNSI's CRM Siebel Open UI delivers a rich user experience and helps the Customer Service Representative (CSR) agent to better understand and address the needs of the customers in an effective and efficient manner. The CRM Siebel application is in production in

The Team CNSI Advantage

Team CNSI's CRM solution delivers the most comprehensive customer service experience with the goal of servicing provider inquiries and delivering exceptional experiences to provider callers across all channels.

- Presents a comprehensive view of critical information about a customer with powerful search capabilities
- Enables the customer representative to generate the correspondence from any location with the access to the internet
- Extensive usability features to reduce service times through Siebel Open UI
- Reduced call handling times and improved first-call resolution rates
- Secured real-time integration with evoBrix module using Web services
- Organized Hierarchy matrix for controlled access and visibility of data
- Robust computer telephony integration (CTI) and integrated with interactive voice response (IVR)

MTPSM-3-001

the states of Michigan and Washington as part of their MMIS implementations. In the states of Michigan and Washington, respectively, 600 and 180 Call Center personnel use the Siebel application to serve providers and other trading partners. The application provides the CSR a complete, 360-degree view of the caller, including the caller's call history, other correspondence, and key metrics. The application allows multiple inquiry transactions in a single page, reducing overall call handling time and increasing customer satisfaction.

Team CNSI's CRM solution leverages Oracle's Siebel CRM product to create a scalable and integrated CRM system. Our solution incorporates Siebel Open UI as the main CRM component. The CRM solution provides a powerful feature to track the call history. It also facilitates attaching and linking documents to a Service Request.

Figure 3.10.14-10 shows the statistics of Team CNSI's CRM implementation metrics across multiple states in the past five years. Note that calls processed via IVR are counted in the ticket volume.

Team CNSI's CRM Implementations in Other States		
	MI MMIS	**WA MMIS**
Average number of tickets (provider service requests) per month)	6,056	16,519
Real-time Web service integration with MMIS modules	Yes	Yes
Number of providers serviced using contact center	163,836	223,885
Number of service requests originating from Phone channel for providers	353,179	290,569
Number of service requests originating from fax/Web portal/email/IVR/other channels for providers	10,198	700,630

Figure 3.10.14-10. Team CNSI's CRM Statistics. Service request throughput statistics across various types of service delivery in the last five years for the states of Michigan and Washington.

The CRM system integrates provider, facilities (Organizational Providers/Plans), customer support, and other MMIS information to facilitate researching provider inquiries without requiring a separate sign-on, toggling between the systems, or dual entry of information. The solution provides the ability to document and track caller information such as caller demographics including other critical elements of a call tracking system such as status, type, and resolution. The system provides the ability to link a service request to another service request to relate the information in the system. It also provides the ability to display and upload the related correspondence history of a provider with respect to a service request. Team CNSI's CRM solution enables comprehensive usability features for users to manage and track interactions with providers.

The CRM Business Architecture Schematic is shown in Figure 3.10.14-11.

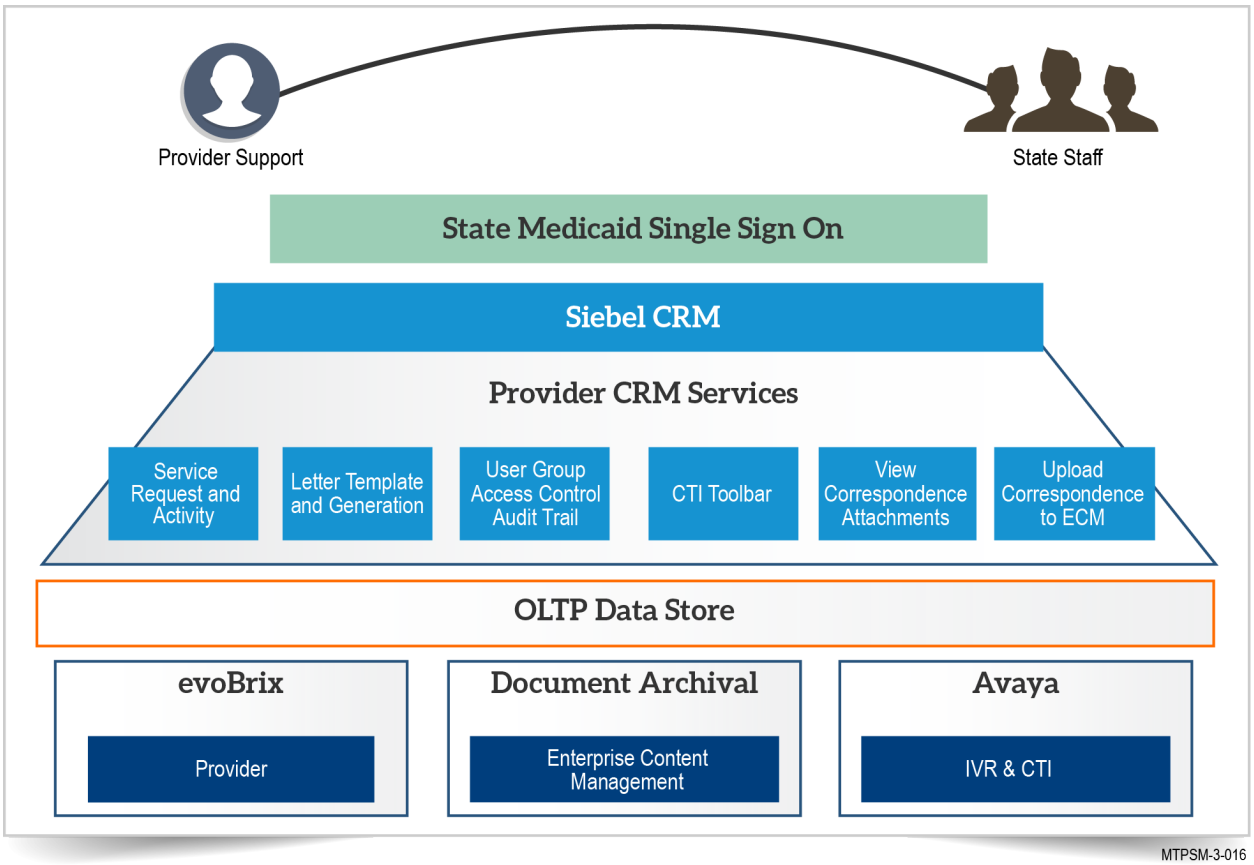


Figure 3.10.14-11. CRM Business Architecture. CRM MITA business architecture specifies functionality, triggers, shared data, and results.

Technical Components and Advantages

The following sections describe the major components of our solution and highlight the unique features of our CRM Siebel Application.

The key CRM components leveraged for meeting the requirements are:

- Siebel CRM SOA

  Team CNSI's CRM tool delivers extensive new pre-built, SOA-enabled, highly scalable web services for critical CRM business processes and components. The CRM system interfaces with the evoBrix Provider Management Information System (PMIS) to provide secured access to data through Oracle Service Bus (OSB) layer.

- Siebel CRM Assignment Manager

  Team CNSI's CRM Assignment Manager routes business entities and work items to the most appropriate candidates by enforcing business rules set by service organizations. Assignment Manager does this by matching candidates (that is, employees, positions, and organizations) to predefined and user-configurable assignment objects. Assignment Manager can be used to automatically assign Siebel entities such as service request activities to the appropriate CSR.

- Siebel CRM Enterprise Integration Manager

  Team CNSI's CRM Enterprise Integration Manager (EIM) is used to import and update provider and facilities information in the CRM tool from the evoBrix PMIS application.

- Siebel User Security and Access

  CRM responsibilities restrict CRM page access to only authorized users. Responsibilities controls access to the views whereas Position controls access to data. Siebel can be integrated with Single Sign On (SSO) and can seamlessly connect to the application using secured LDAP authentication.

- Computer Telephony Integration:

  The IVR telephony infrastructure uses a high-availability, real-time interface with the CRM system and evoBrix PMIS to accomplish the following:

  - Create tickets in the CRM system for all calls
  - Track caller actions within the IVR system and report them to the CRM application
  - Authenticate callers with information provided by the caller against the CRM tool and evoBrix PMIS data store
  - Retrieve and playback information requested by the caller by fetching the most current data from evoBrix PMIS and the CRM system
  - Caller information is passed on, so that the customer service representative has the relevant caller information available

CRM01

The Contractor's solution shall provide the capability to automatically alert external entities (e.g., managed care companies and financial management companies for self-directed care) and other Agency users about their providers' enrollment status and enrollment status changes.

Team CNSI's solution provides the ability to automatically alert external entities and other State Agency users about provider enrollment status and enrollment status changes, including managed care companies and financial management, through the evoBrix ISR solution. The evoBrix ISR solution sends the provider enrollment status file via File Exchange Process by leveraging ESB features. Team CNSI's solution has a pre-built interface called Provider Enrollment Update for communicating enrollment status and changes to external entities. For additional details on the evoBrix ISR solution, please see section 3.10.1.6 Interfaces.

CRM02

The Contractor shall provide a voice messaging system for after hours callers indicating the hours of operation and provide options for leaving messages.

Team CNSI's Call Center solution enables the voice messaging system using the Avaya Modular Messaging system. When a caller calls after normal hours of operation, the IVR system sends the call to a pre-configured voicemail box. The voice messaging system greets the caller with a prerecorded after-hours message and then requests that the caller leave a voice message. Once the caller records the message, the message is stored along with the incoming phone number of the caller. The stored after-

hours messages can later be retrieved by the CSR using a message access number. The Avaya Modular Messaging system also allows the caller to leave a personalized message to a specific CSR, if the caller already knows the extension of the representative.

CRM03

The Contractor shall establish and maintain a toll-free telephone number for the call center.

Team CNSI will establish and maintain a toll-free telephone number (TFN) for the call center. The providers are greeted by a unique menu of available options by the integrated IVR system. The IVR determines the correct menus to be used based on the TFN, which will be included in the implementation solution.

CRM04

The Contractor shall use Computer Telephone Integration (CTI) to provide personalized routing and work-object handling based upon identifiers received from the caller regarding language, inquiry area, and ability to produce reports on both electronic and voice transactions.

Team CNSI's CRM tool provides an integrated CTI Toolbar, which acts as a middle layer that connects the IVR and the agents to the CRM Application. The CTI Toolbar helps the CSR manage telephone calls using call controls within CTI rather than using dedicated hard phones. The CSR can accept, transfer, or hold the call. An automatic screen of key customer dashboard data is displayed to the as soon as a call is accepted. The softphone controls the availability of the CSR for skill-based routing, including language, inquiry area, and skill level. The CSR can also complete after-call work related to a recent call and can choose when he or she is ready to start accepting new calls. The CSR can also make outbound calls using the softphone, which can be easily documented in the CRM tool.

The CTI enablement using Avaya IVR and Siebel is depicted in Figure 3.10.14-12.

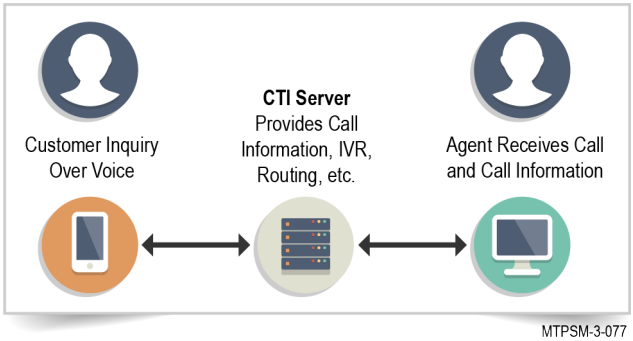


Figure 3.10.14-12. CRM IVR Transfer Process Overview. CRM represents the call routing from IVR to Siebel CRM.

Service requests and activities are used to track all interactions with providers and are reportable through online inquires or established reports. Team CNSI's Avaya solution supports interactive logging of all transactions and the comprehensive ability to report call statistics. The reports available can broadly be categorized into two types as described in Figure 3.10.14-13. The listed reports provide a 360-degree view of the Call Center performance. Additional reports can be configured as per the State's need during the solutioning session.

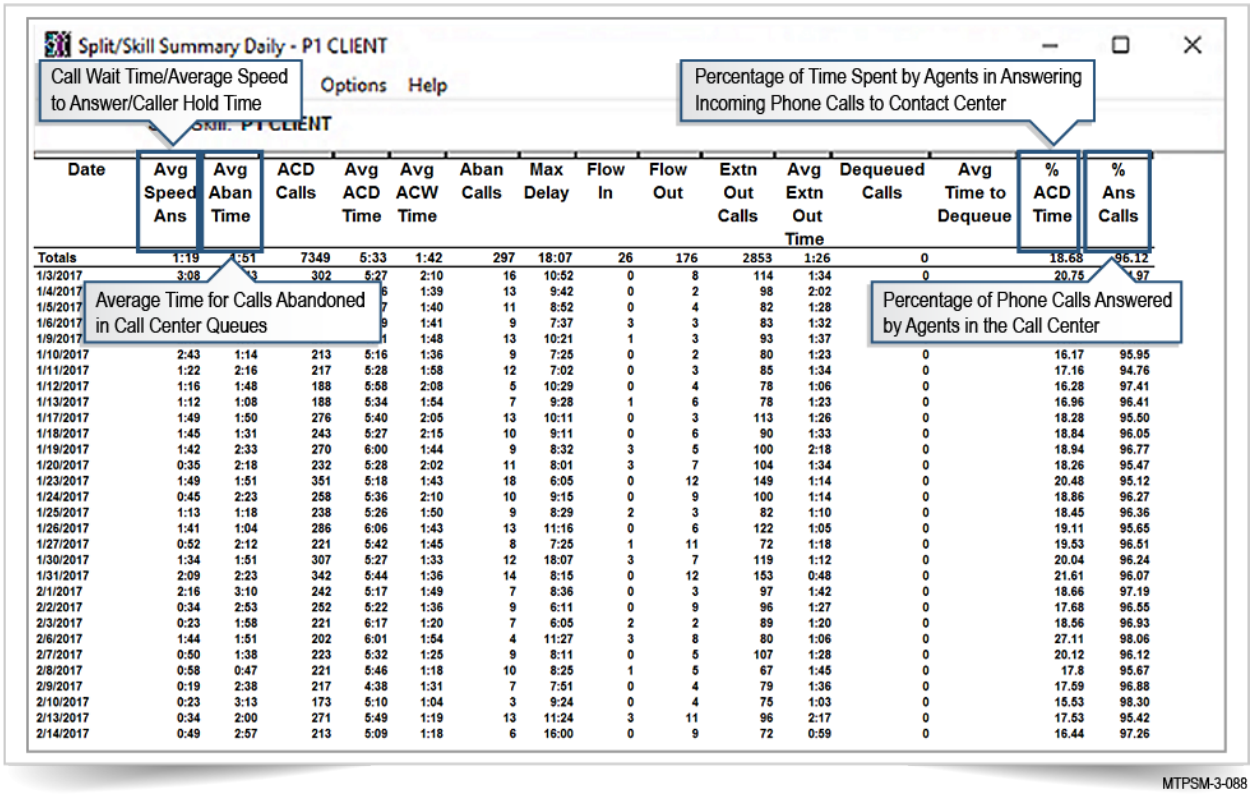
Report Type	Description	Report Names
Avaya CMS/Call Center Reports	Provide details on the overall functioning of the call center. Avaya CMS reports can be real-time reports, historical reports, or integrated (combination or real time and historical) reports.	■ Skill Status Report ■ Agent Group Report ■ Daily Summary Report ■ Agent Graphical Information Report

Report Type	Description	Report Names
	Additional reports can be configured as defined during solutioning activities.	■ Skill Comparison Report
Avaya Aura Experience portal/IVR Reports	Provide details on all the transactions that are performed during the IVR calls and overall performance of the IVR systems. These reports can be generated on a pre-defined schedule or on demand.	■ Application Summary Report ■ Application Detail Report ■ Call Summary Report ■ Call Detail Report ■ Session Detail Report ■ Performance Report ■ Active IVR Calls Report ■ System Monitor Report

Figure 3.10.14-13. Call Center Reports. Lists various report available in Team CNSI's IVR and Call Center Solution.

CMS reports provide in-depth details about Call Center performance. These reports can be used to find the call abandonment rate, average time prior to abandonment, and calls placed on hold, along with other details such as percentage of calls answered within set service levels, how many calls were handled, and summarizing activity. Reports can be obtained for a single skill or multiple skills. Reports can also be obtained for any timeframe such as hourly or daily.

Reports can provide information on call abandonment rate and average time prior to abandonment, including for calls placed on hold. Figure 3.10.14-14 shows a daily summary report for a single skill over a 30-day period.



Date	Avg Speed Ans	Avg Aban Time	ACD Calls	Avg ACD Time	Avg ACW Time	Aban Calls	Max Delay	Flow In	Flow Out	Extn Out Calls	Avg Extn Out Time	Dequeued Calls	Avg Time to Dequeue	% ACD Time	% Ans Calls
Totals	1:19	:51	7349	5:33	1:42	297	18:07	26	176	2853	1:26	0		18.68	96.12
1/3/2017	3:08	:3	302	5:27	2:10	16	10:52	0	8	114	1:34	0		20.75	.97
1/4/2017					1:39	13	9:42	0	2	98	2:02				
1/5/2017					1:40	11	8:52	0	4	82	1:28				
1/6/2017					1:41	9	7:37	3	3	83	1:32				
1/9/2017					1:48	13	10:21	1	3	93	1:37				
1/10/2017	2:43	1:14	213	5:16	1:36	9	7:25	0	2	80	1:23	0		16.17	95.95
1/11/2017	1:22	2:16	217	5:28	1:58	12	7:02	0	3	85	1:34	0		17.16	94.76
1/12/2017	1:16	1:48	188	5:58	2:08	5	10:29	0	4	78	1:06	0		16.28	97.41
1/13/2017	1:12	1:08	188	5:34	1:54	7	9:28	1	6	78	1:23	0		16.96	96.41
1/17/2017	1:49	1:50	276	5:40	2:05	13	10:11	0	3	113	1:26	0		18.28	95.50
1/18/2017	1:45	1:31	243	5:27	2:15	10	9:11	0	6	90	1:33	0		18.84	96.05
1/19/2017	1:42	2:33	270	6:00	1:44	9	8:32	3	5	100	2:18	0		18.94	96.77
1/20/2017	0:35	2:18	232	5:28	2:02	11	8:01	3	7	104	1:34	0		18.26	95.47
1/23/2017	1:49	1:51	351	5:18	1:43	18	6:05	0	12	149	1:14	0		20.48	95.12
1/24/2017	0:45	2:23	258	5:36	2:10	10	9:15	0	9	100	1:14	0		18.86	96.27
1/25/2017	1:13	1:18	238	5:26	1:50	9	8:29	2	3	82	1:10	0		18.45	96.36
1/26/2017	1:41	1:04	286	6:06	1:43	13	11:16	0	6	122	1:05	0		19.11	95.65
1/27/2017	0:52	2:12	221	5:42	1:45	8	7:25	1	11	72	1:18	0		19.53	96.51
1/30/2017	1:34	1:51	307	5:27	1:33	12	18:07	3	7	119	1:12	0		20.04	96.24
1/31/2017	2:09	2:23	342	5:44	1:36	14	8:15	0	12	153	0:48	0		21.61	96.07
2/1/2017	2:16	3:10	242	5:17	1:49	7	8:36	0	3	97	1:42	0		18.66	97.19
2/2/2017	0:34	2:53	252	5:22	1:36	9	6:11	0	9	96	1:27	0		17.68	96.55
2/3/2017	0:23	1:58	221	6:17	1:20	7	6:05	2	2	89	1:20	0		18.56	96.93
2/6/2017	1:44	1:51	202	6:01	1:54	4	11:27	3	8	80	1:06	0		27.11	98.06
2/7/2017	0:50	1:38	223	5:32	1:25	9	8:11	0	5	107	1:28	0		20.12	96.12
2/8/2017	0:58	0:47	221	5:46	1:18	10	8:25	1	5	67	1:45	0		17.8	95.67
2/9/2017	0:19	2:38	217	4:38	1:31	7	7:51	0	4	79	1:36	0		17.59	96.88
2/10/2017	0:23	3:13	173	5:10	1:04	3	9:24	0	4	75	1:03	0		15.53	98.30
2/13/2017	0:34	2:00	271	5:49	1:19	13	11:24	3	11	96	2:17	0		17.53	95.42
2/14/2017	0:49	2:57	213	5:09	1:18	6	16:00	0	9	72	0:59	0		16.44	97.26

Figure 3.10.14-14. Daily Summary Report. Displays an overview of the daily summary report for a range of days in a specific skill in the Call Center.

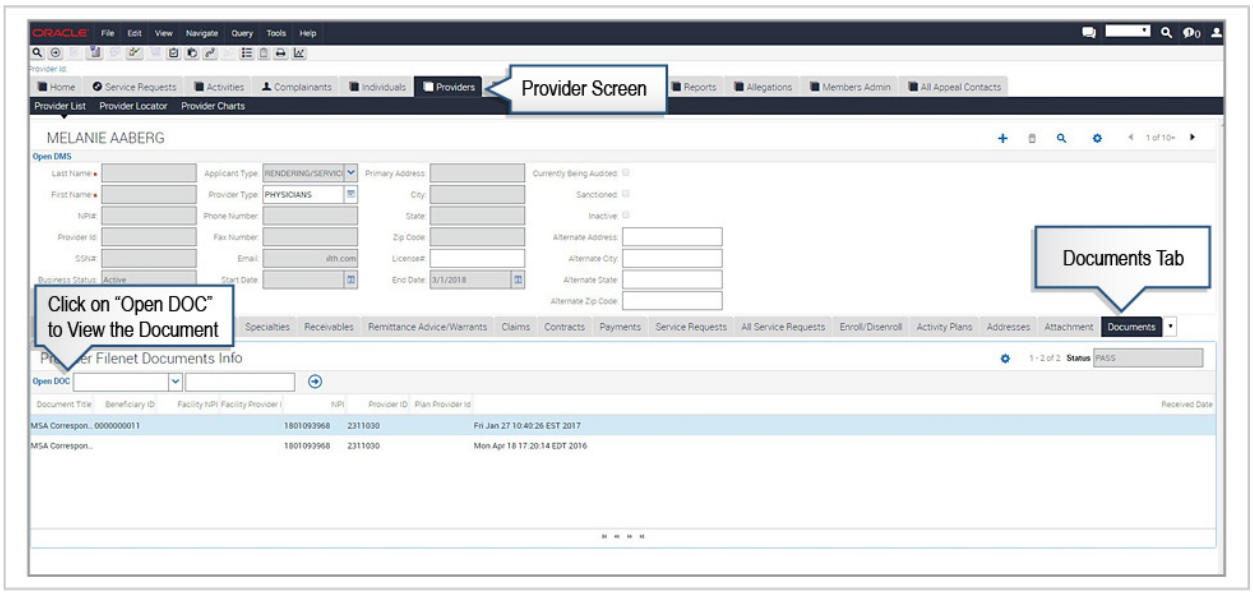
©2017 CNSI | Option B-20

CRM05

The Contractor shall provide, configure and maintain an automated call and contact tracking system (CRM tool) for all calls and correspondence received.

Service Request Tracking

Team CNSI's CRM solution has a service request module, which is used to manage and track provider, facilities, and other stakeholder inquiries. Each service request has a unique identifier, the Service Request ID (SR ID), which is auto-generated in the CRM application when a new service request record is created, either manually by a CSR using the CRM tool, or real-time via a CRM Web services invocation or using batch jobs. A service request can be categorized based on area, type, and reason. The designated user can work on each request and assign the request to another user within the business unit or organization. All related correspondence of a provider is displayed in the Service Request Documents View, shown in Figure 3.10.14-15.



MTPSM-3-357

Figure 3.10.14-15. Service Request Documents View. Displays related correspondence of a provider.

The Service Requests screen displays diverse options based on the ownership and organization hierarchy. These views pages are:

- My Service Requests
- My Team's Service Requests
- All Service Requests

The Service Requests view shown in Figure 3.10.14-16 displays the List and Detail information of the record.

©2017 CNSI | Option B-21

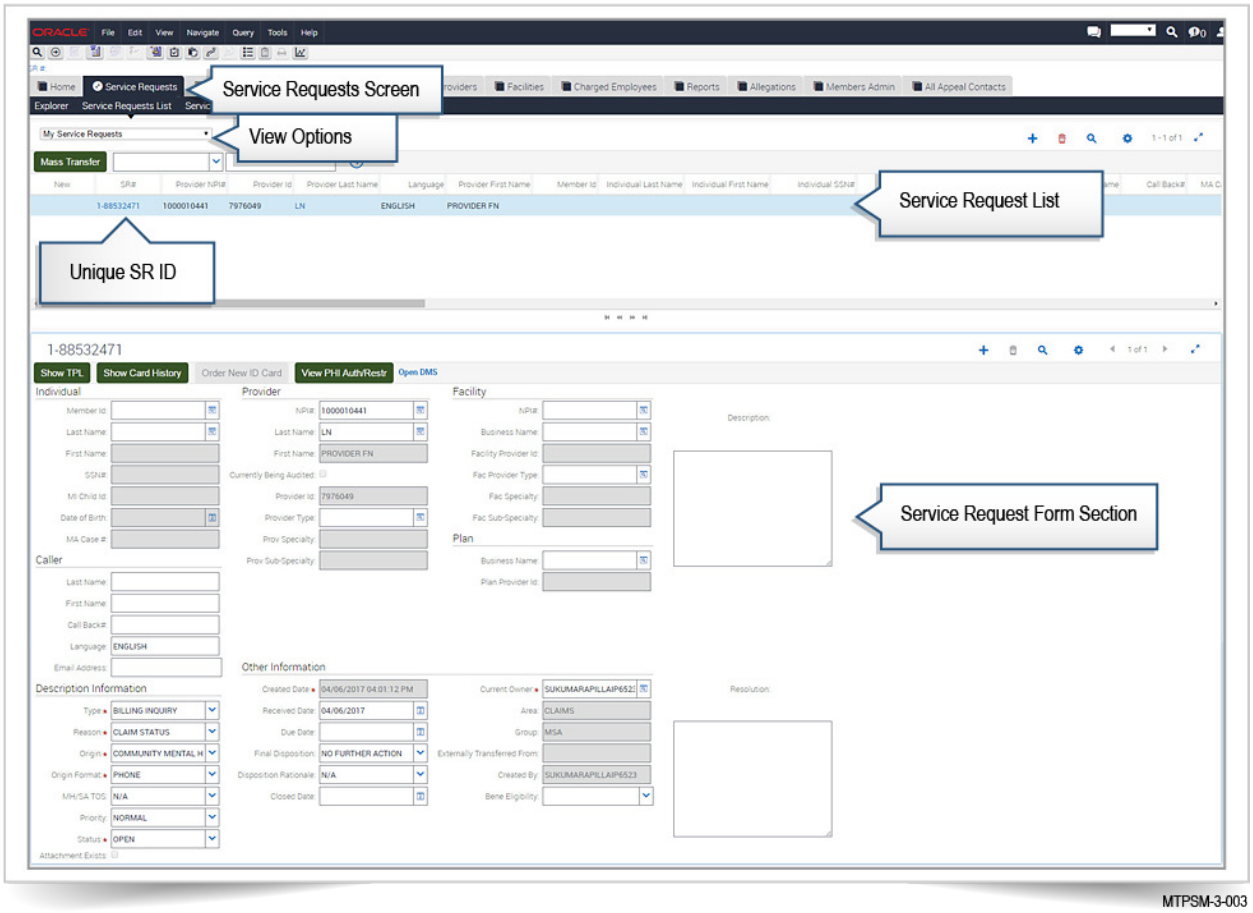


Figure 3.10.14-16. CRM Service Requests View. Service requests allow a user to track the provider, facilities, and caller information.

Activity Tracking is a child entity of a service request which tracks the multiple tasks related to a service request in an organized manner, as depicted in Figure 3.10.14-17.

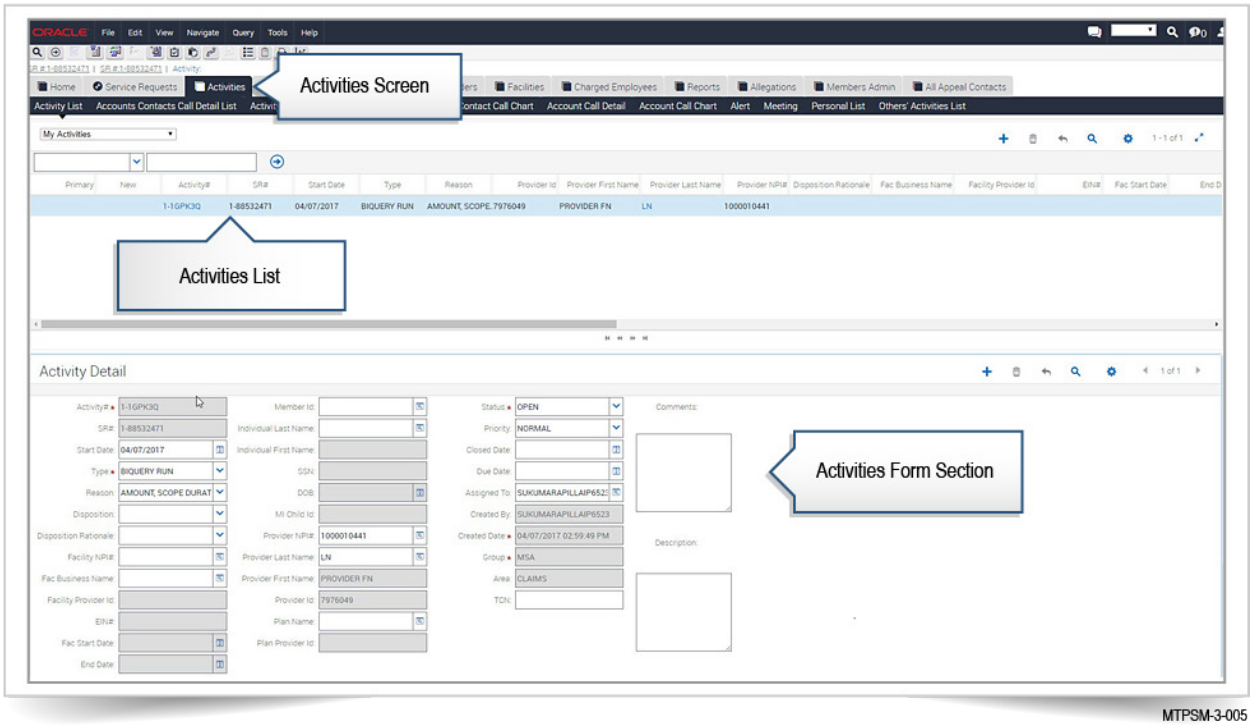


Figure 3.10.14-17. CRM Activities View. Activities allow the capture of detailed information and tracking of transactions, escalations, tasks, and action items.

CRM06

The CRM tool must log and track information for each call that includes at a minimum the following elements:

a. time of call
b. date of call
c. identifying information on caller
d. representative ID
e. call type
f. call category
g. inquiry description
h. ticket status
i. response description
j. call reference number

Team CNSI's CRM solution provides the ability to log and track information for each call in the Service Requests, using data fields as listed in Figure 3.10.14-18.

Call Log Information Comparison	
Fields in Requirement	**Fields Provided in Solution**
Time of Call	Service Request Created Time
Date of Call	Service Request Created Date
Identifying Information of Caller	Provider Name, NPI #, Provider ID, Other Caller Information
Representative ID	Current Owner

Call Log Information Comparison	
Fields in Requirement	**Fields Provided in Solution**
Call Type	Service Request Type
Call Category	Service Request Reason
Inquiry Description	Service Request Description
Ticket Status	Service Request Status
Response Description	Service Request Resolution
Call Reference Number	Service Request Number

Figure 3.10.14-18. Call Log Information. List of call log information that is offered by Team CNSI's solution in response to MT PSM requirements.

Additionally, there are fields such as Area, Origin, Origin Format, Source, Priority, Severity, Closed Date, Owner, Resolution, and Description. Call resolution information can be entered in the Resolution and Description fields. There are IVR specific fields in a Service Request record that capture the call duration, caller type, IVR start time, IVR end time, caller phone number, and IVR transfer reason.

CRM07

The Contractor's CRM tool shall have the ability to link the CRM record and the workflow tool to automatically route appropriate tickets to the State for review.

Team CNSI's CRM solution can be configured to automatically enable routing of service requests and activities based on certain criteria to CSRs using CRM Assignment Manager. The automated assignment manager workflow is applicable for all CRM users, including all State users and Call Center agents. CSRs can also manually assign a new owner to a service request based on the area.

The CRM Assignment Manager routes work items, such as service requests, to the most appropriate candidates by enforcing business rules, as illustrated in Figure 3.10.14-19. Assignment Manager accomplishes this function by matching candidates (that is, staff members, positions, and organizations) to predefined and user-configurable assignment objects. To assign the most qualified candidate to each object, Assignment Manager applies assignment rules that are defined for each candidate. Assignment criteria and rules can be defined to automatically assign service requests to CSRs. Figure 3.10.14-20 depicts the CRM Responsibilities Administration view. CRM positions restrict data access to authorized users.

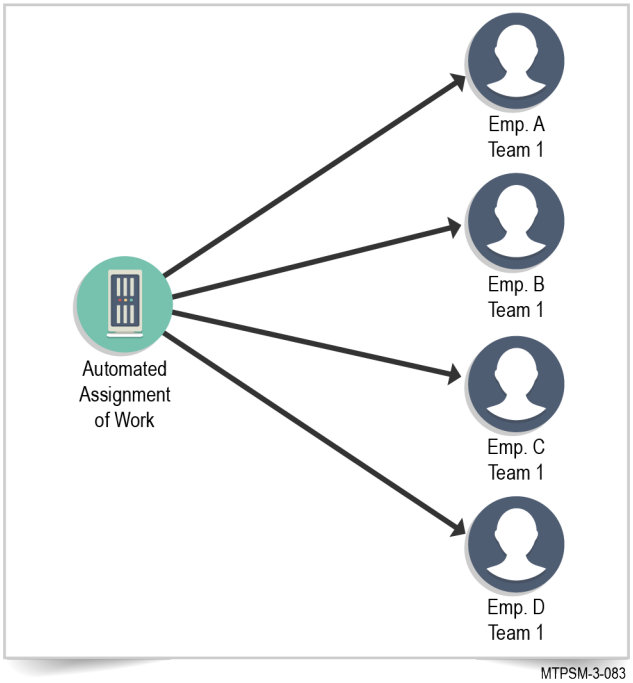


Figure 3.10.14-19. CRM Siebel Assignment Manager. This overview represents the auto assignment of Service Request to the employee based on their skillset.

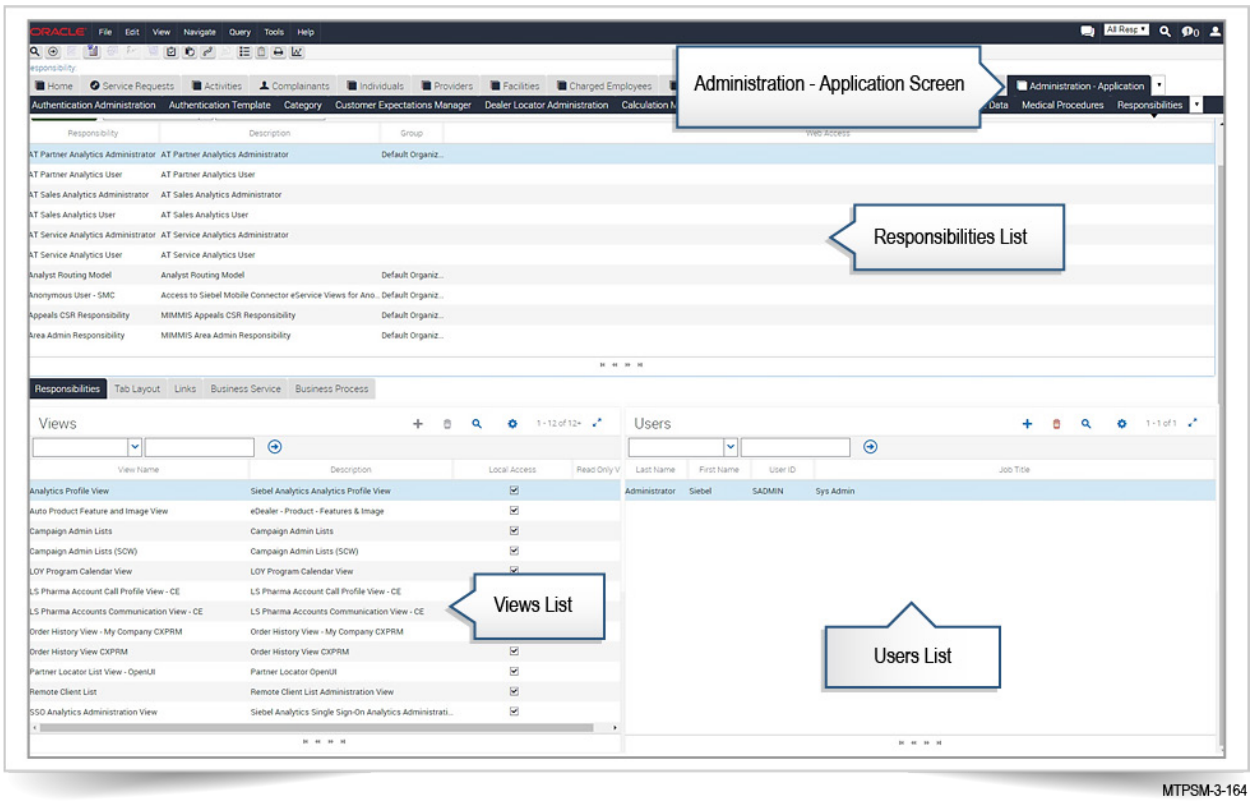


Figure 3.10.14-20. CRM Responsibilities Administration View. Our solution provides comprehensive CRM-related administration capabilities for centrally managing page access.

Siebel Notifications

CRM Workflows can also be configured to create activity or email alerts for supervisory staff if the required service level metrics are not met. It facilitates the enhanced monitoring on the management of service requests and activities.

As shown in Figure 3.10.14-21, the CRM tool monitors and sends an email notification to the business owner to resolve the Service Request before the due date.

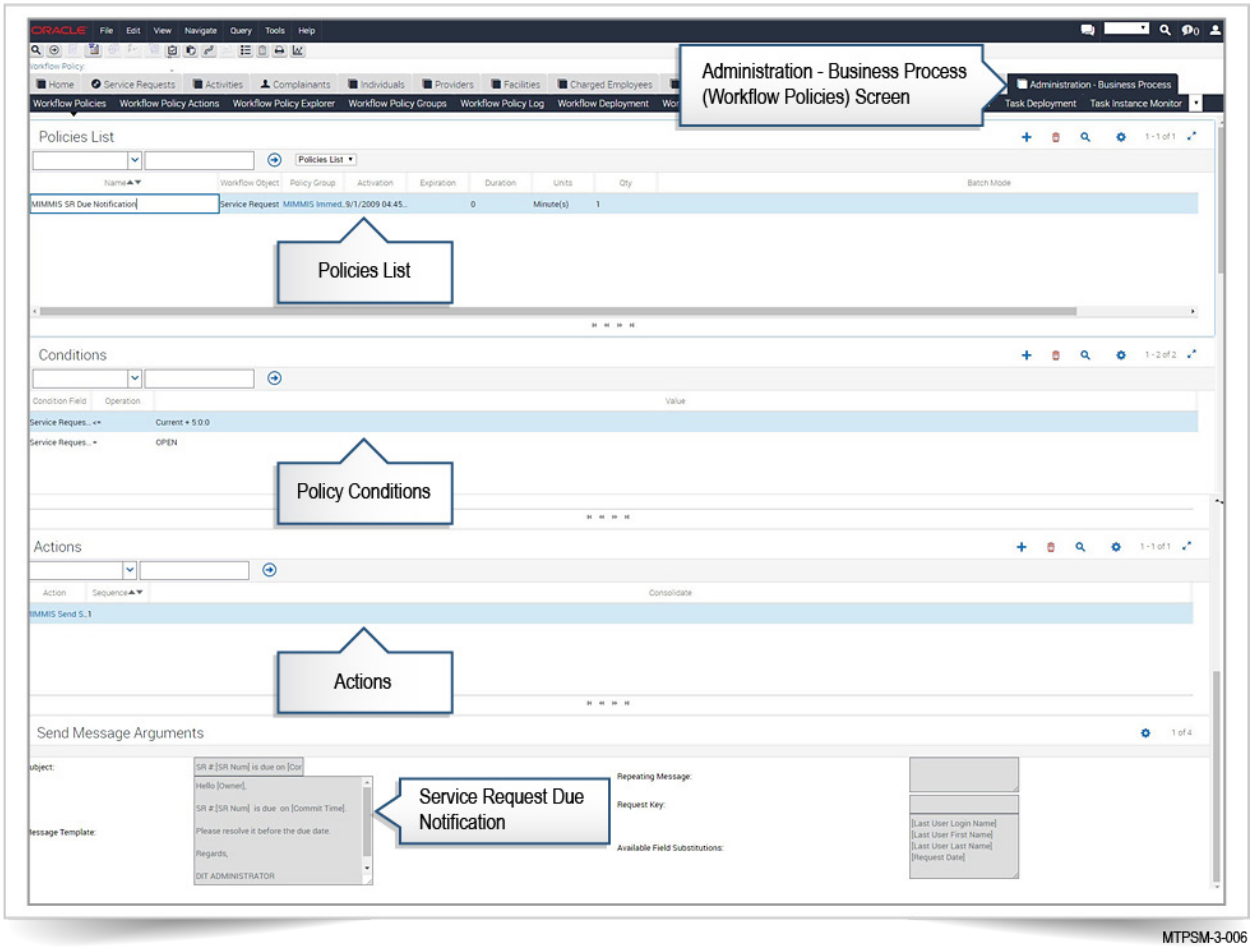


Figure 3.10.14-21. CRM Notification. The system sends an email to the user to resolve the open Service Request before the due date.

CRM08

The Contractor's CRM tool shall have the ability to link related CRM tickets.

Team CNSI's CRM solution provides the functionality to relate a Service Request to another Service Request. This Related Service Request exists as a view tab under a Service Request. The CSR can view if there is any history of related service requests created for the caller. This tab provides assorted options under this view tab that displays the "Child" and "Parent" service requests where the CSR can link service requests as "child" of another. If the user identifies a service request duplicate or same kind of another, this functionality helps the user to link both SRs so that it can process/track easily. The CSR can easily remove the link of a Child Service Request by deleting the child record from the Related Service Requests view. Figure 3.10.14-22 shows the CRM representing Related Service Requests in a Service Request screen.

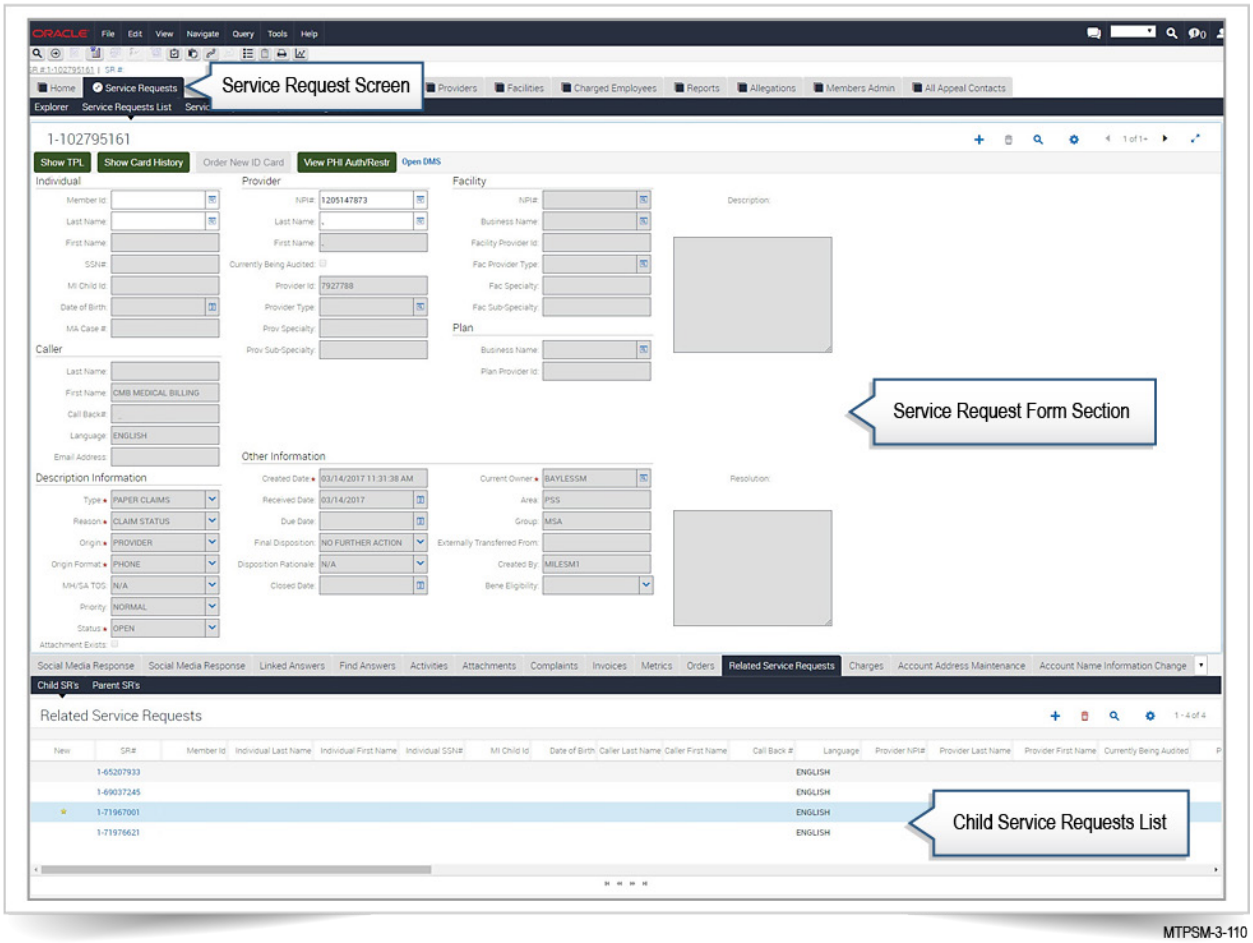


Figure 3.10.14-22. CRM Related Service Requests. The CRM tool is able to link a Service Request to another Service Request.

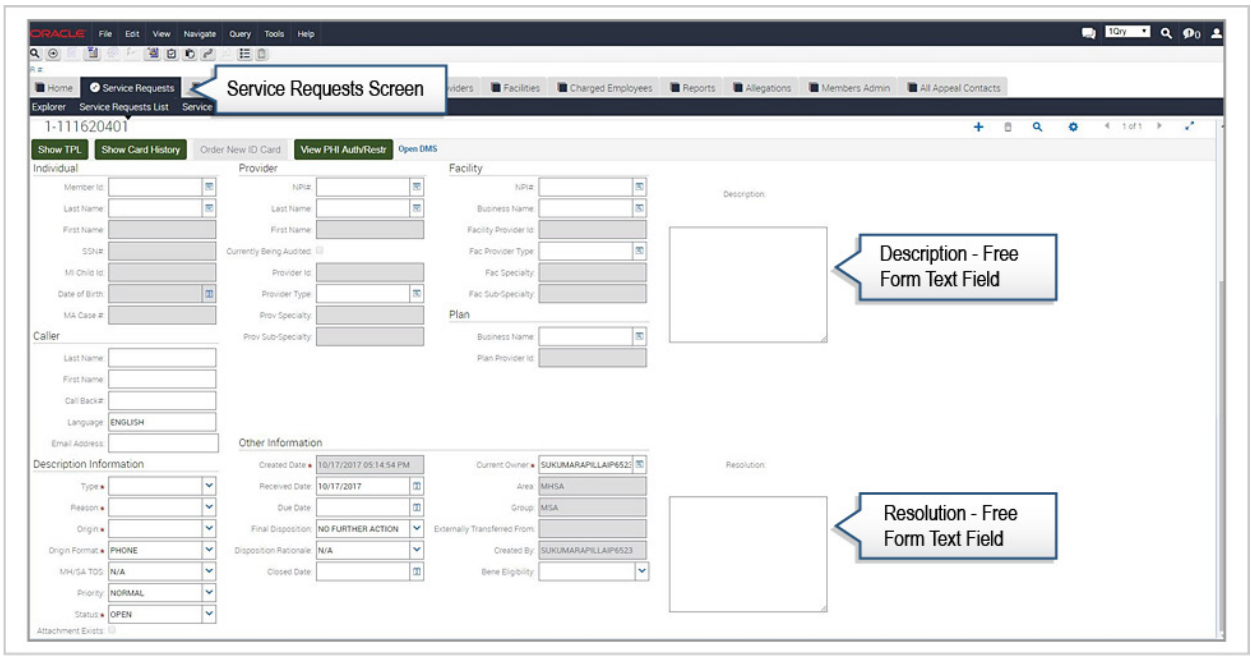
CRM09

The Contractor's CRM tool shall have the ability to include a free form text field for each CRM ticket for comments and/or resolution.

Team CNSI's CRM solution Service Request module provides free-form text boxes to capture critical information such as resolution and description. The CSR can copy any text or input values up to 2000 characters.

Figure 3.10.14-23 shows the free-form text field on a Service Request screen.

©2017 CNSI | Option B-27



MTPSM-3-355

Figure 3.10.14-23. Free-form Text Input Tool. This screenshot shows the CRM tool that allows the user to input a free-form text field in the Service Request List.

CRM10

The Contractor's CRM tool shall have the ability to provide for online display, inquiry, and updating of call records with access, including, but not limited to, call type, API or NPI number, inquirer's name, representatives ID or name, provider name, or a combination of these data elements.

Team CNSI's CRM Inquiry Tracking Service Request and activity record captures and displays critical information as follows:

- Caller information that includes key elements such as NPI, Provider ID, and call duration
- The status of the service request with end to end integrated life cycle information

The CSR can drill down on the SR ID to navigate to detailed views related to a service request. Service Request Activities displays all the linked activities. Figure 3.10.14-24 shows the CRM Service Requests Activities view.

©2017 CNSI | Option B-28

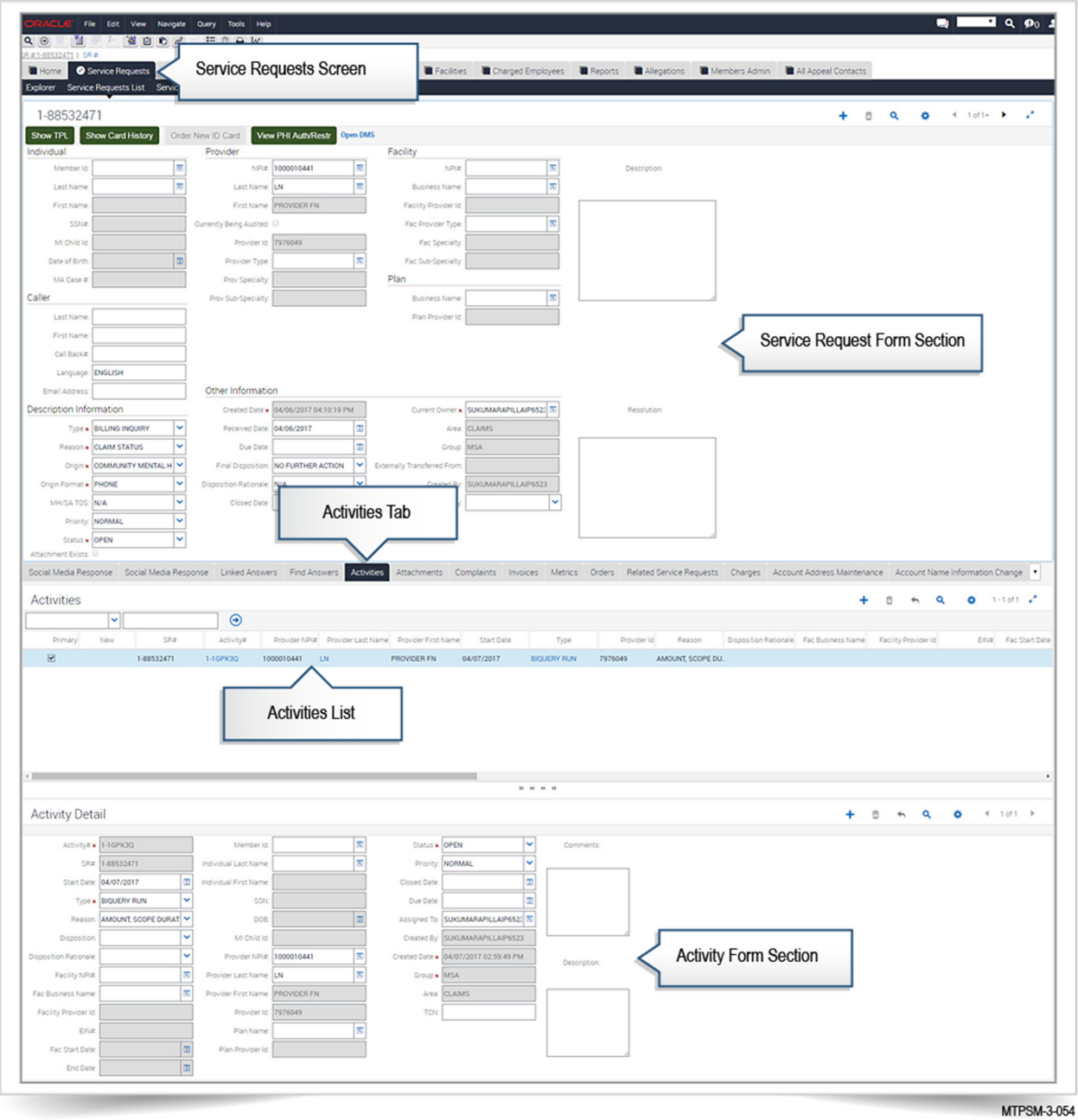


Figure 3.10.14-24. CRM Service Requests Activities View. Displays CRM transactions, action items, and escalations against specific service requests for the associated provider, facilities, or contact providing CSRs with a detailed snapshot for a ticket.

CRM11

The Contractor's CRM tool shall have the ability to provide State resources or designated resources local and remote access to the CRM system.

Team CNSI's CRM solution provides State or other designated staff with online access to the CRM application along with high security access profile model.

- No additional application software is required to access the application except a standard web browser.
- Built in access control protocols ensure that the designated staffs access only his/her data.
- The integration modules are highly secured and provide access to the user to view the real-time data from evoBrix PMIS solution.
- The audit trail feature on a Service Request provides a powerful history tracking of a service request data on add, update, or delete operations. The access profile can be set accordingly so that the designated staff are accessing the audit data to ensure the quality of the tracking data.

Access Control

Team CNSI's CRM solution has a powerful access control, which is the term used to describe the set of Siebel application mechanisms that control user access to data and application functionality.

The Responsibility screen maintains the access to all the views in the application. A user's access to a view depends on the CSR responsibility. Refer to Figure 3.10.14-20 which depicts the CRM Responsibilities Administration view. CRM positions restrict data access to authorized users.

Positions are designations defined in a division. These designations are set up in a hierarchical structure to restrict data visibility. Positions are assigned to a user in the system for a division. A user can have more than one position. A user's access to data depends on his or her position in the system.

Figure 3.10.14-25 depicts the CRM Position Administration view. Every CRM user is assigned responsibilities and positions to enforce authorized access to the CRM application.

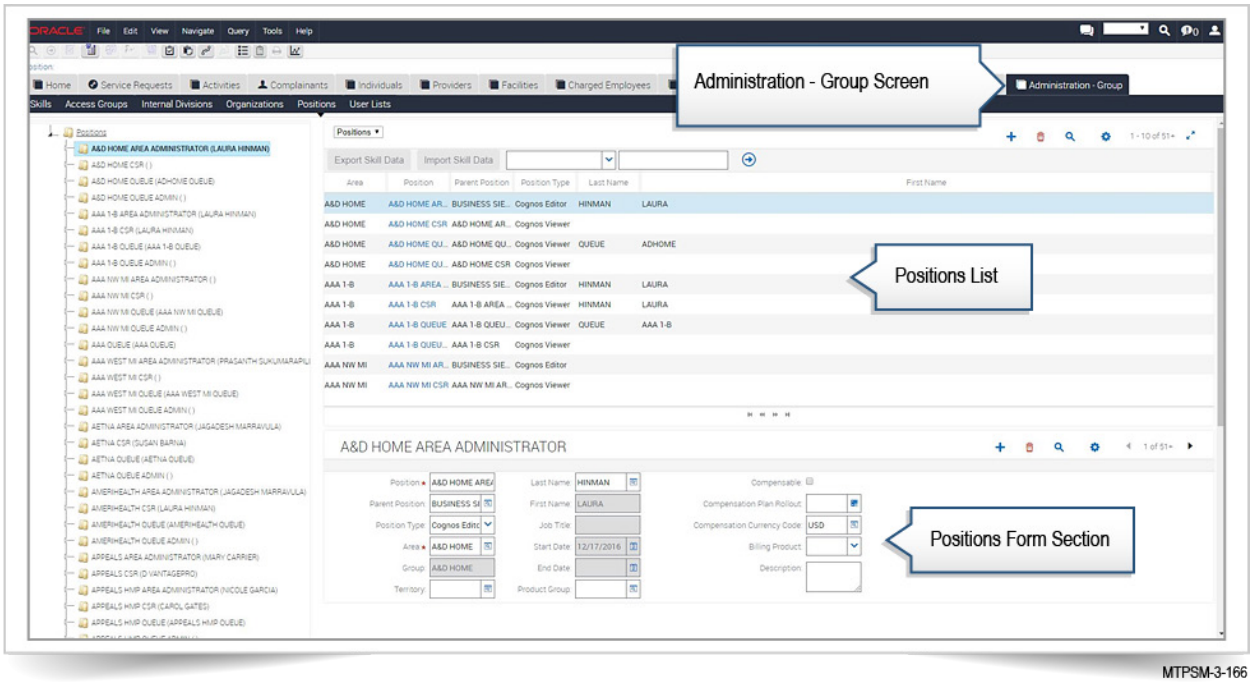


Figure 3.10.14-25. CRM Position Administration View. Our solution provides comprehensive CRM administration capabilities for centrally managing record level access.

Every application user is defined as an employee in the system. A user always has one responsibility and position defined. All new users are by default set with New User Responsibility and Position in the system.

©2017 CNSI | Option B-30

Figure 3.10.14-26 depicts the CRM Employee Administration view.

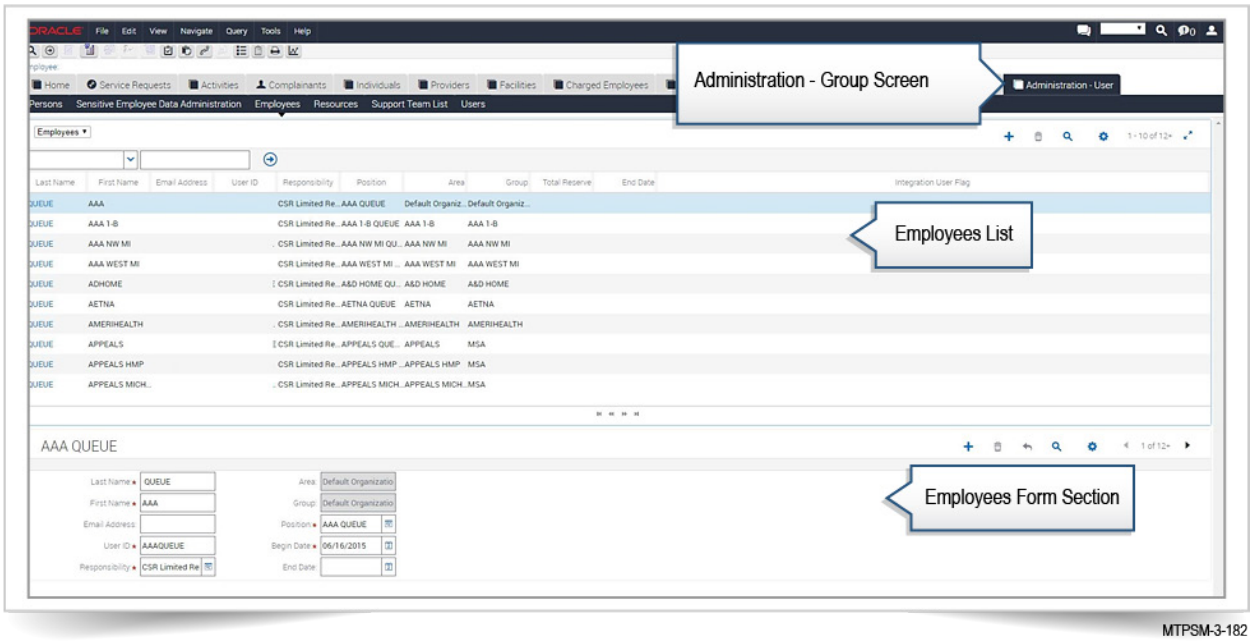


Figure 3.10.14-26. CRM Employee Administration View. Employee administration encompasses evoBrix PMIS crosswalk information used during evoBrix Web Service and Direct Application Access usage, avoiding dual-logins and providing a secured access to evoBrix PMIS information.

Audit Trail

Team CNSI's CRM solution provides an audit trail feature that creates a history of the changes that have been made to data in Siebel Business Applications. An audit trail is a record showing who has accessed an item, which operation was performed, when it was performed, and how the value was changed. Therefore, it is useful for maintaining security, examining the history of a specific record, documenting modifications for future analysis, and record keeping. Siebel Audit Trail logs information without requiring any interaction with, or input from, the users.

Critical fields of the service request can be audited for tracking changes, as shown in Figure 3.10.14-27.

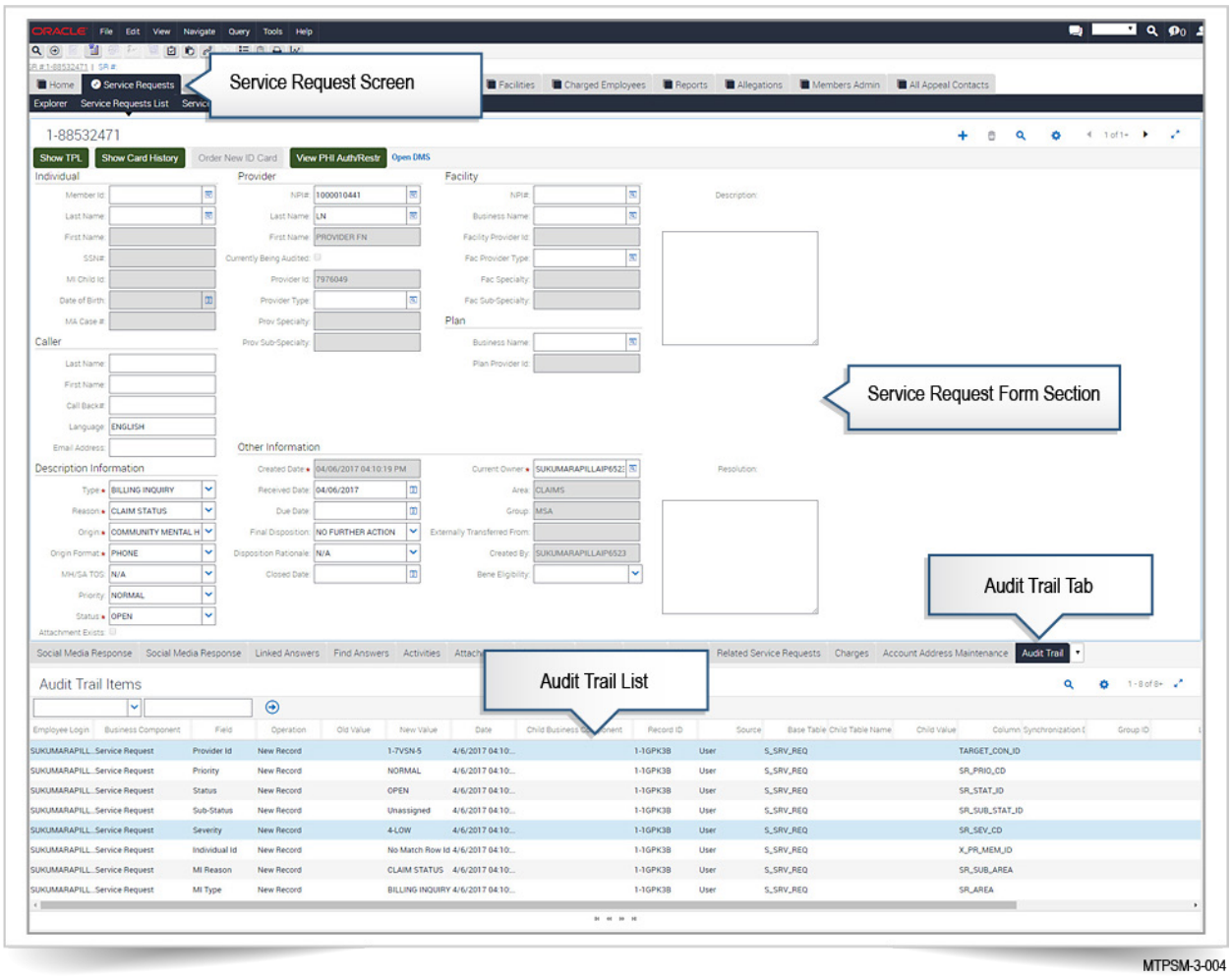


Figure 3.10.14-27. CRM Service Requests Audit Trail View. The Audit Trail list captures insert and update information along with user ID, date, and time.

CRM12

The Contractor's CRM tool shall have the ability to utilize CTI to auto-populate CRM screens with caller's basic information and access to contact history.

Team CNSI's CRM tool provides a wide variety of fields as part of the service request and activity modules to capture detailed contact information. The CRM tool is integrated with the IVR system using CTI. CTI provides automatic work object handling and routing of caller information to the CSR servicing the call. Team CNSI's solution leverages Oracle's configured Siebel, Avaya Enablement Service (AES) for Siebel, and IVR solution to provide optimized work-object handling based upon identifiers received from the caller regarding language area

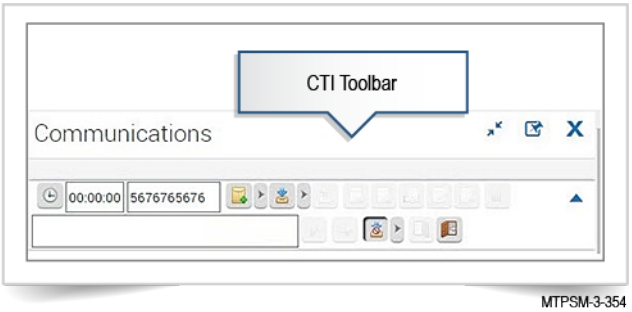


Figure 3.10.14-28. CTI Toolbar. CRM Siebel CTI Toolbar represents the call pop feature for agents.

©2017 CNSI | Option B-32

of inquiry, and auto populates the caller data on Service Request and activities. The CRM Communications Toolbar, shown in Figure 3.10.14-19 on the preceding page, is a state-of-the-art softphone that enables CRM users to execute CTI commands using the CRM Web client. CRM communication toolbar supports functionality including login/logout of softphone, offline work codes, ready/not-ready state, accept call, make call, release call, blind transfer, consultative transfer, conference transfer, hold call, retrieve call, and call duration.

CRM13

The Contractor's CRM tool shall have the ability to navigate from or between CRM screens to other data relevant to the call within the Provider Services module allowing multiple screens to display at one time.

Team CNSI's CRM tool provides a screen view which displays multi view tab with respect to the referenced data context such as Service Request, Provider, and Facilities. The solution provides seamless flow of data within a single view where the necessity of switching between the PMIS screens is reduced due to the integration with PMIS to fetch all the necessary data in real time.

For example, a user can click Provider Last Name or Provider NPI to navigate to multiple view tabs within the context of the selected Provider Record, and the staff can view the different related tabs such as provider licenses, location, and addresses, as shown in Figure 3.10.14-29. The same feature applies across the Siebel application where the hyperlink enables the thread to display where the user originated the navigation. CRM's Enterprise Application Integration (EAI) functionality is used to invoke evoBrix Web services and display the information in the CRM application.

Listed are the evoBrix web services that are used to display provider-related information in the CRM application:

- Provider Locations
- Archived ECM Documents
- Provider Addresses
- Provider License
- Provider Taxonomy

Figure 3.10.14-29 shows the CRM tool and evoBrix PMIS integration overview.

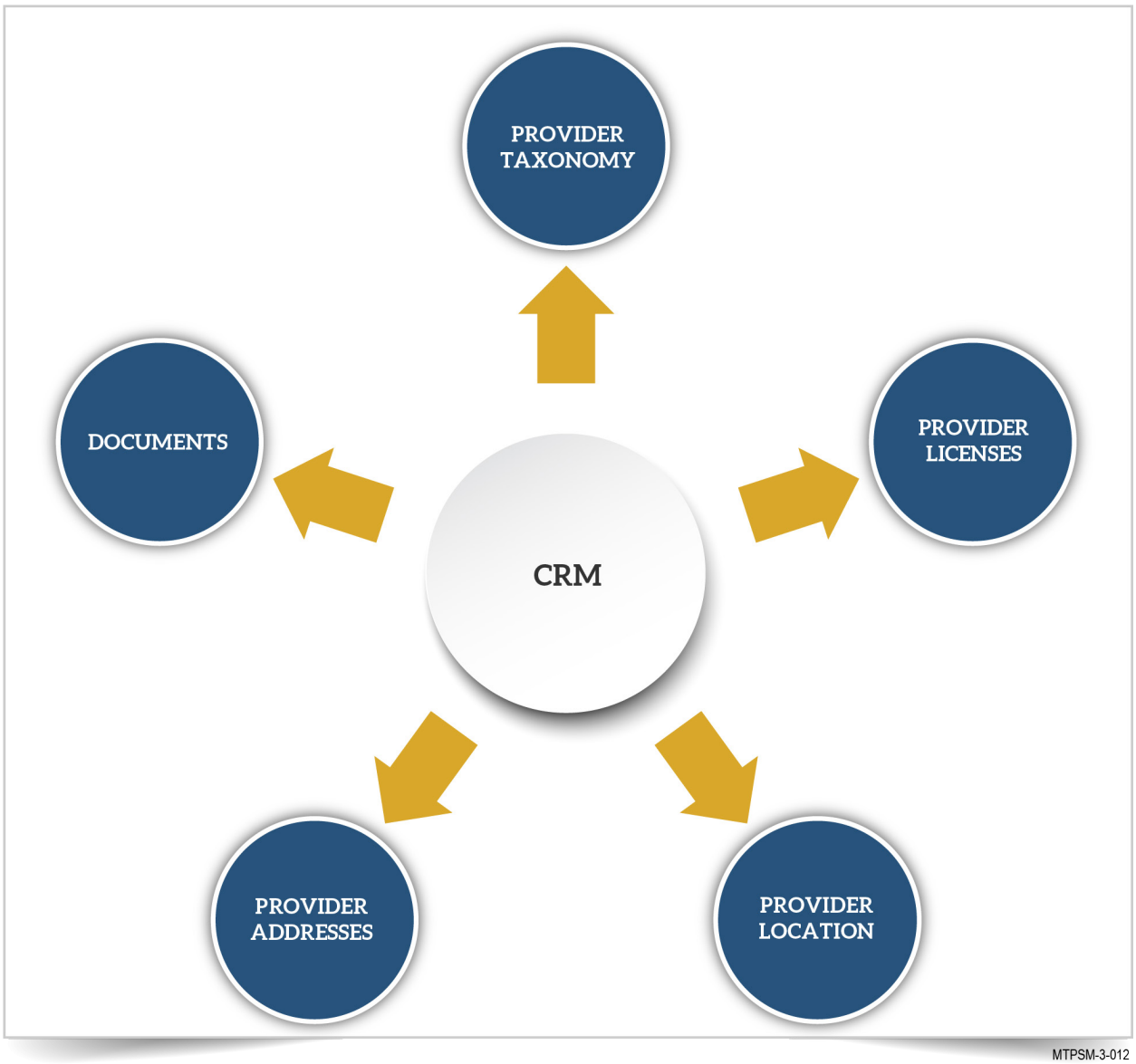


Figure 3.10.14-29. CRM and evoBrix PMIS Integration Overview. Additional web service interfaces retrieve Provider Enrollment information from evoBrix PMIS for displaying in CRM.

CRM14

The Contractor's CRM tool shall have the ability to store the caller's preferred method of communication, including need for deaf or foreign language interpretation.

Team CNSI's CRM solution provides the ability to store the caller's preferred method of communication, language, and special assistance, including the need for deaf interpretation. The solution enables intuitive routing based on various criteria, including language using IVR. Meanwhile when State provide the Language Interpretation Services, Team CNSI's IVR system supports Teletypewriter for the Deaf (TTY) functionality. TTY phone numbers or extensions can be provided for TTY support. In addition, skill-based routing using TTY as a skill can also be used which supports the deaf callers.

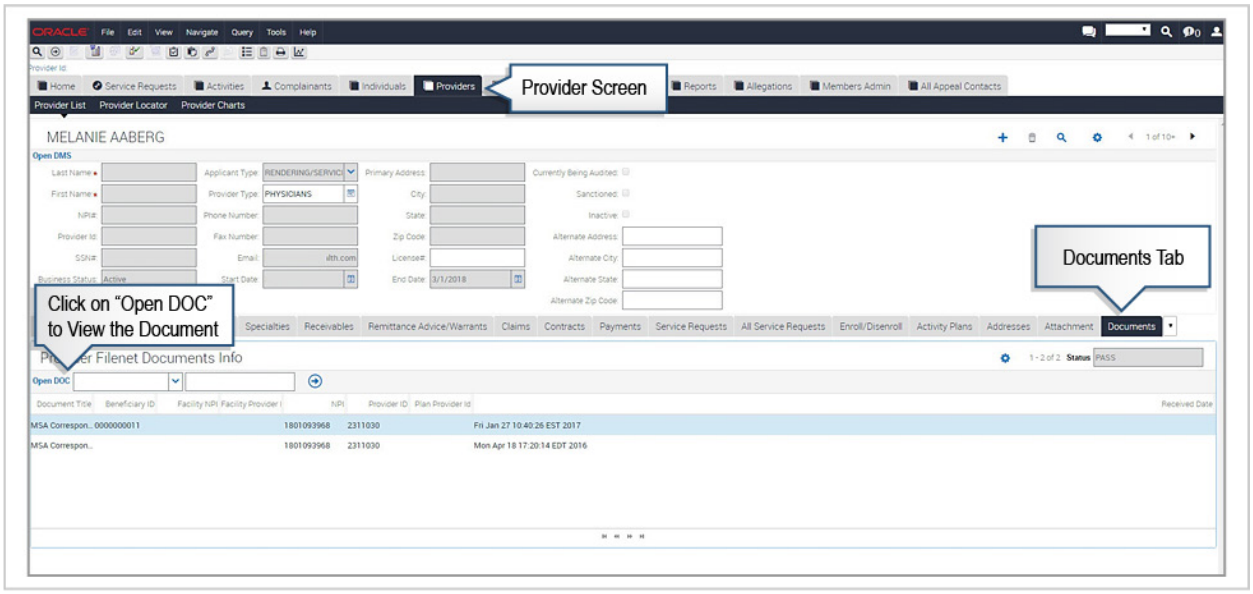
CRM15

The Contractor's CRM tool shall allow users to view related correspondence records from a single correspondence record.

Team CNSI's CRM solution provides the correspondence letters generation feature, in which the correspondence is sent to a Provider or Facility from the CRM. Correspondence templates are stored within the CRM tool and templates are specific to an Area. The letters are generated within the context of a Service Request. A modified letter template can be generated and used by the user on the fly without changing the original letter template.

The Microsoft Word application is used for generating the Mail Merge Document. The generated correspondence is stored in the ECM. The Service Request, Provider, and Facility screen provides a "Documents" subtab that displays the related correspondence to the record queries with respect to Service Request or Provider and Facility.

The Documents are then retrieved from the ECM in real-time and displayed in CRM. The Service Request Attachments view shows all the related correspondence and documents that are associated to the provider using the Service Request record context. Figure 3.10.14-30 depicts the provider correspondence documents in a single view in CRM.



MTPSM-3-357

Figure 3.10.14-30. CRM and ECM Real-time Documents View. Additional web service interfaces retrieve provider-related correspondence from ECM for displaying in CRM.

CRM16

The Contractor's CRM tool shall have the ability to upload or associate attachments to correspondence records.

Team CNSI's solution provides the Siebel file attachment applet, which is a type of applet that provides access to an external document, such as a spreadsheet, word processing document, or slide presentation in

©2017 CNSI | Option B-35

Siebel CRM. The files can be uploaded in any format and referenced as the Service Request linked documents.

The association can be made by clicking the "New File" button, which opens the file browsing option where the CSR can choose and upload in the Attachment view tab under Service Request. The same document can be archived in the ECM real-time web services view.

Correspondence Generation

Team CNSI's CRM solution Siebel correspondence templates can be created or edited in Microsoft Word. Correspondence templates contain fixed text and one or more merge fields. The merge fields are placeholders that are populated with variable information from a Siebel database, such as a contact's name and address or when users generate a correspondence for recipients. Users can create their own personal correspondence templates, and administrators can create correspondence templates for users.

The configurable templates list is shown in Figure 3.10.14-31.

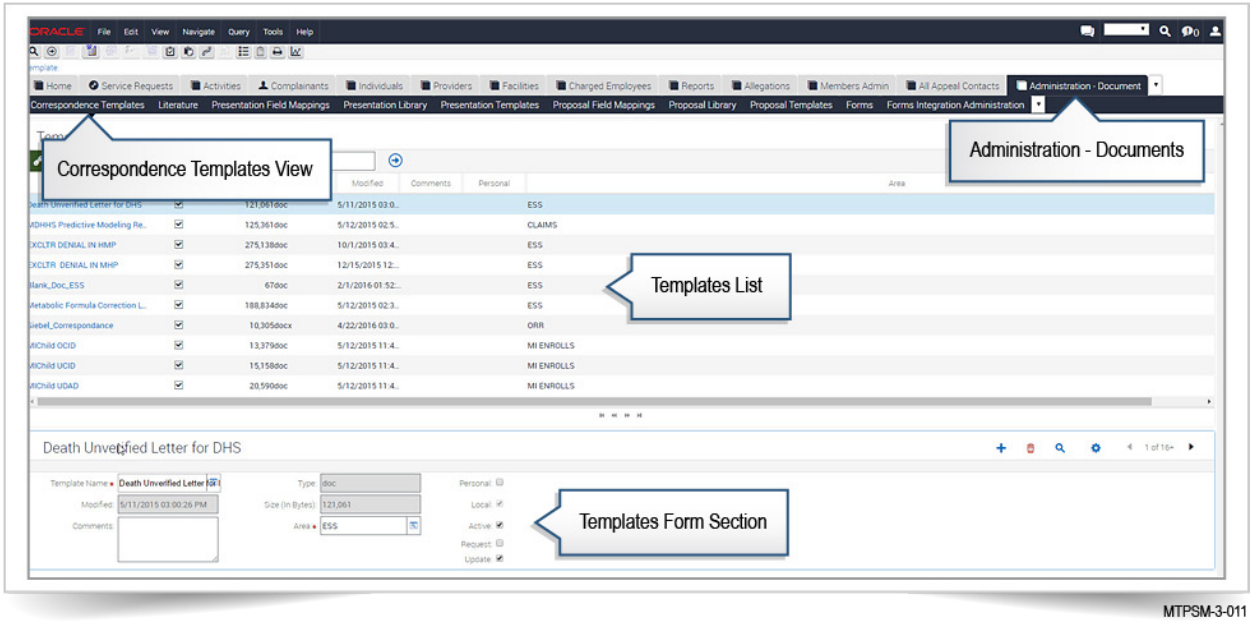


Figure 3.10.14-31. Configurable Templates. The CRM tool allows the Business Owner to create their own templates and can drag the merge field in it.

Correspondence Upload in ECM

When a Service Request is created, the CSR can use the Send Letter (CTRL+L) command to navigate to the Correspondence view and select the template that needs to be archived in FileNet, as shown in Figure 3.10.14-32. With the click of the "Generate" button in the Correspondence applet, the details of Service Request are updated in the template and changes the Document status to "Merged." The "Send to FileNet" button archives the merged document in FileNet through a real-time interface.

©2017 CNSI | Option B-36

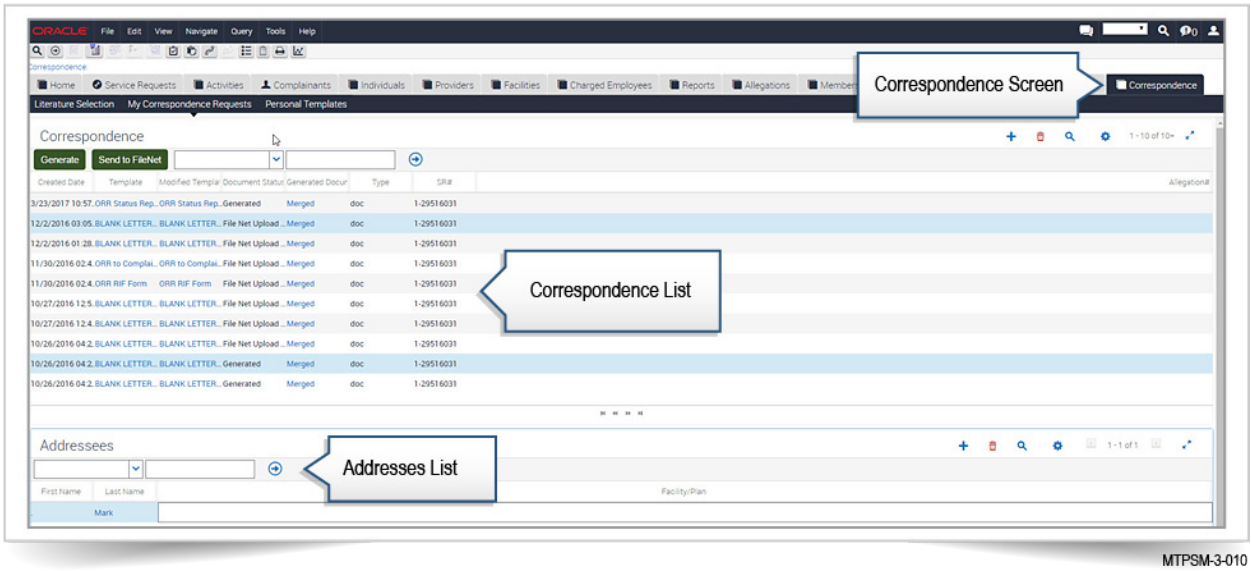


Figure 3.10.14-32. Send Correspondence CRM. Provides the capability to generate the correspondence letter using configurable templates and send to Document Management System.

Service Request Attachment Process

The CRM tool provides the Attachments tab, as shown in attachment and archival process presented in Figure 3.10.14-33, where reference documents can be attached in any document format within Siebel. These documents are stored and maintained within Siebel. The document can also be uploaded to the DPHHS centralized ECM for providing access to the documents for non-CRM users.

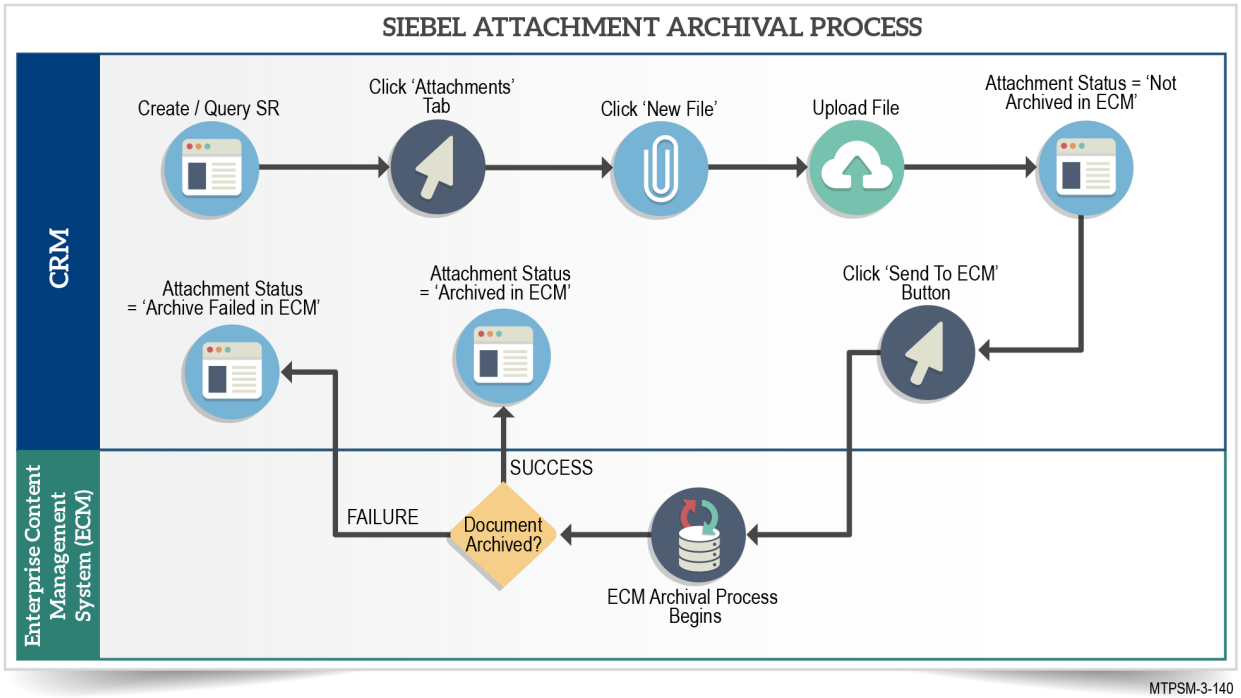


Figure 3.10.14-33. Seibel Attachment Archival Process. The Siebel attachment created against a Service request is uploaded to the centralized ECM for the archival purposes so that non-Siebel users can retrieve the data from ECM.

©2017 CNSI | Option B-37

Figure 3.10.14-34 shows the Siebel Attachment Upload List view where the user can upload the documents on a Service Request.

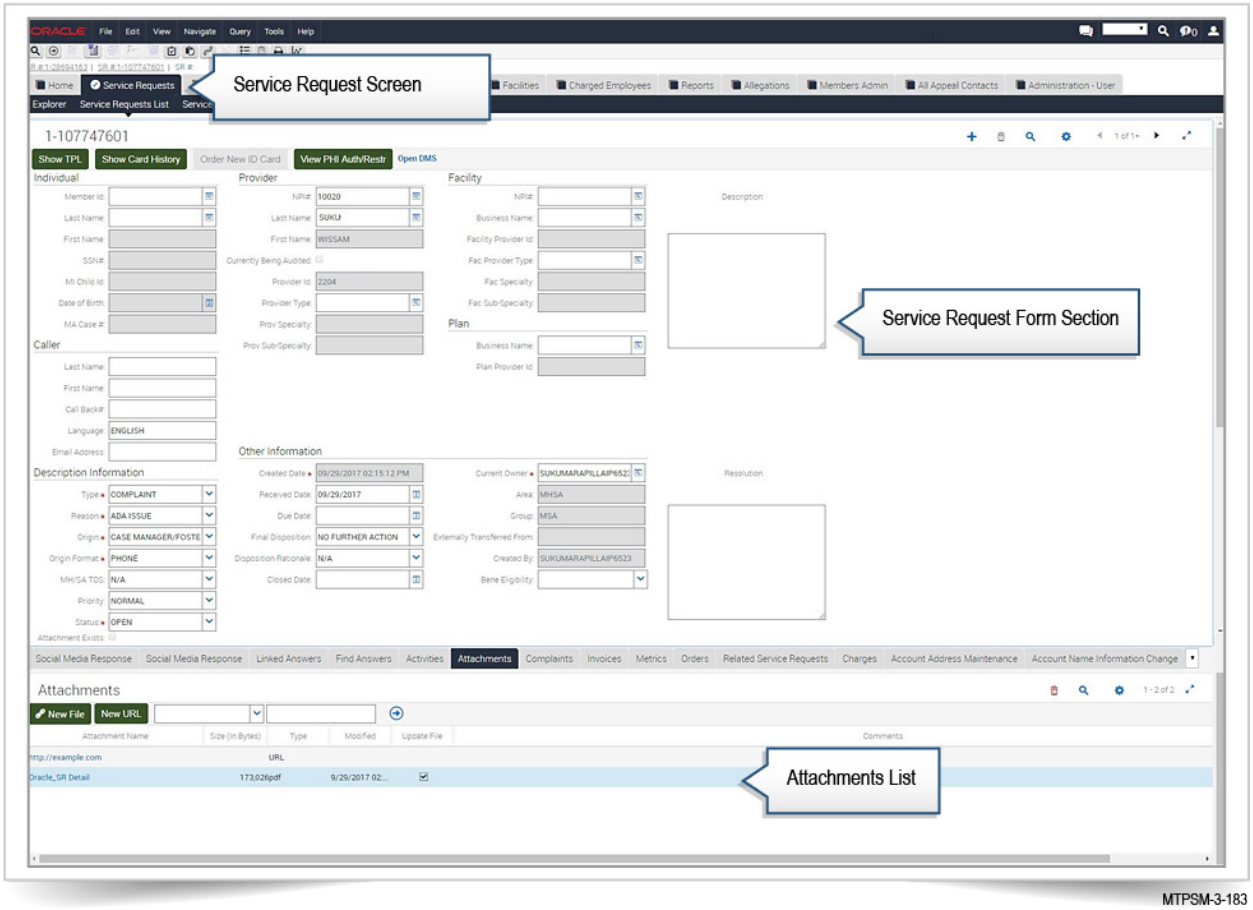


Figure 3.10.14-34. Siebel Attachment Uploaded in the Service Request List. The user can attach a file created in another application to a record wherever the Attachments view is available within a screen.

CRM17

The Contractor's CRM tool shall have the ability to present the contacts authorized to perform business functions with the State's healthcare programs on behalf of the provider or entity.

Team CNSI's CRM solution provides the Demographics information on a Service Request which represents the caller provider information who authorized the CSR and Area Administrator to perform the requested business operations through State staffs. Refer to Figure 3.10.14-16 for the provider demographic information placeholders used to capture the authorized provider caller in a Service Request.

The demographics data are loaded in the CRM tool through back-end jobs that run daily. The demographics information Providers/Facility information, as shown in Figure 3.10.14-35 and Figure 3.10.14-36. It provides key details such as Provider Name, Facility Name, and NPI, respectively.

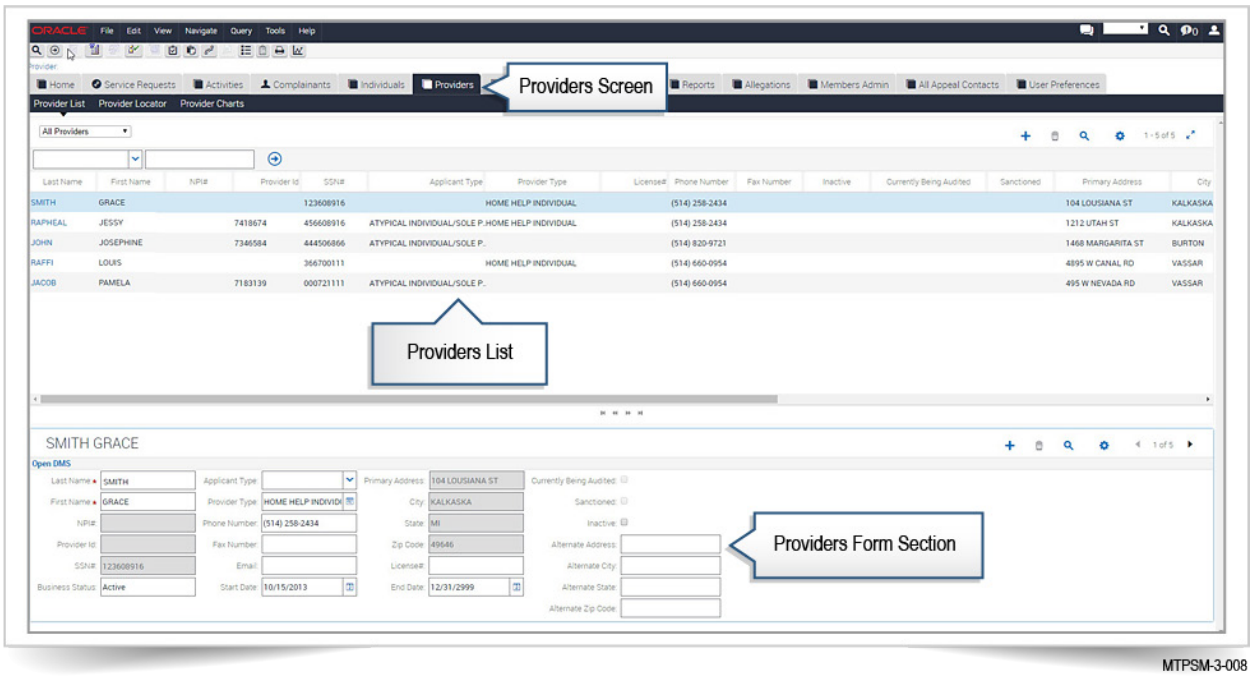


Figure 3.10.14-35. CRM Provider List View. The provider demographics information helps the CSR to verify the caller information while creating Service Request.

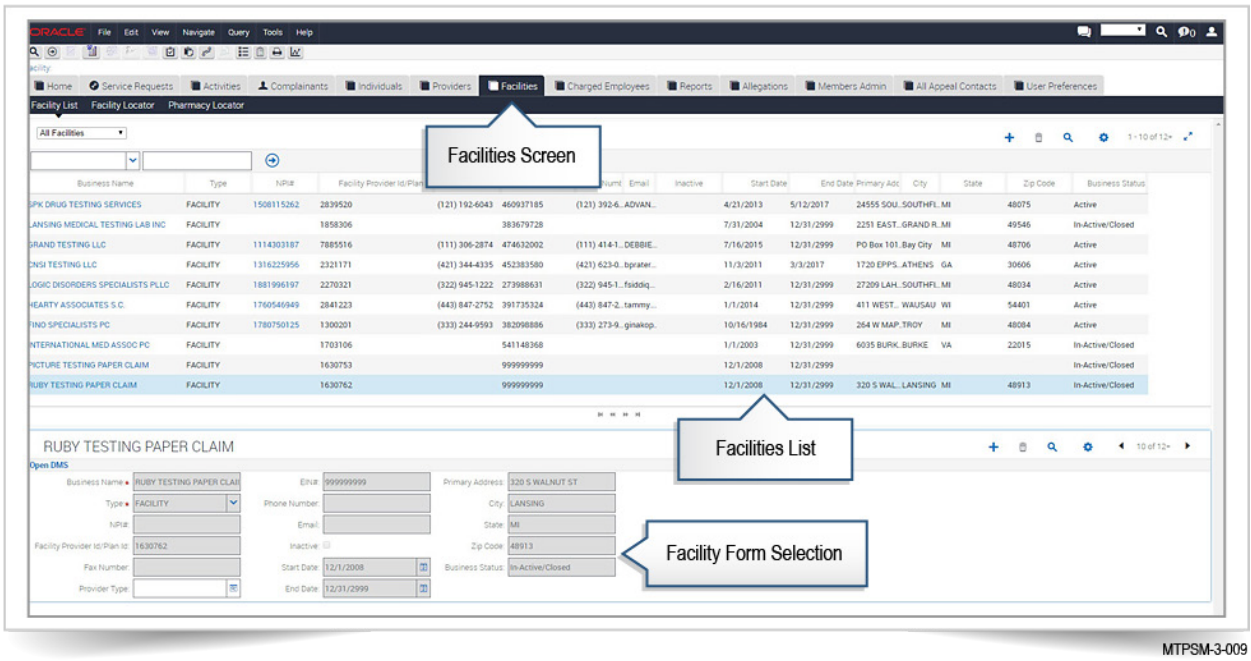


Figure 3.10.14-36. CRM Facilities List View. The Facilities demographics information helps the CSR to verify the caller information while creating the Service Request.

CRM18

The Contractor's CRM tool shall have the ability to accommodate searches on call center records by characteristics such as call type, category, CRM number, name of provider, provider number, contact name, other entity names, service authorization number, category of service, user ID, and any combinations thereof.

Team CNSI's CRM tool supports searching by the service request, activities, and provider attributes. A search based on multiple fields is also supported. The fields that are supported for searching for various entities include those listed below:

- Call Type
- Call Reason
- Provider details such as NPI, Provider ID, Provider Name
- Organizational facility name and Facility NPI details
- Current Owner User ID
- Caller First name and Last Name

Additional fields also available for performing further narrow down search as follows.

- Service Request Entity:
  - Service Request attributes, such as Service Request ID, Status, Source, Received Date, Priority, Creator, Owner, Group, Area
- Activity Entity:
  - Activities attributes such as Activity ID, Status, Type, Call Reason Type, Call Reason Sub Type, Start Date, End Date, Due Date, Priority, and Owner
  - Associated Provider information such as Provider ID, Last Name, and First Name
  - Associated Facility NPI, Facility ID, Plan ID, and Facility Name

Team CNSI's CRM solution provides multiple ways to execute searches

- Search using the New Query and Go (execute query) buttons that are displayed in the Form Section and List Section

Searchable Service Request attributes are shown in Figure 3.10.14-37.

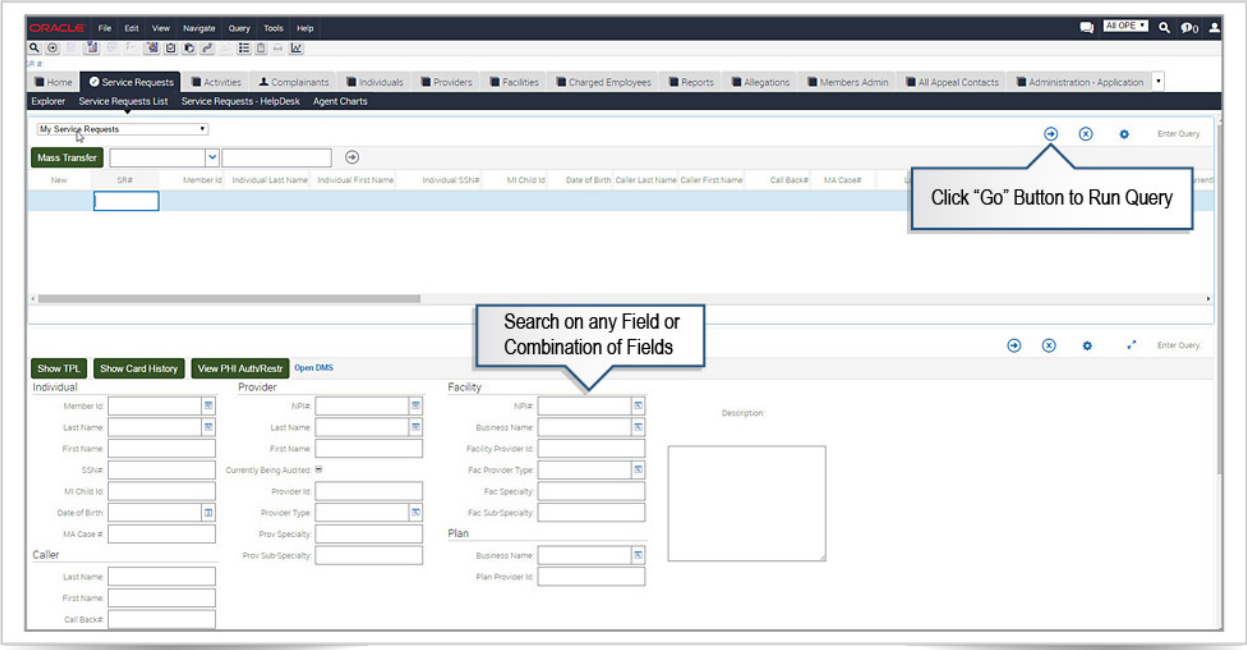


Figure 3.10.14-37. CRM Searchable Service Request Fields. Extensive service request search capabilities are provided, including the use of multiple fields, wildcards, and keywords enables quick searches.

- Team CNSI's CRM solution allow users to have predefined queries (PDQs), which allow users/administrators to specify the search criteria on CRM fields and retrieve the records accordingly. The users can leverage this functionality to view the desired sets of records by using a PDQ. The CSR needs to select the appropriate PDQ from the Queries list. The list of PDQs is context sensitive and dependent on the current CRM screen user. The CRM tool automatically search for relevant records matching the query and display it in the list and form sections.

  Example PDQs for the Service Request screen are shown in Figure 3.10.14-38.

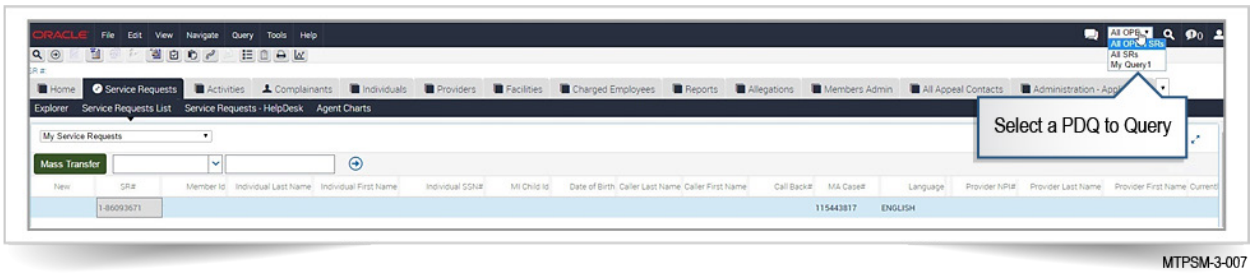


Figure 3.10.14-38. CRM Predefined Query Feature. CRM entity-based pre-defined queries support both private and public queries.

- Search using Query Assistant to build a complex query. Query Assistant is displayed in the Form Section and List Section when the Query button is clicked. CCSRs can click the Query Assistant button, which displays a search form where they can enter complex query criteria.

  Figure 3.10.14-39 shows CRM Go (Execute Query) and Query Assistant Buttons.

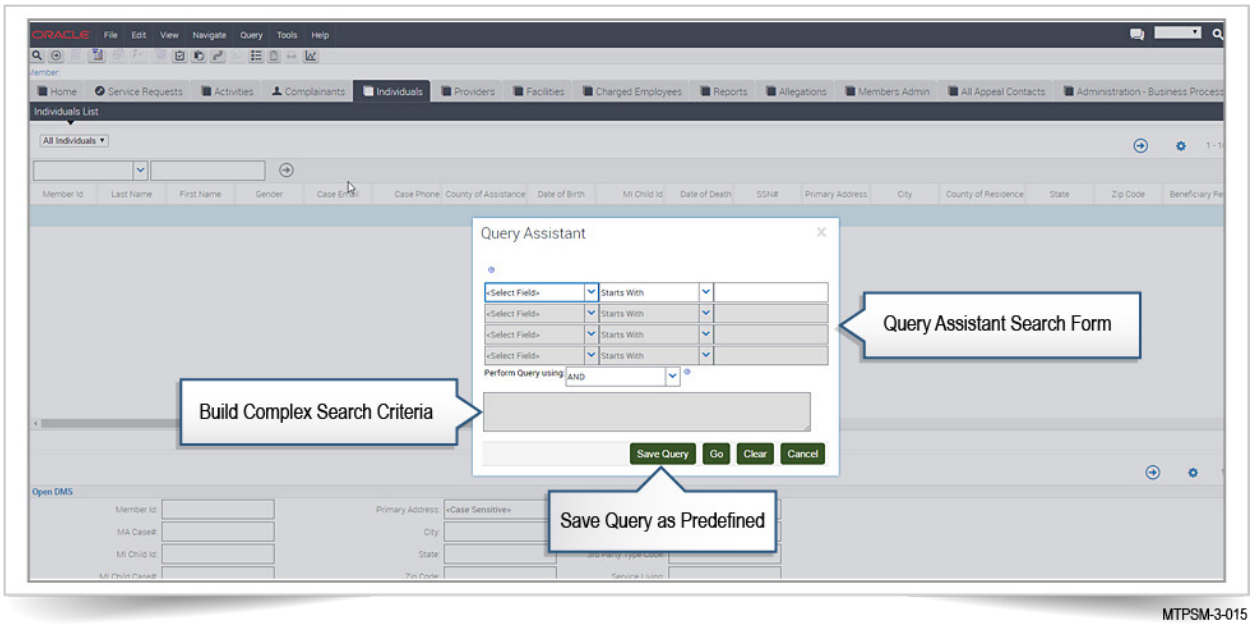


Figure 3.10.14-39. CRM Go (Execute Query) and Query Assistant Buttons. The ability to enter query criteria in list form for any field combination provides CCSRs with versatile and easy-to-access search options.

A CSR can enter a query, save any query as a predefined query, and use it later. Administrators can create public PDQs that are available to all users in the Queries list. The PDQs displayed in the Queries list are different for each entity, such as service request, activity, and provider, in the CRM application.

This is shown in Figure 3.10.14-40. CSR-created PDQs are considered private to the user.

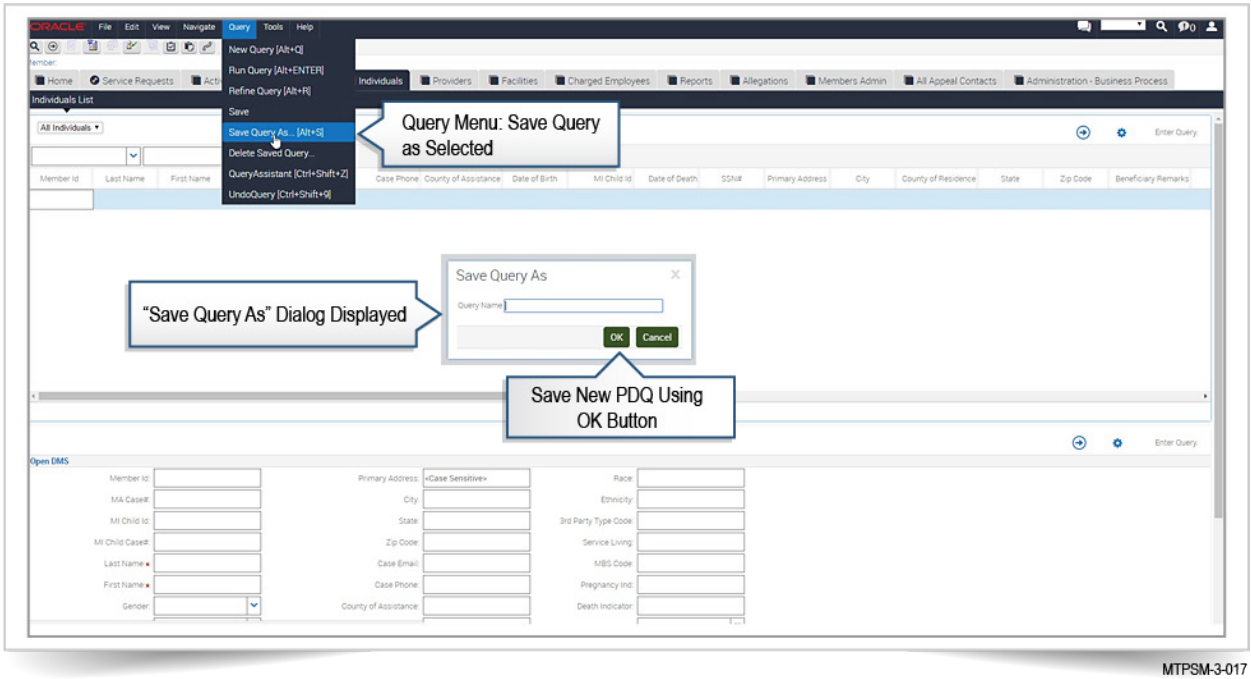


Figure 3.10.14-40. CRM Query List Menu. PDQs enable saving complex queries that are used frequently, providing the CSR with easy access to frequently used queries without requiring re-entry.

©2017 CNSI | Option B-42

3.10.14.4 Provider Call Center

This section outlines the requirements for a Provider Call Center. The Offeror's proposed Option B services must include a provider Call Center for new and revalidation applications and enrollments. The Contractor will also provide enrollment support for providers during the enrollment process. Typically, this support includes responding to provider's questions about their responses to the application questions. The base provider solution will include context sensitive help throughout the enrollment process, which is intended to reduce the number of help desk solicitations. In addition to fielding questions related to enrollment and re-enrollment, the Contractor will also be responsible for additional activities (e.g., fielding questions related to changes in provider information, financial information, provider suspension for administrative reasons, or for other reasons such as IRS "B" Notices). The Offeror must describe their approach to meet each of the Provider Call Center requirements defined in Attachment F, Requirements Matrix.

The Provider Call Center is a critical function of a successful provider services operation. With the ever-increasing complexity and constant changes in the health care environment, providers need not only to feel supported, but also to know through consistent interactions that their needs are both understood and are being addressed to their satisfaction. Team CNSI has in-depth experience in delivering that high level of customer service by providing:

The Team CNSI Advantage

Team CNSI's Call Center solution features robust capabilities to deliver higher levels of customer service to the full provider community.

- Proven multichannel capabilities developed for Medicaid operations
- Award winning customer service tailored to healthcare provider needs
- Access to real-time information reduces call handling times and improves first-call resolution rates
- Easy access design promotes usage of self-service capabilities and reduces costs

MTPSM-3-115

- A staff of knowledgeable customer service representatives (CSRs) made up of skilled and experienced provider enrollment specialists
- Ready access to relevant information in real-time
- Prompt answers to questions, supported by multiple technologies
- Multiple access points including streamlined self-service methods to quickly find needed information
- Consistent and accurate information
- Automated tracking and reporting of all contact types, from initiation through closure

As part of our provider services offering, Team CNSI believes that each provider Call Center interaction provides an opportunity to build positive relationships with the provider community. With that guiding principle, Team CNSI designed the Call Center solution to include an integrated offering of leading components. This solution is based on the same components implemented in Washington and has been proven to deliver improved customer service and effective operations, resulting in increased first call resolutions and reduced call wait times. In the states of Michigan and Washington, respectively, 600 and 180 Call Center personnel use the Team CNSI's solution to serve consumers, providers and other trading partners. The solution provides the CSR a complete, 360-degree view of the provider, including the provider's application data, call history, financial information, and correspondence over time. Using these tools, we can address inquiries related to enrollment along with questions regarding financial information, provider suspension, IRS B notices, changes to provider information, and provide other general information. We provide thorough training to ensure Team CNSI CSRs have the knowledge to answer basic and complex inquiries we anticipate.

Team CNSI member Noridian brings over 50 years of experience in federal and state health care services, including direct support of providers participating in these programs. Evidence of our success in

delivering excellent provider services can be seen in Noridian twice being awarded the CMS Provider Customer Service Program (PCSP) of the Year award, in addition to consistent praise by the providers served. In addition, Noridian is ranked highest in the country on measures of provider satisfaction for its performance on the Jurisdiction F Medicare Administrative Contractor (MAC) contract that supports providers in the following NASPO states: Montana, North Dakota, Oregon, South Dakota, and Wyoming.

An additional feature of our provider management services is a robust provider training program. Provider training is a critical component of the overall success of the MT PSM solution implementation and operations. Effective training for providers is the key to maximizing acceptance, satisfaction, and use of the new solution. Ongoing training supports the need for provider awareness of policy changes and associated updates that impact the enrollment process. In fact, effective training decreases provider calls as they are able to navigate technology through self-service. This has a multi-point value as it increases provider satisfaction through prompt access to enrollment and updates while simultaneously decreasing the cost of the program as fewer staff are required to support provider telephone inquiries. Team CNSI will design a comprehensive provider training program engrained with our knowledge of effective provider education methods and associated materials based on the successful processes used for past implementation and operations activities.

Our experience and past success prepares us to offer DPHHS a high quality, low-risk provider service approach based on proven practices and lessons learned. We are ready to develop a strong and effective team during implementation, based on recruitment, hiring, and training practices honed over the past five decades supporting Call Centers. Team CNSI will be prepared to support all aspects of new applications processing enrollment, re-enrollment and revalidation, as well as ongoing maintenance and updates, financial information, disenrollment, suspensions, reinstatements, and other related support topics.

PRCC01

The Contractor shall provide a provider enrollment Call Center to support and instruct providers in the application process, renewal process, provider management, and recertification process. The Call Center shall also support the financial enrollment process into the State financial system.

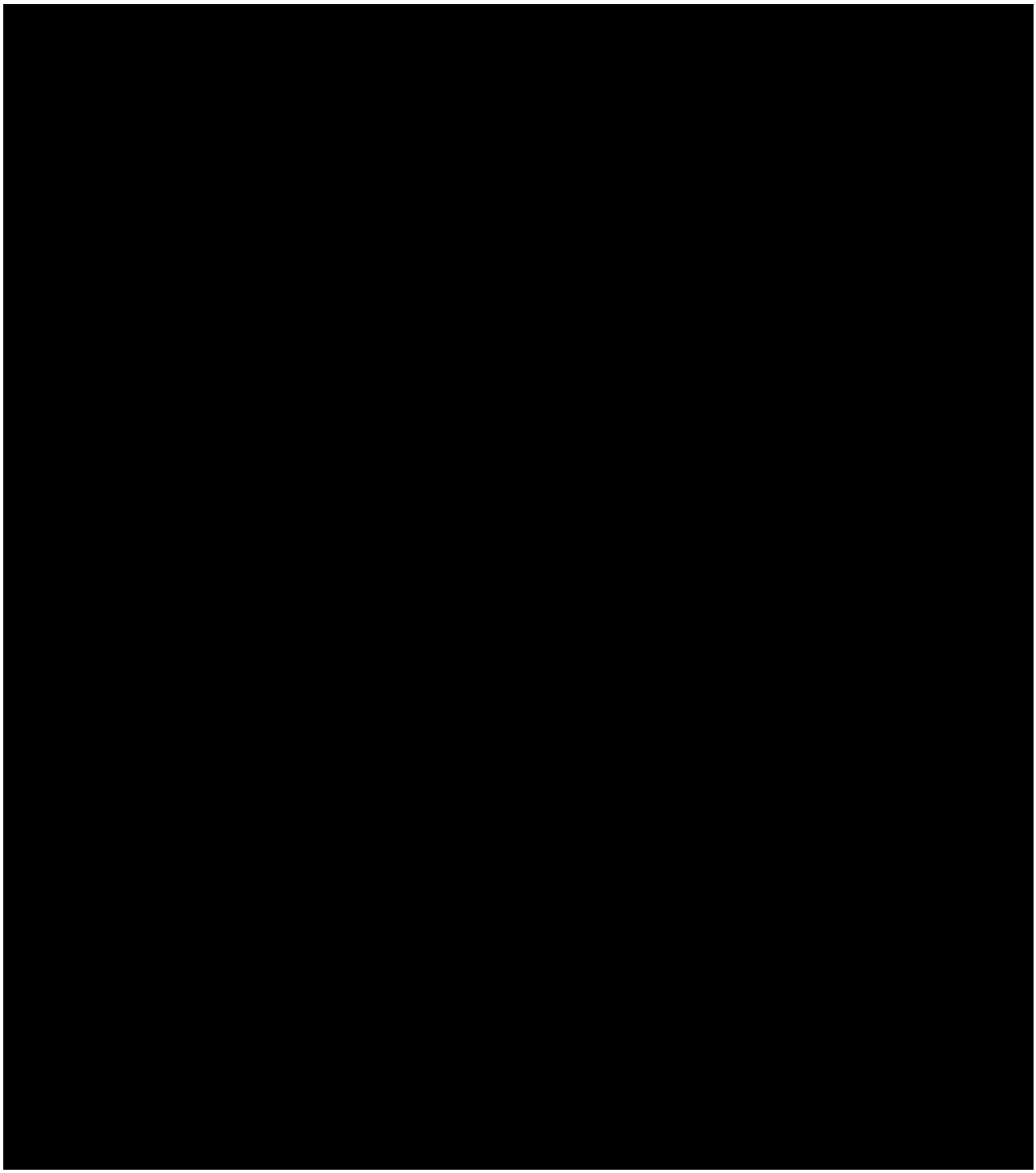
Team CNSI recognizes that customer service functions have evolved from purely a service request response function to a relationship management mission. Our Call Center solution maximizes customer satisfaction by utilizing tools and data-driven analysis to support our proactive service model. Instead of simply providing answers to questions, we analyze recurrent issues to identify root causes. Using that information, we suggest process changes or modify training materials to proactively improve the provider experience. We have achieved tangible benefits using this approach, such as increasing clean application submissions, by modifying provider support information and providing additional training. These efforts resulted in reducing unnecessary enrollment delays, directly impacting provider satisfaction.

Team CNSI provider management and Call Center operations work to safeguard the Medicaid Program while providing timely, high-quality service to providers. We define our standard operating procedures by inquiry type, which facilitates the ability to manage to standards and turnaround times. We receive work through various channels and for various means, for example, calls to the Call Center, emails, chat, fax, and letters. The process for responding to requests for assistance is similar, but customized, for each method of receipt.

Team CNSI will support and instruct providers in the application process, renewal process, recertification and other provider management functions. Collection of provider financial information is a standard function of the enrollment process. Our Call Center staff will be trained to provide assistance to providers

to include financial data such as bank routing/account numbers and Employer Identification Number (EIN) in enrollment. A PMIS report will be used to pull the provider financial information for entry, by Team CNSI business operations staff, into the appropriate State's accounting system. Details of this process can be found in Section 3.10.14.7, Collect and Enter Provider Financial Information in State Financial Systems.

Figure 3.10.14-41 depicts the Call Center solution overview.



The process flow shows the integration between Siebel CRM and the Avaya telephony components. Integration between the CRM and other MT PSM components uses web services for real time information retrieval. The Call Center technology, methodologies, and processes are described below, additional technical details can be found in Section 3.10.14.3, Customer Relationship Management, and Section 3.10.14.5, Interactive Voice Response.

- Step 1: Multi-channel access to assistance

  Multi-channel, data-driven customer interaction gives providers access to the information they need in the way they choose to receive it. Team CNSI provides an enhanced user experience by including interactive self-service applications, such as the IVR and provider portal, in addition to voice support with knowledgeable CSRs.

- Step 2: Integrated technology solution

  Our customer-focused team members are supported by a suite of leading technologies, which are proven in the production environment in Washington and are being implemented in Utah state Medicaid programs. Utilizing a proven solution, with COTS products integrated in production environments, provides for a low-risk solution.

- Step 3: Computer Telephony Integration (CTI)-supported access

  As calls enter the system, providers are requested to provide specific information, such as NPI or tax ID, to complete the authorization process. In addition, they are provided the opportunity to select or say the reason for their call. This information is attached to the call and will be passed along to other applications or agents when a call is transferred. By implementing a Call Center with CTI capabilities, Team CNSI will reduce the average duration of calls by ensuring that a higher percentage of call time is spent productively rather than gathering basic caller information. Using CTI provides a higher level of customer service and allows our CSRs to handle a larger call volume, without increasing staffing levels.

- Step 4: Skills-based routing supports single call response

  As an experienced provider of modern contact center services, our solution offers a multi-channel environment where providers can connect with us in the manner they find most suitable to their needs. Each CSR maintains a profile within the system that identifies both program-level knowledge areas (such as enrollment or technical support) and skills (assisted chat, email, voice). As contacts flow in, the system identifies the channel (voice, email, chat, fax) and automatically routes it to an open CSR best suited to handle the inquiry, based on their knowledge and skill. All CSRs will be cross-trained to support multiple knowledge areas and multi-channel input methods to ensure full coverage of incoming contacts.

  The CRM application is tightly integrated with the multi-channel contact center solution, and provides the mechanism to track all communications and document the resolution and outcome. Incoming calls for technical support will be routed to the technical help desk analysts, with access to the Open-source Ticket Request System (OTRS), which includes ITIL-compliant best practices for incident management.

- Step 5: Call recording, training, and work force management

  Utilizing the Avaya Work Force Optimization tools will improve our services by:

- Capturing and analyzing voice and non-voice customer interactions with a scalable, flexible, and secure recording platform. Leadership will be able to determine where our service is excellent and where to make changes.
- Defining and delivering a consistent provider experience that meets goals and provider expectations. Leadership will be able to leverage interaction data to determine enhancements to service processes, policies, and agent practices.
- Improving customer satisfaction, CSR performance, and job satisfaction, with targeted coaching plans and courses that help improve CSR knowledge, efficiency, and productivity.

- Step 6: Enhanced provider experience with personalization

  Providers and trading partners have access to program information in multiple ways:

  - Through the provider portal, via the inquiry screens
  - Self-service access through the IVR
  - Team CNSI CSR support through calls, emails, or chat sessions

- Step 7: Management and reporting

  The MT PSM solution includes out-of-the-box reporting capabilities delivered through both Cognos and Avaya. Team CNSI will use the Avaya software application to monitor telephone statistics, described in section 3.10.14.5 Interactive Voice Response System.

  Avaya provides a real-time display of available agents, average online time, average talk time, average hold time, average speed of answer, calls in queue, total calls offered, total calls answered, service level percentage, and total time the agent was available to take calls. Call center management use this monitoring tool to generate SLA and overall performance reporting, manage Call Center workload, and monitor that performance expectations are being met. Additionally, the Team CNSI's solution also includes HealthBeat, which supports business activity management functions, supports SLA tracking and reporting, and provides dashboard views of operational processes. This enables the operation's team to constantly monitor the overall health of the system, the operation, and how we are meeting DPHHS goals.

Team CNSI's commitment to provider support and education is the bedrock of our provider services approach. We will tailor our existing processes to include education and support for entry of data into the different states' financial systems. Our experience has shown that better educated providers have fewer errors when submitting original enrollment applications or going through the renewal and recertification process, which in turn reduces inbound inquiries, and ultimately improves the providers' perception of services received. With a data-driven approach to education, common provider errors in applications are reduced or eliminated. Online self-service functions have more accurate data, which results in fewer requests for additional information and ultimately more timely processing of applications, renewals, and recertification increasing providers' satisfaction with the whole process.

PRCC02

The Contractor shall research and provide documentation for administrative hearings, appeals and court cases; and participate in these activities upon direction from the State.

Our provider management solution includes a complete and comprehensive audit trail with detailed history to support administrative hearings, appeals, court cases, audits and inquiries such as Freedom of Information Act requests, congressional inquiries, Office of Inspector General (OIG), Government

©2017 CNSI | Option B-47

Administration Organization (GAO), law enforcement officials, or offering support for appeals being reviewed by an administrative law judge. In our experience, we have responded to requests from law enforcement for information concerning provider applications and enrollment related communications in fewer than five business days. We can rapidly respond to requests for verification of provider information, typically within one business day of receipt of request by the provider or DPHHS. Our in-depth experience supporting hearings and appeals efforts has lead us to develop our best-practices process to include the ability to archive and retrieve not only provider data, but also policy, procedure, work instruction documentation, and other artifacts. We are prepared to participate in administrative hearings, appeals, and court cases in support of government agencies including Office of General Counsel (OGC), OIG, and DPHHS.

TRN15

The Contractor shall conduct training for identified system/component users on the system relative to their use initially and upon updated functionality prior to the initial production deployment and within 45 days of each major release into the Production environment

Prior to system deployment, Team CNSI performs an operational readiness review which includes required training to ensure success of the organization and provider community once in production. For training, the operational readiness review focuses on two core areas:

- Organizational Readiness: Ensuring that the State and Team CNSI organizational teams are trained on their jobs, have appropriate documentation and procedures for their roles, and, when possible, have had the opportunity to practice those procedures. This is a joint responsibility between Team CNSI and the State.
- User Readiness: Ensuring that the users (Team CNSI staff, providers, and the State) have had training and have been supplied documentation on how the system functions and, thereby, know how to use the system and how to contact help when needed.

As discussed in Section 3.10.2.7 Training, this training provides trainers (for train-the-trainer activities) and end-users with what they need to use the system confidently. In addition, Team CNSI will provide a user guide/manual organized by procedures and roles to facilitate use of the system. The procedures in the guide/manual are formatted as job aids that provide end users with the steps needed to complete each procedure for their role. The classes and procedures in the user guide/manual make it very easy for users to understand how the system can help them complete their jobs.

One of the necessary elements to be considered with any change is the degree and level of training that may be required to accompany changes to the system. When a change is identified and introduced through the change management process, Team CNSI will assess each aspect of the change's impact to the environment including the impact upon communication, training, and publications related to system functionality. The change management process and the training plan will be used to coordinate timing and approvals that ensure changes required to revised artifacts are updated to coincide with approved system changes. Training, when needed for changes, including major releases, is delivered within 45 days of the change/release.

TRN17

The Contractor shall develop and provide as necessary, training for the Provider Community. The training must be structured to address the Contractor's solution functionality for enrollment, maintenance, and revalidation.

Team CNSI has an extensive history of successfully delivering training for providers and stakeholders. Team CNSI member Noridian brings over 50 years of experience in commercial, federal, and state health care service and administration. Current contracts reach nearly 340,000 providers and suppliers. These services have spanned all provider types and vast geographic locations, which prepares us to offer a low-risk approach to DPHHS based on proven practices and lessons learned. Noridian already has relationships with the Montana, Oregon, North Dakota, South Dakota, Hawaii, and Wyoming provider communities through its work as a MAC, making Team CNSI an excellent partner for multiple of the participating NASPO ValuePoint states. Noridian will build upon the foundation of its relationships in Montana throughout the implementation and operations phase as it connects with additional Medicaid provider stakeholders not already familiar with Noridian.

During the implementation phase, we develop training materials, tutorials, and package training for presentation through Team CNSI's Cornerstone Learning Management System (LMS). It is important that providers are familiar with changes to their current environment and understand the benefits of the new systems made available to them. To fulfill this, we explain what system functions will change, how interface with commonly required material, and where to find resources to assist them in using self-service tools to manage their provider information. We focus on the use of Team CNSI self-service portal as the main source for implementation news, schedules, and events.

Team CNSI uses the industry-standard ADDIE method, discussed in Section 3.10.2.7 Training, to guide training development and delivery for all audiences. ADDIE is the standard training development paradigm recommended by the American Society for Training and Development. Because our provider training program is guided by best practices, decades of health-care training experience, and ongoing process improvement, we offer DPHHS a worry-free, low-risk training solution that will help the providers use the new provider enrollment system confidently and accurately.

The evoBrix PMIS enrollment functions are designed to be easy to learn and use. Once initial positive momentum is achieved through a basic understanding of the system, providers are soon able to navigate and use features that are consistent throughout the system. To provide users with a baseline understanding of the system, Team CNSI provides computer-based training (CBT) including:

Computer-based eLearning modules:

- User Account Registration and Enrollment Process
- Enrolling as a New Individual Provider
- Enrolling as a New Group Provider
- Enrolling as a Special Provider – Facility/Agency/Organization (FAO), and other State Specific enrollment types
- Enrollment Modifications/Maintenance – Individual
- Enrollment Modifications/Maintenance – Group Practice
- Enrollment Modifications/Maintenance – FAO, atypical providers, and other State Specific enrollment types
- Revalidation Procedures
- Understanding the provider Site visit process

Team CNSI's training approach covers a spectrum of methods to accommodate all learning types, provider locations, and preferred formats of training. This includes the following possible methods:

- **eLearning courses** are pre-recorded and available 24 hours a day, 7 days a week via the website. The tutorials incorporate multiple types of media including static content such as slides, forms, audio

recordings, and video with screen-capture technology. This enhances the learning experience by associating real situations with training materials.

- **Webinars/Demonstrations** provide online training and video sharing, simulating "face-to-face" and "in person" training sessions and meetings without the costs associated with travel. Webinars allow for activities such as real-time, interactive conferences; sharing training presentations; application demonstrations; and web tours. When surveyed, providers have indicated a preference for this type of training as it allows providers to participate without requiring staff to leave the office.

Our focus when we conduct any education with the provider community is to stress the positive benefits of the Medicaid system as it relates to the provider. We want to create a lasting, positive relationship with providers and trading partners and work towards that goal with every interaction including phone calls, emails, seminars, letters, CBT courses, and the self-service portal. Our education activities are specifically geared to foster rapport with providers. Team CNSI is very successful at establishing a positive connection with each provider we serve.

3.10.14.5 Interactive Voice Response System

This section outlines the requirements for an Interactive Voice Response System. The Offeror's proposed Option B solution shall include an Interactive Voice Response (IVR) System in order to welcome and route incoming provider calls; convey educational alerts during hold times; and intelligently queue providers until Contractor staff is available. The IVR system will include the ability for the provider to leave a message, during or outside, normal business hours. The Offeror must describe their approach to meet each of the Interactive Voice Response System requirements defined in Attachment F, Requirements Matrix.

The Interactive Voice Response (IVR) system is a critical component for achieving effective Call Center operations. IVR systems save time and reduce costs by effectively directing and managing incoming customer calls. An IVR efficiently implemented lets the Call Center Customer Service Representative (CSR) focus on high priority tasks and delivering excellent customer service.

When it comes to designing and implementing an IVR solution, simplicity is the key. Self-service solutions leveraging IVR can offer immense value if they are easy to use from the provider perspective. Team CNSI's IVR solution is designed keeping both simplicity and scalability in mind, and can be leveraged for small to large scale Call Centers.

The Team CNSI Advantage

Team CNSI's Call Center solution features robust capabilities to deliver higher levels of customer service to the full provider community.

- Proven multichannel call center with computer telephony integration (CTI) coupled with both interactive voice response (IVR) and customer relationship management (CRM) applications currently supporting multiple Medicaid customers
- Award winning customer service processes minimize administrative burdens and increase provider satisfaction through effective self-service capabilities
- Extensive usability features to reduce service times and provide faster and improved customer service experience
- Secured real-time integration with evoBrix using Web services offering access to real-time information to service customer calls
- Robust capabilities reduce call handling times through real-time integration with CRM

MTPSM-3-026

Team CNSI's IVR solution brings together as much call information as possible and passes it to the CSR so that the CSR can focus on providing a high level of customer service without spending time collecting basic call details. When a provider call reaches a CSR, the CSR is already aware of whether the provider is authenticated and the type of assistance for which the provider is asking. Hence, Team CNSI's IVR solution is not only effective but also provides a positive experience to the providers.

Team CNSI's IVR solution is based on the same components implemented in the State of Washington and has been proven to deliver improved customer service. The same components are being planned to implement our IVR solution in the State of Utah as well.

Team CNSI's Call Center, including IVR, is designed using Avaya systems. All the components of our IVR solution are carefully chosen to provide required functionality and meet our customer needs. Avaya IVR is an open standards-based web services platform IVR built using the open standard VoiceXML and Java technologies and designed specifically to incorporate today's networked IP and Session Initiation Protocol (SIP)-based enterprise call centers. Team CNSI's IVR solution truly complements its CRM Call Center, as seen in Figure 3.10.14-42.

Avaya IVR Features	Description
Intuitive Menu Driven Design	Avaya IVR solution provides an intuitive menu driven design including dynamic and static menus. Industry leading solution Nuance is used for automatic speech recognition. The IVR provides callers easy access to speak to an agent using keywords like Transfer or using numerical Dual Tone multi-frequency (DTMF) key '0'.
Dual Tone multi-frequency (DTMF) and Speech Recognitions Support	Avaya IVR solution will provide support to both DTMF and Speech inputs. Caller can select an option or can speak to navigate through the IVR menus.
Multi-Language Support in IVR	Avaya IVR solution can be easily configured to support multiple languages. Currently our UTAH IVR solution is supporting the implementation to run in English and Spanish.
Text to Speech (TTS) Support	Complex messages such as coverage and phone numbers are played back to the caller using a text-to-speech engine instead of pre-canned or pre-recorded messages, providing flexibility and scalability.
Text Telephone (TTY) Support	Avaya IVR system will support TTY functionality. TTY phone numbers or extensions can be provided for TTY support. In addition, skill-based routing using TTY as a skill can also be used.
Integration with Team CNSI's evoBrix Provider Management Information System (PMIS)	The IVR solution is integrated with Team CNSI's evoBrix PMIS solution, ensuring that callers have the latest information from evoBrix PMIS.
SOA architecture	The SOA benefits the overall solution in that it avoids unnecessary data replication and increases scalability of the solution, in the process making it a highly manageable solution.
Voice mail and direct agent transfer	Our IVR solution provide option for callers to talk directly to a CSR using the agent id. This reduces the time for agents to handle the cases quicker and provides satisfaction to caller. Caller can also leave voicemail if the agent is unavailable.
Computer Telephony Integration (CTI) Support	Avaya IVR solution enables sending relevant information about the caller to agents via the CRM solution. This feature, also known as the Computer-Telephony Integration (CTI) screen pop, enables the agent to better serve the customer because all relevant information about the caller is already presented on agent's screen, saving valuable time that would otherwise have been spent searching for caller information.
Skill Based Routing	Team CNSI's IVR solution provides intuitive routing based on various criteria including language. IVR assigns skill values to incoming queue calls so that calls can be sent to the most qualified agents. Skills-based routing is configured through your IVR.
Work Force Optimization	Our Call Center solution provides Call recording, Screen monitoring, Performance monitoring and Forecasting using Avaya Work Force Optimization solution.

Figure 3.10.14-42. Avaya IVR Features. Team CNSI's Avaya IVR solution contains many available features.

Technical Components and Advantages

The following section describes the major components of our solution, and highlights the unique features and benefits of our Call Center application.

Team CNSI's Avaya IVR is a scalable, configurable, robust solution that employs the principles of service-oriented architecture (SOA). It is composed of an integrated system with distributed services. For example, calls are initially handled by the IVR system; however, to play back certain information to the caller or to authenticate the caller, a pre-published service is invoked to retrieve the information in real time. Similarly, real-time activity tracking of the caller is accomplished by invoking the tracking service within the Oracle Siebel CRM application.

The core component of the Avaya IVR solution is the Media Processing Platform (MPP). MPP does collection of touch-tone, recognition of speech, and plays out text-to-speech. It can interface to the Legacy Time Division Multiplexing (TDM) based architecture or the new SIP-based architecture for receiving speech calls. The MPP also generates events which are later produced as reports to obtain more details about the voice calls.

The Avaya Call Center components which will be leveraged for meeting the requirements are:

- Avaya Aura Experience Portal (AAEP)

  Avaya Aura Experience Portal comprises next generation releases of what was previously known as Avaya Voice Portal. Experience Portal provides organizations with a single point of orchestration for all automated, multimedia, self-service, and IVR applications across inbound phone or video, as well as outbound phone, email, or Short Message Service (SMS) applications. Avaya Aura Experience Portal supports SIP, Internet Protocol (IP), TDM, and mixed environments, and provides robust management, reporting, development, and virtualization capabilities.

  The Experience Portal system consists of the following major subsystems:

  - The Experience Portal Manager (EPM) that controls the Experience Portal system
  - One or more MPPs that process all incoming and outgoing calls
  - An auxiliary EPM server that handles outgoing calls, email processors, and SMS processors when the primary EPM server is unavailable

  The Experience Portal network consists of the following external systems:

  - Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) servers
  - Application servers

  A SIP network includes the following external servers:

  - Session Manager
  - Gateways, such as Audio Media Gateway or Avaya G450 High Density Trunk Gateway

- Avaya Aura Communication Manager (ACM)

  Avaya Communication Manager is the open, highly-reliable, and extensible IP Telephony foundation on which Avaya delivers Intelligent Communications to enterprises, large and small. Communication Manager effectively scales from less than 100 users up to 36,000 users on a single system.

Communication Manager is an important component of the Avaya architecture, which consolidates several components into a holistic package that enterprises need for Unified Communications. This software is available with a single-user licensing fee. Communication Manager provides centralized call control for a distributed network of gateways and a wide range of analog, digital, and IP-based communication devices. Communication Manager comes with several built-in mobility applications, call center features, and advanced conference calling capabilities.

- Avaya Aura Call Center Elite

  Avaya Call Center Elite features Avaya Expert Agent Selection (skills-based routing) and the full complement of advanced Call Vectoring (conditional routing) capabilities. The Elite package includes Avaya Virtual Routing for effective load-balancing across multiple sites, and Business Advocate to dynamically match each customer to the optimal agent.

  Call routing types include:

  - Expert Agent Selection (EAS): Avaya Aura Call Center Elite has a feature of, where agent selection is done based on the best available agent for that specific call. This is based on the expertise level for all agents on that skill. This expertise level needs to be set in Avaya Aura Call Center Elite. There are 16 expertise levels. If all agents are set at equal expertise level, then it would route the call to most idle agent.
  - Least Occupied Agent (LOA): Call Center Elite can be configured so that the calls are equally distributed among all the agents in the skill. The Least Occupied Agent call distribution method considers an agent's total call occupancy rate since logging on, not just how long it has been since the agent's last call

- Avaya Aura Enablement Services (AES)

  Avaya Application Enablement Services (AES) is a software platform that leverages the capabilities of Avaya Aura Communication Manager. AES provides an enhanced set of Application Programming Interfaces (APIs), protocols, and web services that expose the functionality of Avaya Communication solutions to corporate application developers, third-party independent software vendors, and system integrators. AES provides a platform that supports existing call center application requirements, along with new, emerging APIs.

- Avaya Control Manager

  Avaya Control Manager is a centralized administration tool for the Avaya environment allowing administrators to manage users, agents, skills, extensions and all other Avaya related objects from a single, web-based application. Administrators become more productive as agent provisioning and skill assignments take a fraction of the time required before, maximizing preparedness for customer interactions. With Control Manager, administrators can unify, streamline, and centralize the management of Avaya Call Center operations. In addition, the administrator can track events and take necessary action to meet customer needs.

- Avaya Call Management system (CMS)

  Supervisor users who access the real-time, historical, and integrated reports subsystems using the two methods of accessing CMS reports which include CMS Supervisor Web and CMS Supervisor Personal Computer (PC) client. It outlines how reporting works and the reports that are available.

- Avaya Aura Workforce Optimization (WFO)

  Avaya Quality Monitoring (QM): QM is a software application customarily used for call center quality monitoring and performance optimization. With QM, the voice interaction along with agent screen activity can be captured for later review and evaluation. Voice and data (screen) can be randomly captured or recorded based on user-defined business rules. The QM application uses the Contact Recording Package as the underlying recorder in a Quality Monitoring implementation.

  Quality Evaluation Optimization: Assessment program solution service examines your organization's unique business drivers and goals. Then, it maps these to your quality monitoring evaluation forms and scoring schemes, and introduces best practices to reinforce them. The service can help you drive more effective performance management that can deliver a real competitive advantage

The IVR telephony infrastructure uses a high-availability, real-time interface with the CRM system and evoBrix PMIS to accomplish the following:

- Create tickets in the CRM system for all calls.
- Track caller actions within the IVR system and report them to the CRM application.
- Authenticate callers with information provided by the caller against the CRM and evoBrix PMIS data store.
- Play back information requested by the caller by retrieving the real-time data from evoBrix PMIS and the CRM system.
- Transfer the call to a customer service representative using the computer–telephony interface. Caller information is passed on, so that the customer service representative has the relevant caller information available.

Figure 3.10.14-43 provides an overview of Team CNSI's Avaya IVR Business Architecture. The figure describes trigger point functionalities provided by Team CNSI's Avaya IVR.

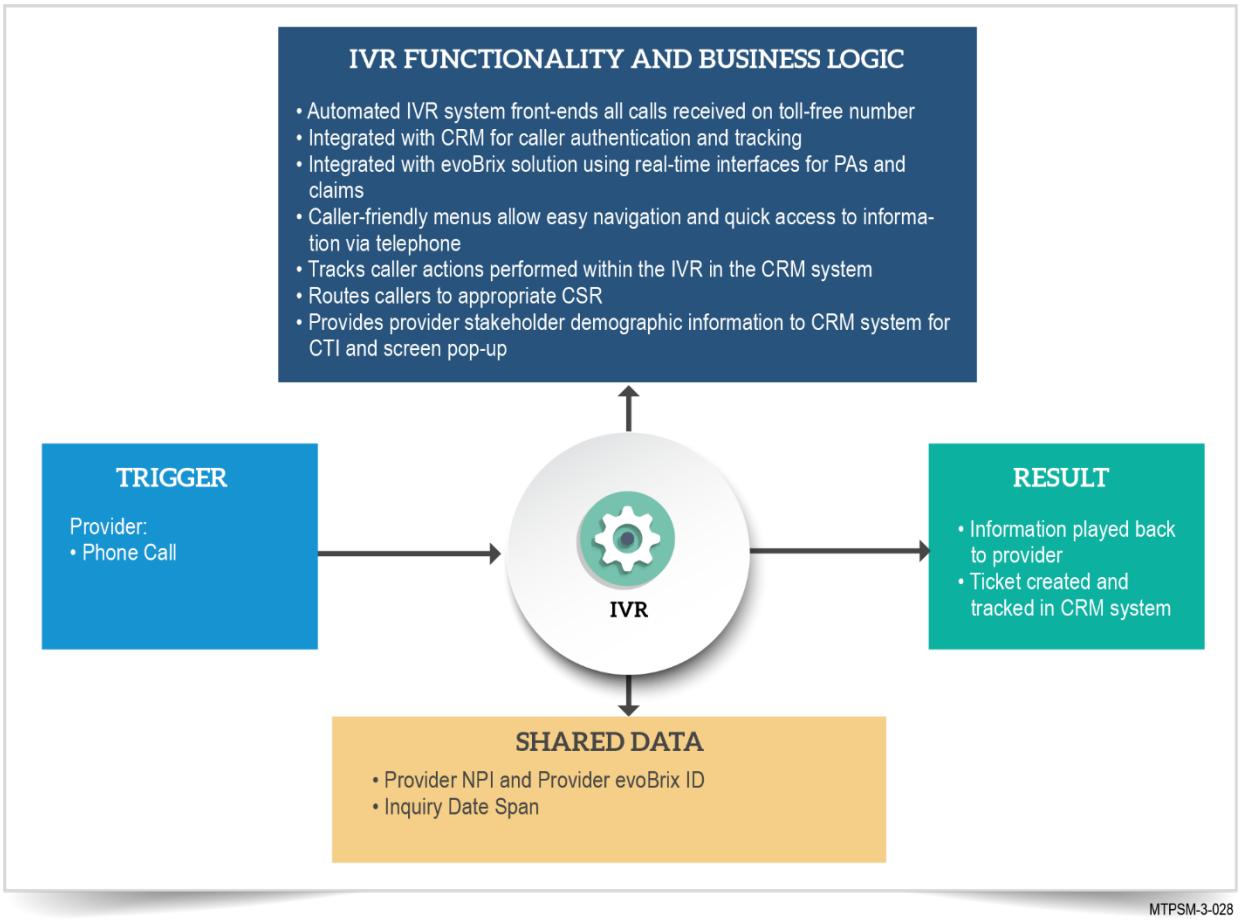


Figure 3.10.14-43. Business Architecture for the Proposed Team CNSI's IVR Solution. Our effective IVR process flow solution provides a cost-efficient and scalable model.

Figure 3.10.14-44 describes Team CNSI's Avaya IVR solution benefits.

Benefits of Team CNSI's IVR	Description
Proven track record	Team CNSI's Avaya IVR solution has been implemented successfully for Washington Medicaid system and is being developed for State of Utah Medicaid system.
Easy to integrate	Our systems are integrated using standard web services and common https protocol.
Support for Session Initiation Protocol (SIP)	SIP reduces the complexity of the systems and provides the capability for the Call Center to be truly Multi Channel Call Center (provides support Voice, E-mail, message, FAX and Chat)
Detailed call tracking and monitoring enterprise application integration (EAI) framework	Team CNSI's IVR solution is designed to create activity within the CRM system for IVR calls. This gives a 360-degree view of each contacts to call center at single place. This reduces the time spent to connect the dots, in case of issues and also provides a seamless experience to the caller.
Provides multichannel support for Email, messages, FAX, and Chat	Team CNSI's IVR solution can be easily configured for multi-channel support.

Benefits of Team CNSI's IVR	Description
Enhanced cost benefits	As more and more calls are front ended, overall efficiency is improved, providing significant operational cost benefit to DPHHS. Increasing self-service utilization decreases call center operations costs while increasing first-contact resolution.

Figure 3.10.14-44. CNSI's IVR Benefits. Team CNSI's Avaya IVR solution has many benefits.6

Contact Tracking Using CRM

Team CNSI's CRM solution has a service request module, which is used to manage and track provider and other stakeholder inquiries. Each service request has a unique identifier, Service Request ID (SR ID), which is auto-generated in the CRM application when a new service request record is either manually created by a CSR using CRM or a real-time CRM Web services invocation or using batch jobs. Each service request has an owner, and can be categorized based on Area, Type, and Reason. Since IVR creates Services Request and relative Activities within the CRM system, IVR calls can be easily tracked within Team CNSI's CRM solution.

IVR01

The Contractor shall provide and maintain secure and user friendly interactive voice response (IVR) system with scripts approved by the State to respond to inquiries using a telephone menu and response system.

Team CNSI will operate the IVR system with scripts approved by the State to respond to inquiries using a telephone menu and response system. Each call within Team CNSI's IVR system is initially answered and greeted by the IVR system. Callers will be prompted for language preferences and requested to enter identifying information (e.g., provider NPI) for authentication. Once authenticated, the caller will be presented with a list of transfer and self-service options.

Team CNSI will host an IVR system for the State which will be both secure and user friendly. To ensure that Team CNSI's IVR system is user friendly, Team CNSI will take the following measures:

- Incorporate user-friendly language: Present voice prompts in the user's language and in a friendly tone.
- Avoid jargon: Avoid use of technical terms and unfamiliar acronyms which are difficult for the caller to understand.
- Be precise: Use short and concise phrases for menu items which are easier to remember.
- Explain customer errors: If an error occurs in the IVR system, the caller will be told what the error was, and the type of correct input is expected will be explained in more detail.
- Enable DTMF and Speech Input: Allow the provider to provide their inputs by using phone touchpad or by speaking.
- Provide easy access to talk to a CSR: Provide the option to talk to a CSR in all menus.
- Play informative messages: Play holiday or outside of office hours messages after the welcome message to let the provider know that the Call Center is closed.
- Play Alerts: Play system alerts and provider-specific alerts to the provider.

To host a secure IVR, Team CNSI's IVR will take the following measures

- Use Session Border Controller: Session Border Controller is a component in the Avaya IVR Architecture comes with SIP firewall to detect Intrusion Detection and Prevention System. It supports policy configuration to disallow external calls, transfers, and forwards from certain domains, users, or untrusted environments.
- Communication using https: All the web service calls from IVR will be using https protocol for secured transaction.
- Authentication: The IVR Business Logic rules will ensure that the provider access only his/her data. The caller has to first authenticate and then provide necessary information (as per the rules) to retrieve any details from the IVR.

Figure 3.10.14-45 provides an overview of the Team CNS IVR solution logical process flow illustrating evoBrix-Siebel-IVR integration and the communication protocols. The Figure provides a high-level overview of how different components are integrated in Team CNSI's IVR solution.

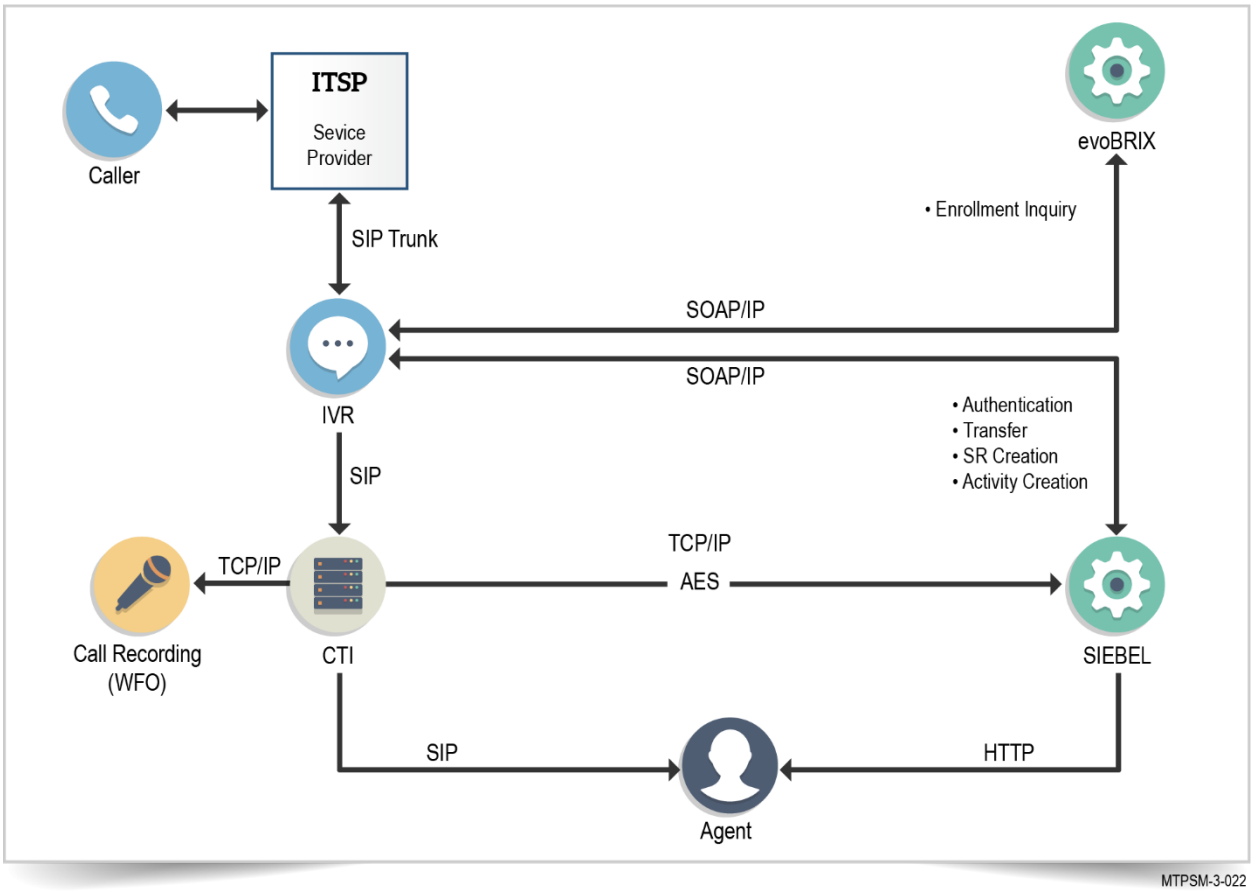


Figure 3.10.14-45. System Overview for the Proposed Team CNSI Solution. Our call center business architecture, functionality, triggers, shared data, and result provides a cost-efficient, scalable model for development.

Team CNSI's IVR solution is closely integrated with our CRM solution and MMIS using a Web services framework. The common reusable services enable the system to respond consistently across the different access channels. Team CNSI's IVR solution provides two levels of authorization verification for all supported transactions:

- Web service based authentication using CRM web services for provider authentication.

- MMIS web services enforce all business and data access rules which are defined to the web service responses. This enables for a central security and authorized access across communication channels.

The following self-service options will be available in the IVR for providers:

- Enrollment inquiry

Other than above self-service options, the current IVR solution can create service requests using IVR, providing system alerts and provider-specific alerts. In a case where the caller cannot be serviced in the IVR, the caller will be routed to the appropriate queue based on selection.

The figure below provides an overview of the IVR call flows. When the provider makes a phone call to the call center, the call reaches the IVR. The IVR plays a welcome message to the caller and attempts to authenticate the caller. After the authentication process completes (whether the caller is authenticated successfully or not), the caller is presented with the main menu. The main menu consists of a number of self-service options and transfer options. If the caller choses one of the self-service options, then the IVR checks whether the caller was successfully authenticated during the authentication process. If the caller was authenticated then the caller is presented with a sub menu and the flow continues as per the design. Otherwise the caller is sent to the Call Center using the appropriate queue. Also, if the caller chooses a transfer option from the main menu, the caller is transferred to an appropriate queue. For IVR call tracking, a service request is created after the authentication process is over and an activity is created and associated with the service request after each activity the caller performs in the IVR.

Figure 3.10.14-46 represents the overview of the Team CNSI's IVR call flow.

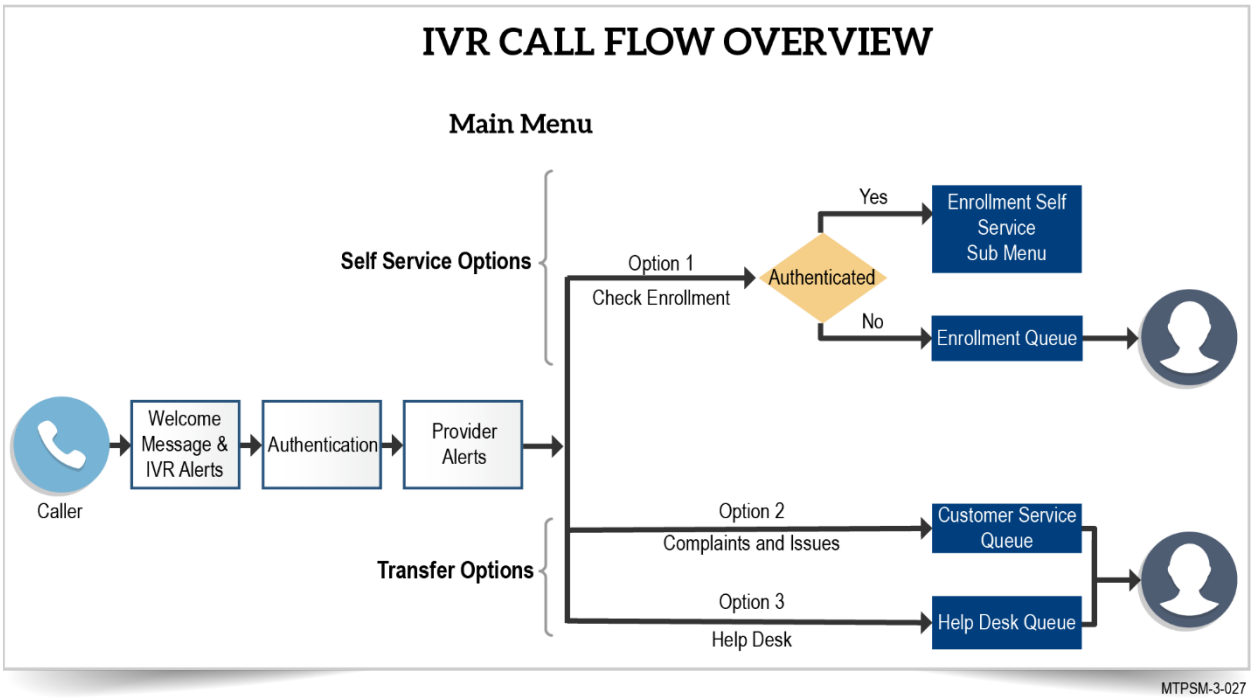


Figure 3.10.14-46. IVR Call Flow Overview. An overview of the IVR call flow illustrating authentication process and menu.

IVR02

The Contractor's IVR system shall have the ability to use educational scripts for callers on hold or waiting in the queue.

Team CNSI's IVR solution will use Avaya Communication Manager (ACM) for call routing and CTI functionality. When a call is on hold waiting to be answered by a CSR, ACM will play educational scripts to caller based on the rules defined. Team CNSI will use messages or scripts approved by the State to play those messages. Depending on the approval from the State, the message can be played once or multiple times. When the call is ready to be transferred to an available agent, the scripts will be interrupted.

In addition to playing educational scripts on ACM, Team CNSI's IVR solution has extensive capability to play System Alerts and provider-specific alerts. These alerts can be utilized for playing educational scripts as well. Refer to Figure 3.10.14-46 for details on the IVR call flows.

IVR03

The Contractor's IVR system shall provide quality monitoring tools and processes to enable a continuous improvement cycle for toll-free call center services that includes:

a. Plug-in/double-jack monitoring,

b. Silent monitoring,

c. Record and review

d. Voice and screen/multi-media monitoring, for call center supervisors, State resources or designated resources.

Team CNSI's IVR uses Avaya Workforce Optimization (WFO) Select for quality monitoring and call recording. Avaya Workforce Optimization Select is a web-based suite of tightly-integrated tools designed to enhance and improve all aspects of the call center operations and performance. The solution is easy to implement, maintain, and manage in a variety of call center deployment models from centralized call centers to distributed branches and work-at-home agents. Team CNSI will also set up supervisors for live monitoring of voice and screen.

Team CNSI's Avaya WFO Select solution provides all the features in the requirement above along with additional features. Please find a detailed list of features in Figure 3.10.14-47.

Features of Avaya WFO	Description
Call Recording	■ Record inbound and outbound calls selectively or in bulk
Quality Monitoring	■ Synchronized voice and on-screen agent activity. ■ Customized agent evaluation forms tailored to business needs
E-learning and coaching	■ Recorded contacts to help agents and learn hand in hand ■ Assign lesson plans to agents which the agent can learn at own ease
Speech and data analytics	■ Index and organize recordings ■ Find the calls based on key words
Performance management/scorecards	■ Vital feedbacks for the performance along with the performance

Figure 3.10.14-47. Avaya WFO Features. All the features available in Avaya's WFO.

In addition to the WFO tools and processes described above, Team CNSI has comprehensive reporting capabilities to ensure our Call Center operations are running smoothly and meeting expectations over time. Team CNSI's Avaya solution supports interactive logging of all transactions and the comprehensive ability to report call statistics. The reports available can broadly be categorized into two types as described in Figure 3.10.14-48. The listed reports provide a 360-degree view of the Call Center performance. Additional reports can be configured as per the State's need during solutioning session.

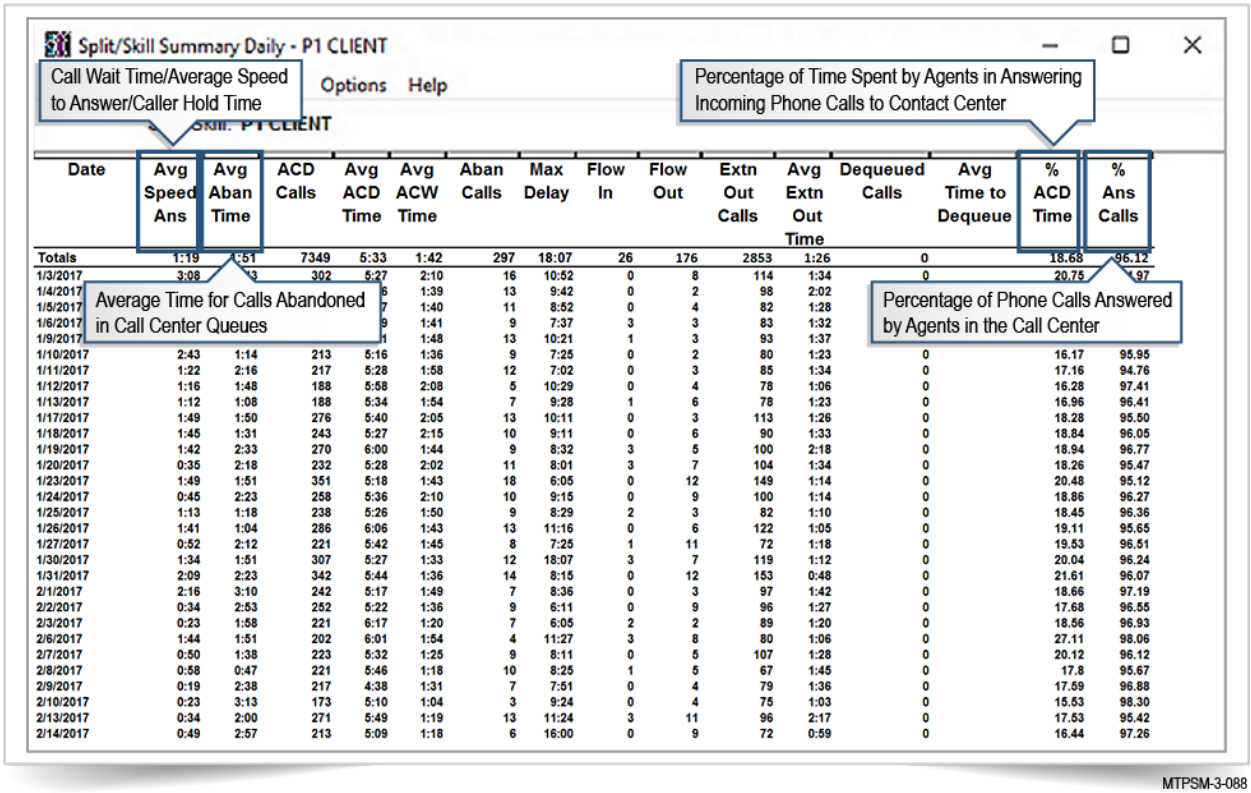
Report Type	Description	Report Names
Avaya CMS / Call Center Reports	Provide details on the overall functioning of the call center. Avaya CMS reports can be real-time reports, historical reports, or integrated (combination or real time and historical) reports. Additional reports can be configured as defined during solutioning activities.	■ Skill Status Report ■ Agent Group Report ■ Daily Summary Report ■ Agent Graphical Information Report ■ Skill Comparison Report
Avaya Aura Experience portal / IVR Reports	Provide details on all the transactions that is performed during the IVR calls and overall performance of the IVR systems. These reports can be generated on a pre-defined schedule or on demand.	■ Application Summary Report ■ Application Detail Report ■ Call Summary Report ■ Call Detail Report ■ Session Detail Report ■ Performance Report ■ Active IVR Calls Report ■ System Monitor Report

Figure 3.10.14-48. Call Center Reports. Various report available in the Team CNSI's IVR and Call Center solution.

CMS reports provide in depth details about the Call Center performance. These reports can be used to find the Call abandonment rate, average time prior to abandonment, calls placed on hold along with other details such as percentage of calls answered within set service levels, how many calls were handled, and summarizing activity. Reports can be obtained for a single skill or multiple skill. Reports can be also be obtained for any timeframe including hourly or daily.

The following report provides information on call abandonment rate, and average time prior to abandonment, including for calls placed on hold.

Figure 3.10.14-49 shows daily summary report for a single skill over a 30-day period.



Date	Avg Speed Ans	Avg Aban Time	ACD Calls	Avg ACD Time	Avg ACW Time	Aban Calls	Max Delay	Flow In	Flow Out	Extn Out Calls	Avg Extn Out Time	Dequeued Calls	Avg Time to Dequeue	% ACD Time	% Ans Calls
Totals	1:19	:51	7349	5:33	1:42	297	18:07	26	176	2853	1:26	0		18.68	96.12
1/3/2017	3:08	:3	302	5:27	2:10	16	10:52	0	8	114	1:34	0		20.75	.97
1/4/2017			6		1:39	13	9:42	0	2	98	2:02				
1/5/2017			7		1:40	11	8:52	0	4	82	1:28				
1/6/2017			9		1:41	9	7:37	3	3	83	1:32				
1/9/2017			1		1:48	13	10:21	1	3	93	1:37				
1/10/2017	2:43	1:14	213	5:16	1:36	9	7:25	0	2	80	1:23	0		16.17	95.95
1/11/2017	1:22	2:16	217	5:28	1:58	12	7:02	0	3	85	1:34	0		17.16	94.76
1/12/2017	1:16	1:48	188	5:58	2:08	5	10:29	0	4	78	1:06	0		16.28	97.41
1/13/2017	1:12	1:08	188	5:34	1:54	7	9:28	1	6	78	1:23	0		16.96	96.41
1/17/2017	1:49	1:50	276	5:40	2:05	13	10:11	0	3	113	1:26	0		18.28	95.50
1/18/2017	1:45	1:31	243	5:27	2:15	10	9:11	0	6	90	1:33	0		18.84	96.05
1/19/2017	1:42	2:33	270	6:00	1:44	9	8:32	3	5	100	2:18	0		18.94	96.77
1/20/2017	0:35	2:18	232	5:28	2:02	11	8:01	3	7	104	1:34	0		18.26	95.47
1/23/2017	1:49	1:51	351	5:18	1:43	18	6:05	0	12	149	1:14	0		20.48	95.12
1/24/2017	0:45	2:23	258	5:36	2:10	10	9:15	0	9	100	1:14	0		18.86	96.27
1/25/2017	1:13	1:18	238	5:26	1:50	9	8:29	2	3	82	1:10	0		18.45	96.36
1/26/2017	1:41	1:04	286	6:06	1:43	13	11:16	0	6	122	1:05	0		19.11	95.65
1/27/2017	0:52	2:12	221	5:42	1:45	8	7:25	1	11	72	1:18	0		19.53	96.51
1/30/2017	1:34	1:51	307	5:27	1:33	12	18:07	3	7	119	1:12	0		20.04	96.24
1/31/2017	2:09	2:23	342	5:44	1:36	14	8:15	0	12	153	0:48	0		21.61	96.07
2/1/2017	2:16	3:10	242	5:17	1:49	7	8:36	0	3	97	1:42	0		18.66	97.19
2/2/2017	0:34	2:53	252	5:22	1:36	9	6:11	0	9	96	1:27	0		17.68	96.55
2/3/2017	0:23	1:58	221	6:17	1:20	7	6:05	2	2	89	1:20	0		18.56	96.93
2/6/2017	1:44	1:51	202	6:01	1:54	4	11:27	3	8	80	1:06	0		27.11	98.06
2/7/2017	0:50	1:38	223	5:32	1:25	9	8:11	0	5	107	1:28	0		20.12	96.12
2/8/2017	0:58	0:47	221	5:46	1:18	10	8:25	1	5	67	1:45	0		17.8	95.67
2/9/2017	0:19	2:38	217	4:38	1:31	7	7:51	0	4	79	1:36	0		17.59	96.88
2/10/2017	0:23	3:13	173	5:10	1:04	3	9:24	0	4	75	1:03	0		15.53	98.30
2/13/2017	0:34	2:00	271	5:49	1:19	13	11:24	3	11	96	2:17	0		17.53	95.42
2/14/2017	0:49	2:57	213	5:09	1:18	6	16:00	0	9	72	0:59	0		16.44	97.26

Figure 3.10.14-49. Daily Summary Report. Overview of a daily summary report for a range of days in a specific skill in the Call Center.

3.10.14.6 Staffing

This section addresses requirements for Provider Call Center staffing. The Offeror's proposed Option B services must include staffing to review provider information, maintenance requests and all supporting materials, in order to verify provider changes, prior to updating the provider records. The Contractor will review and approve or deny low risk, high volume enrollments per Agency criteria. Moderate and high-risk enrollments will be routed to and reviewed by Agency internal staff before a final enrollment decision is made. The Offeror must describe their approach to meet each of the staffing requirements defined in Attachment F, Requirements Matrix.

Team CNSI brings the proven ability to manage efficiency and quality of healthcare operations. In today's healthcare market space, administrative services must continually be performed with greater efficiency without sacrificing quality. While the solution brings the technology necessary to achieve this goal, our approach to operations management is treated with equal rigor and priority. Our experience running operations in multiple states for decades has shown us that technology cannot achieve the operational goals on its own; success requires the right people using it correctly to reach its full potential. Team CNSI has re-engineered its service delivery models to infuse greater efficiency and higher quality to its customers. This has enabled our call center service functions to be governed based on Lean Six Sigma principles throughout our team, bringing enhanced productivity and quality to many functions in our provider management services portfolio. Incorporating Lean-based strategies has had two important outcomes at Team CNSI and for our customers. First, Lean processes have driven efficiencies and cost reductions; and second, the adoption of Lean Management practices has helped transform the culture of front-line managers to enable sustained process improvements.

Optimizing a process using Lean principles is not a one-time activity, however. Sustained optimization requires cultural change management that focuses on Lean approaches to consistently identify and enact process improvements in daily operations. Team CNSI gives data, tools, and coaching to our leaders so they can achieve, maintain, and continue to refine desired productivity and quality. It is this focus on well-equipped management that enables us to develop productive staff that consistently achieve a high quality. Even when teams are led by experienced management that consistently meet SLAs, we have learned that adoption of a Lean Management model has resulted in efficiency gains of up to 50 percent in individual processing steps. Team CNSI member, Noridian, found up to 50 percent improvement in productivity for provider enrollment and appeals process steps, and continues to further refine all processes to achieve continual improvement gains. In addition to these accomplishments, Team CNSI has created customized processes that ensure productivity standards are not only reviewed monthly or weekly as in many operations; but productivity is monitored daily and even hourly, assuring Team CNSI's customers it has the tools in place to identify any workload spikes immediately. This allows for remediation steps to be taken promptly, mitigating the risk of adverse impact to achievement of SLAs. These practices are now a part of the fabric that positions us to bring excellence in the delivery of healthcare administrative services.

The Team CNSI Advantage

Team CNSI brings over 50 years of experience supporting providers through the complex healthcare system. In fact, we have been supporting Montana healthcare providers for 11 years. This experience enables us to:

- Create approaches that are tailored to rural provider settings, ensuring rural and urban providers receive the same access and support
- Identify and train staff to provide excellent service to providers from initial point of contract through ongoing support
- Cross-train and manage staff to achieve all service level agreements
- Continue to innovate and manage operations to enhance support

MTPSM-3-235

Team CNSI brings 11 years of experience supporting Montana's healthcare provider community. In fact, Team CNSI member Noridian currently supports all Medicare Parts A, B and DME providers in Montana. In the past decade Noridian has developed relationships with many of the Montana providers and is familiar with some of the challenges that Montana faces. Headquartered in Fargo, North Dakota, Noridian understands the challenges that are unique to largely rural states, and has adapted its approaches to bring excellent service to rural providers as well as those providing care in more urban settings. We will adapt these successful experiences and tailor to reach the Medicaid provider community successfully and with emphasis on quality service.

STF01

The Contractor shall provide staffing to perform provider enrollment tasks defined by the Agency to include at a minimum:

-Receive, review and verify provider information submitted to the screening process;
-Verify provider data against Provider databases and the NPPES;
-Notify providers to request additional documentation as needed;
-Determine provider status;
-Update provider record with all necessary enrollment data;
-Process and store provider agreements;
-Send financial enrollment data to State's financial system;

©2017 CNSI | Option B-62

-Activate provider enrollment for benefits/claims transactions in the Benefits Management system;
-Review provider information maintenance requests and all supporting materials; and
-Verify provider changes prior to updating the provider records.

Staffing levels shall be maintained to meet enrollment process SLA's for timeliness and accuracy.

Team CNSI acknowledges STF01 and agrees to comply with its corresponding SLAs.

We use our past experience meeting provider enrollment service levels to assure appropriate staffing levels are met and maintained throughout the life of the contract. Through team member, Noridian, Team CNSI has been supporting healthcare administrative services and provider enrollment for decades, dating back to the inception of the Medicaid program. Throughout our rich history of administering healthcare, Team CNSI's members have continued to grow, improve, and innovate. These individual advancements are now assembled as a cohesive team bringing success administering a wide variety of healthcare administrative services, each having contributed to the continued adaptation and success that DPHHS can rely on. Our processes continue to adapt and change with industry standards, legislation, and changes to data sources such as NPPES evolve over time. Highlights of Team CNSI's service performance include:

- Educating over 340,000 healthcare providers and suppliers
- Enrolling and credentialing nearly 750,000 active Medicaid providers
- Operating a full-service provider contact center with over 2.4 million calls per year achieving a 97+% first call resolution rate
- Managing operations for over 20 million Medicaid- and Medicare-covered lives.

This experience prepares Team CNSI to identify qualified resources, recruit, and train staff to take on the identified provider enrollment tasks.

STF02

The Contractor shall provide Provider Enrollment Call Center staffing sufficient to maintain services that meet or exceed the Service Level Agreements for the Call Center productivity. The Contractor shall describe its staffing model that includes the ratio of staffing to Call Center operation volume (including, for example: total Call Center volume, average call wait time, rate of abandoned calls, length of call, open vs. closed trouble tickets).

Team CNSI considers the total number of providers, anticipated new provider enrollment, the numbers of moderate-risk and high-risk providers, and the expected number of contact per provider type to anticipate the total workload. The team CNSI staff model includes staff to support three primary workstreams. A summary of the approach to establish staffing for each category is provided.

- Provider Site Visits. Team CNSI evaluates the total number of site visits based on the numbers of providers in each risk category and evaluates an average monthly number of visits. We then establish a relative schedule for revalidation, giving us some insight into which provider groups will require site visits at what times of the year. Our approach distributes staff across the state and site visits are assigned to the staff person closest to the site to be visited. This approach limits staff travel time and manages travel costs.

©2017 CNSI | Option B-63

- Provider Call Center. Team CNSI uses existing contract experience to anticipate the number of provider inquiries we are likely to receive based on the advanced Team CNSI technology solutions and our experience in implementing those solutions. For this work, we assume that significantly fewer providers will be placing calls to the call center for assistance with enrollment. This can be achieved through the implementation of Team CNSI's evoBrix PMIS solution which intuitively walks providers through the application process. This user-friendly application, coupled with provider computer-based training and webinar demonstrations, will assure that providers have the tools they need to enroll and update enrollment with minimal call center assistance.

- We use the anticipated call volume and our historical ability to achieve a 97 percent rate of first call resolution to design our staffing solution. Our experience is supplemented by the historical call length DPHHS has cited to support an expected 5-minute average call length. We routinely meet our client's expectations for contact center support with an average speed of answer of 60 seconds and are committed to achieving that same service for DPHHS and Montana's Medicaid providers. Using Montana's provider metrics, we anticipate a daily call volume under 100 calls. Our staffing approach has a ratio of one full time equivalent to roughly 50 calls each day.

- Team CNSI uses industry standard tools for assessing call center staffing models, such as the Erlang C staffing calculator. This model requires that metrics such as confidence level, abandon rate, amount of time between calls (wrap time) and average call length be entered to calculate the number of agents required to perform the work. This is supplemented with the predicted number of calls received per hour to calculate required number of agents. It is important to note that calls are not received in equal distribution throughout the day. Therefore, it's necessary to staff to meet the peak volume of calls per hour to assure that daily metrics are achieved. Taking this into account, we estimate four call center agents are required to support the base-level provider count for the contract.

- Provider Enrollment Processing and Data Matching. Team CNSI's advanced, highly automated provider management solution presents significant opportunity for provider self-service, and automates many of the processes required to review and credential a provider. As a result, we are able to be very lean in the staffing required to support providers through this process. Our experience successfully implementing this solution in multiple states brings the expertise to accurately predict the length of time required to complete new application review as well as perform review of application changes or updates. These staff are assigned to handle any mismatched information and make corrections to the financial systems as needed.

Team CNSI provides oversight, quality assurance, and training for all staff to assure SLAs are achieved. The use of Team CNSI's innovative HealthBeat dashboard provides real time insight to the operations team's productivity and performance. We believe that regular monitoring of not only monthly metrics, but also weekly, daily, and hourly metrics allow us to focus on achieving Lean operations, focused on high efficiency and strong quality. Early visibility to any performance slumps allows us to proactively make adjustments long before SLAs are in jeopardy.

STF03

The Contractor shall designate at least one (1) in-state staff position to conduct site visits. This position is considered to be a key staff position. Other staff will need to be available as necessary to meet SLAs for site visits. Please describe how you can meet the requirement with at least two (2) staff positions for site visit coordination.

©2017 CNSI | Option B-64

Based on Montana's provider population, Team CNSI will designate two staff in the state to conduct site visits. These staff will telecommute from two separate locations in the state to provide coverage across Montana's significant geographic footprint; placement of staff is strategically evaluated for each state and the approach may differ for other NASPO states. Team CNSI identifies providers in each risk category and creates a schedule for revalidation. We create a balanced stream of revalidation workload to best use staffing resources, minimize any "bubbles" of workload, and not create unnecessary burden for the providers. To that end, we evaluate the provider's risk category, last validation date, and schedule the provider for a revalidation timeframe, assuring that providers are revalidated in the timeframe appropriate for their risk level. When factoring in the total number of moderate risk level providers being revalidated every five years and the high-risk level providers being revalidated every three years, this nets an average of 375 site visits that must be performed annually. We add this to the 500 annual new site visits defined in the RFP to generate an average of 72 site visits that must be performed each month. It is reasonable to accomplish this work with two staff based on our approach that conducts multiple visits during each trip, grouping revalidation visits with visits to newly enrolling providers.

When possible, team CNSI will also consider geographic location as the revalidation schedule is established. To maximize cost efficiency, staff will be scheduled to visit locations near each other to conduct multiple site visits. When site visit staff are not performing site visits, they are available to respond to provider inquiries and review provider enrollment applications. This approach to staffing assures that 1) staff are productive when no site visits are scheduled, and 2) the staff conducting site visits stay informed of enrollment processes and new information to remain knowledgeable and able to respond to provider inquiries. Figure 3.10.14-50 shows the Medicare distribution of providers and suppliers across Montana; we will generate a similar map for Medicaid providers to assist us in selecting staff from areas of greatest provider population density, as well as identifying the areas to which we'll most often travel.

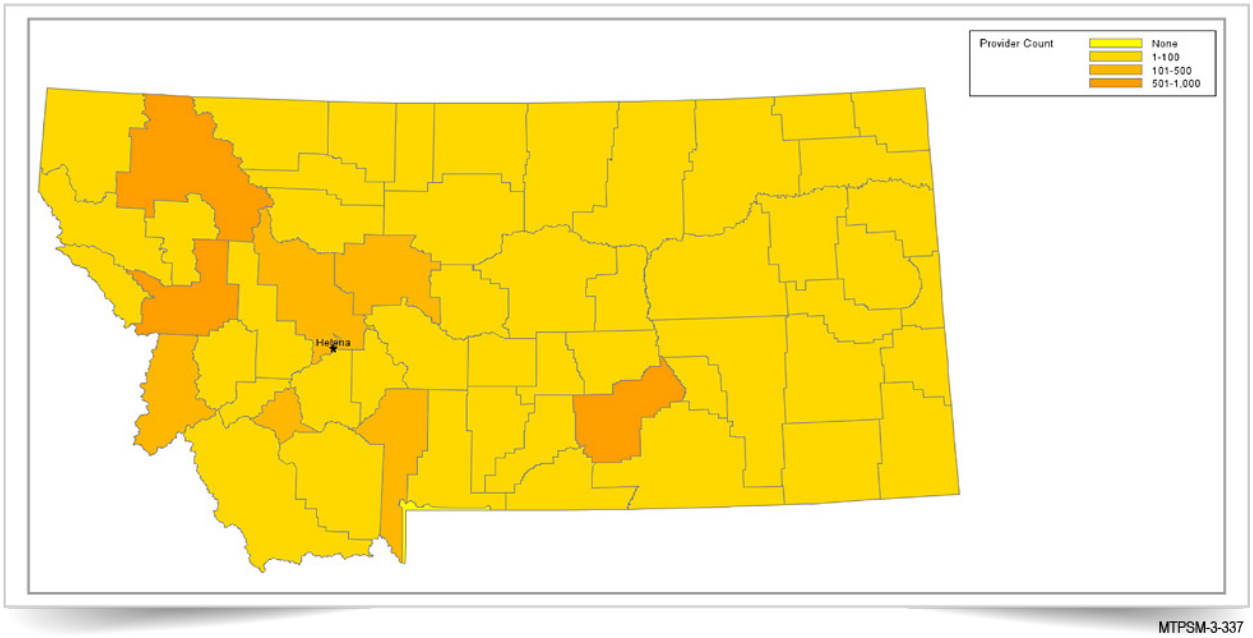


Figure 3.10.14-50. Montana Provider Heat Map. Team CNSI maps out the density of providers across the state to assist in planning for site visits.

STF04

The Contractor shall designate a Business Operations Manager to lead the Contractor's Business Operations for Provider Screening, Enrollment and Monitoring, including:

-Document Management and Workflow Performance

-Provider Data Management

-Provider Support Services (training and site visits)

-Provider Enrollment Call Center

-Financial Enrollment Process coordination with State Auditor's Office (SAO)

This position is considered to be a key specific management position.

Team CNSI has selected Ms. Martha Kittrell as its Business Operations Manager. Ms. Kittrell brings experience from her positions as Operations Manager and Provider Enrollment Manager, augmenting the team with valuable provider management qualifications. She brings:

- Over a year of experience managing the implementation of a Medicaid Provider Enrollment project, overseeing 15 FTEs and three site visit specialists.
- Management of the transition of paper enrollment to electronic enrollment for Medicaid providers through the Department of Health Care Finance.
- Over five years overseeing organization costs, quality and productivity by monitoring, tracking and reporting on team accomplishments, achievements, and productivity, as well as maintaining reports and presentations on department performance
- Over a year of experience supporting member outreach and conducting training/briefing sessions, including benefit counseling; referral for care support; claims and enrollment support services to customers; and coordinating health care services with case managers
- Over a year of experience as Member Advocate/Specialist, working directly with members and health plans to provide health education for services available in the community
- Over five years of experience managing two call centers: Provider Enrollment/Re-enrollment and Provider Call Centers of over 15 FTEs, identifying and analyzing issues, planning tasks, implementing solutions, and recommending and implementing changes to improve efficiency and effectiveness

OMC24

The Contractor will provide 250 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 250 system enhancement pool hours are included in the offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.

The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

Team CNSI will accommodate the request to provide 250 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 250 system enhancement pool hours are included in the offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.

Team CNSI agrees that the unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

OMC25

The Contractor will provide 100 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 100 system enhancement pool hours are included in the Offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G Pricing Schedule, Schedule D-Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours.

Team CNSI will accommodate the request to provide 100 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 100 system enhancement pool hours are included in the Offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

Team CNSI agrees that the unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G Pricing Schedule, Schedule D-Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours.

3.10.14.7 Collect and Enter Provider Financial Information in State Financial Systems

This section outlines the requirements for the collection of provider financial information and data entry requirements into the State's financial system. The Offeror's proposed Option B services must include the services to support the collection of financial packet/information from providers and enter the information into a state financial system. The Contractor services will include following up with the provider in the event discrepancies are identified by State auditors. Activities would also entail subsequent work from the

provider's submission of initial financial information and includes essential updates to financial information. The Offeror must describe their approach to meet each of the requirements to collect and enter provider financial information in state financial systems defined in Attachment F, Requirements Matrix.

Accurate financial information is essential to managing the provider payment processes successfully. Team CNSI's evoBrix Provider Management Information System (PMIS) provides a powerful platform for enrollment and provider data collection. During the enrollment process, Team CNSI collects provider financial information, along with demographics and other provider characteristics. Financial information includes:

- Business name
- Business address
- IRS Employer Identification Number (EIN)
- Bank account number
- Bank routing number

The Team CNSI Advantage

Team CNSI has established ISO 9001:2015-based processes for managing provider communication, interaction, and information processes.

- Every interaction with providers is maintained in Siebel CRM for holistic customer service
- PMIS provides a powerful online provider data collection platform, with a full history of updates, for our staff to use to enter data in state financial systems
- PMIS includes an online IRS Form W-9 update capability for providers

MTPSM-3-069

This information is ideally collected directly from the provider during enrollment or during provider updates performed online using the evoBrix PMIS. As needed and as requested by the State, including if State auditors identify discrepancies, Team CNSI business operations staff will also reach out to providers to gather the financial information. Team CNSI communicates financial requests to the provider, and the provider logs into the evoBrix PMIS to enter the data. An evoBrix PMIS report will be used to pull the provider financial information, and Team CNSI business operations staff will enter it into the appropriate state's accounting system. All interactions with the provider are maintained in Siebel CRM to provide a longitudinal record of provider communications.

- While Siebel CRM is used to track provider interaction, Team CNSI uses Open Source Ticket Reporting System (OTRS) to manage business workflow and actions between Team CNSI and the State. During operations, Team CNSI uses OTRS to track, manage, and complete all work requests from State staff. Requests for research, collecting financial information, and updating state accounting systems are all tracked in OTRS from initiation to closure. By doing so, our business operations manager can monitor tickets, resolve any roadblocks, reassign tickets, and report Service Level Agreement (SLA) performance.

The following provides our specific responses to the requirements provided in Attachment F of the Solicitation.

SFMS01

The Contractor shall research and resolve all TIN Mismatch Reports which show all Tax ID's that have returned a mismatch error from the TIN Matching process.

State accounting systems may receive a list of missing or incorrect payee name/TIN from the IRS. IRS first B Notices are sent by State staff to providers if the mismatch is not resolved. Team CNSI will use TIN Mismatch Reports provided by the State to research the mismatches. Team CNSI's business

operations staff will review the mismatch report received from the State Accounting System/IRS against the respective provider's name/TIN information. Team CNSI will review historical name/TIN changes made within the respective calendar year for the providers listed in the mismatch report. Team CNSI's business operations staff will review and approve the changes, and they may reach out to the provider to request the provider to update the W-9 information on file. Team CNSI's evoBrix PMIS provides an online self-service capability to enable providers to update their W-9 information. OTRS will be used to track the TIN mismatch resolution activity.

SFMS02

The Contractor's staff will follow-up with providers regarding any discrepancies identified by the state auditor and the IRS regarding Backup Withholding "B" notices, 1099s, including FEINs. Enter any corrections needed in the applicable state financial system.

As discussed in SFMS01, Team CNSI will conduct research and resolve any discrepancies related to financial information identified by the states. Once the provider record is updated in the evoBrix PMIS, either by the provider or by Team CNSI business operations staff, Team CNSI will generate a report of financial information and use the data to update the state financial system. Team CNSI will conduct the following steps to resolve discrepancies and update the state financial system:

1. Team CNSI's business operations staff will make a phone call to the provider.
2. If the phone call is not successful, our staff will send an email to the provider requesting resolution.
3. We will confirm the accuracy of the information in the evoBrix PMIS. If not accurate, the financial information will be corrected in the evoBrix PMIS either by our staff or by the provider.
4. Our staff will generate a report containing a workflow task summary and the updated information documenting the correction.
5. A second staff member will review the financial information and updates.
6. Assuming the corrections are accurate, the second staff member will update the data in the state financial system.

The workflow will be tracked and managed using OTRS and will be completed within two business days of receipt of the discrepancy.

During implementation and transition to operations, Team CNSI will work with the appropriate state to review the financial system capability to train our staff to perform the update activity. Team CNSI will provide contact information to the state for users that will be authorized to update the state financial system. The state will be required to create and manage the account information to sign into the system.

3.10.14.8 Performance Standards

This section outlines the service level agreement requirements for Option B services. The Contractor shall detail in their response their approach to meet each of the Performance Requirements defined in Attachment F, Requirements Matrix. SLAs are also found separately in Attachment J, Service Level Agreements.

As updated in Amendment 2: The Offeror must describe their approach to meet the Performance requirements defined in Attachment F, requirements Matrix.

Team CNSI is dedicated to delivering quality services that achieve performance measurement and service level agreement (SLA) requirements for the MT PSM project. Our commitment to quality is demonstrated by Team CNSI's use of quantitative management techniques as part of ITIL's continuous improvement activities, as well as by CNSI's choice of International Standards Organization (ISO) 9001:2015-certified Noridian as a Team CNSI member. With standard, repeatable processes that support predictable and consistent outcomes, Team CNSI is committed to providing Montana, along with the other NASPO cooperative states, with the best possible service.

The Team CNSI Advantage

Team CNSI regularly monitors performance measurements and SLAs to proactively address issues and maximize compliance with expectations.

- Service delivery based on ITILv3 focuses on metrics which allows Team CNSI to make data-driven decisions and support accountability for our performance
- ISO-9001 certification in proven business processes helps confirm we meet or exceed required performance measurements
- Highly-integrated, sophisticated reporting tools automatically track SLAs in real time
- Use of processes based on Lean principles provide increased productivity and efficiencies

MTPSM-3-066

As the prime contractor, CNSI serves as the leader of Team CNSI and has ***accountability*** for meeting all SLAs. CNSI is responsible for the quality performance of all its partners, providing DHPPS with a single point of contact. CNSI will be responsible for final delivery of the systems and smooth ongoing operations.

CNSI's partner, Noridian, is a successful administrative services organization and healthcare contractor in federal, state, and commercial markets. As a healthcare-focused company, Noridian brings over 50 years of experience as a healthcare administrative services organization, including Medicare and Medicaid, with extensive call center, provider enrollment, and provider management business functions experience. In fact, Noridian is ranked highest in the country on measures of provider satisfaction for it performance on the Jurisdiction F Medicare Administrative Contractor (MAC) contract that supports providers in the following NASPO states: Montana, North Dakota, Oregon, South Dakota, and Wyoming. Noridian also has been a long-time contractor supporting claims processing and provider management in another NASPO state – Hawaii.

To ensure we meet performance SLAs required by DPHSS, the other NASPO states, and our own internal standards, Team CNSI leverages a comprehensive quality management program based on successful operation of multiple complex healthcare administrative services delivery projects. Team CNSI's quality management program is governed by ISO 9001 quality management standards, under the supervision of our ISO-certified team member. This certification requires demonstration and documentation of a culture and business practices that consistently meet customer requirements through use of repeatable processes. ISO establishes consistent processes for operational quality assurance that focus on document control, record retention, corrective actions, preventive actions, and management review, as well as regular measurement, monitoring, and evaluation (MME) of program results. ISO standards become the foundation for the culture of quality assurance that is in place during the operations phase.

The following subsections describe Team CNSI's approach to meeting the performance requirements described in Attachment F. This includes a discussion of:

- ITIL-Based Approach for System Changes
- Internal Controls and Operational Procedures
- Staff Performance Measurement and Quality Activities
    - Call Center Performance Measurement and Quality Activities

- Enrollment Performance Measurement and Quality Activities

- Using Automation to Meet and Exceed SLAs
- Monitoring and Reporting on SLAs
- Process Improvement

ITIL-Based Approach for System Changes

Team CNSI manages systems updates using its ITIL-based quality management approach during the operations phase. The quality assurance processes are invoked for any update, change, or enhancement to the system. Team CNSI's Change Management Plan, with its associated configuration management and release management components, will be used to manage changes to the MT PSM solution during operations.

At the heart of our Change Management Plan is a strict configuration and version control process. This process verifies quality and accuracy by analyzing and reviewing each proposed change before it is implemented and released. The process controls authorizations for change and includes DPHHS as part of the review and approval sequence.

Adhering to this prescribed methodology produces a quality, low-risk solution as changes are well-tested and well-documented. Thorough documentation of changes produced by the change agents means the operational units are well-informed and prepared for the impacts of system changes.

Internal Controls and Operational Procedures

Central to Team CNSI's comprehensive quality management approach is a robust internal controls and compliance program based on our extensive knowledge of government contracting experience with the General Accounting Office's (GAO's) Federal Standard of Internal Controls. Internal controls are part of Team CNSI's work environment to ensure the completion of specific quality-related tasks, thus contributing to the overall success of business processes which consistently meet and exceed performance measurements. Team CNSI incorporates the GAO's internal control standards as part of day-to-day business processes.

Team-specific operational procedures are important elements of the internal controls program. The detailed procedures are designed to:

- Perform accurate and consistent processing of all business functions
- Provide efficient and effective training to operational team members
- Enable easy access to, processing of, and search for information.

Enrollment and call center staff perform their work in compliance with these detailed, online, step-by-step operational procedures. Team CNSI manages all operational procedures through a document management process based on our ISO 9001:2015 certified control program. We train staff to complete tasks in accordance with operational procedures, and we perform quality assurance on completed work using the operational procedures, which are the foundation for performance of all business activities. Detailed operational procedures contribute to consistent and predictable employee decision-making. The procedures are updated and/or created as needed for each project.

Each operational unit develops the detailed step-by-step tasks needed to perform each business function. Using standard templates and guidelines, the operational procedures contain flowcharts, inputs, outputs, and responsibilities for each activity. Along with that information, the operational procedures provide the performance measurements or SLAs associated with each activity, when applicable. Operational

procedures are stored and version controlled through the Team CNSI's project repository, SharePoint, to ensure staff members are using the current version. The repository provides staff with web access to the operational procedures, related team or procedural content, and training materials.

Requests and revisions to operational procedures can be initiated by any team member for any reason, including changes in process brought about by efficiency or contractor changes, and are processed through a review and approval mechanism in accordance with the Change Management Plan.

Staff Performance Measuring and Quality Activities

Team CNSI fosters a culture of quality and compliance as the basis for work activities. Quality is an expectation at every level and is promoted through these activities:

- Routine monitoring focused on employee performance
    - MME program used to statistically measure performance at the employee and team levels.
    - Monthly one-on-one meetings between management and staff to discuss individual performance and quality
    - Sampling of employees' work products
    - Ongoing training and feedback
- Development of business processes based on Lean principles, which provide visibility into work streams to adjust workload and staff on a real-time basis (the core Lean principle: maximize service while minimizing waste)
- Process reviews to assess business workflows, processes for compliance, and opportunities for process improvements

Team CNSI uses our MME program to monitor and compile statistics on employee and unit performance. These performance measurements are used to inspect trends in meeting workload expectations and identify where underlying issues may be impacting the ability to meet expectations. Operational supervisors and managers inspect work products and timeliness by conducting routine, systematic individual quality assessments on employee work output in each operational area or through examination of automated workload reports that provide metrics on productivity and timeliness. The MME process measures and monitors four elements: (1) Production, (2) Quality, (3) Time and Attendance, and (4) Values and Behaviors. Employee production and quality levels are measured and monitored to evaluate and quantify their performance. Likewise, time and attendance is recorded and quantified. Values and Behaviors, the final element, is more subjective, measuring employee behavior demonstrated in the workplace. Individual employee performance is collected and distributed to authorized individuals via workload reports and dashboards.

As part of employee monitoring, Team CNSI conducts planned individual quality assessments of employees' work for each operational unit. Managers or designated personnel review a sample of each employee's output on a regular basis. The sample rate is defined based on the type of work and staff assessments. For example, new staff or staff who may have been underperforming are subject to an increased rate of sampling until they demonstrate proficiency. A new or changed work process will also be subject to increased sampling.

Team CNSI also conducts business process reviews to confirm that employees are following the prescribed procedures and guidelines for each job as defined in the operational procedures. Managers or designated team members perform these reviews on a scheduled or ad hoc basis. The reviews provide the opportunity to validate that each employee is following standard procedures to perform his or her job and

that the employee understands how to use the operational procedures. The reviewers also look for improvement opportunities and document all findings for review with the employee and/or team.

Managers conduct monthly employee meetings to discuss performance requirements and measure results. These meetings provide an excellent tool for communication between the manager and the employee. Managers are responsible for communicating performance issues impacting contractual performance requirements to management.

Team CNSI is an ardent advocate of Lean principles. Team CNSI's Lean-trained engineers worked directly with each of our operational teams to put Lean processes in place. The engineers spent weeks learning about and breaking down all the many processes in each area. They analyzed team workflows and countless aspects of how work is processed to determine how it can be performed as efficiently as possible. They also assessed whether all activities were performed uniformly or were even necessary, whether a step could be automated or simplified, how many times an item was touched, the wait time with each step, or if the step could be eliminated. The results have been impressive in Team CNSI's current contracts, achieving substantial increases in efficiency and productivity in just a few months.

With expectations defined by and shared through the Lean approach, staff is aware of and held accountable for individual performance; management is accountable for the team's performance. "Daily huddles" take place to share yesterday's results and present the plan for the day. Charts are created, updated, and displayed every day for each team. Management is confident in coaching staff due to having objective data to support coaching, expectations, and actions.

Call Center Performance Measurement and Quality Activities

Team CNSI uses a multi-pronged quality assurance process to confirm we meet or exceed required performance measurements associated with the call center. Customer service representatives (CSRs) capture all information related to written or telephone inquiries in the Siebel Customer Relationship Management (CRM) solution from the initial contact through resolution. The business operations manager and/or designated senior staff members review the CRM history of activities associated with a provider request or question for accuracy and timeliness. We measure accuracy by comparing the steps the CSR took with the published operational procedures we maintain for each job function. Timeliness is monitored using the date and time stamps of each of the activities entered into the CRM. Any incorrect entries or resolutions are compiled and used in determining the accuracy rate. We use the information in training and to provide feedback to the CSRs.

One critical component of our quality initiative is our robust CSR training. To verify our CSRs know how to respond to as many situations as possible, we train the CSRs using, real-life "what-if" scenarios and branching logic so they are prepared for just about any question, including those that may need escalation. New hires or employees new to a position sit on the call center floor and listen in with experienced CSRs as part of the training. This complements our detailed enrollment processing training.

Team CNSI monitors recorded phone calls as another quality check. Designated personnel including the business operations manager monitor a set percentage of calls. We look for accuracy of the response, quality of the response, and professionalism. Feedback to the CSRs is built into our review process as part of our continuous improvement cycle.

Provider surveys also play a part in our quality program. Our call center solution provides an automated survey tool which is used to assess the caller's satisfaction with our call center service. The survey results are consolidated to provide reports to our management and DPHHS. Team CNSI uses individual survey scores to determine training needs for the CSRs or to implement corrective actions.

Enrollment Performance Measurement and Quality Activities

Team CNSI provides an extensive staff training program that covers all aspects of the provider enrollment process. We train all provider enrollment staff on the most common, highest frequency application types for prospective and current providers. As representatives demonstrate proficiency in those applications, we add training on the less common, lower frequency application types. Because management monitors individual staff performance throughout the day to pinpoint the source of peaks or drops in efficiency, they address performance issues through timely, meaningful, targeted training to individual staff as needed.

Team CNSI's enrollment process is built on our implementation of Lean principles in our operations. Following Lean principles, we establish time expectations for each workflow task and have developed tools to measure both individual staff and overall provider enrollment productivity. We use these tools to monitor production not just daily, but hourly, to meet both timeliness and quality standards efficiently. In one of Noridian's current contracts, this processing approach has increased productivity by greater than 40 percent over their prior methodology.

Because of the improved processes, Noridian's CMS Quality Assurance Surveillance Plan (QASP) results have continuously improved throughout the performance of their MAC Jurisdiction E and Jurisdiction F contracts. They have taken our continuous improvement efforts to a new level with automations, improved workflows, cross training of staff, and Lean management principles, which have enabled Noridian to meet 100 percent of QASP metrics in the most recent QASP review, as well as 100 percent of monthly metrics throughout the current year, while continually increasing efficiency.

Team CNSI will tailor our enrollment process to fold in the financial update requirements of some of the NASPO states. Upon completion of an enrollment, steps will be added to the current process to update the financial systems with applicable provider information. The operational procedures used by all staff are used to confirm that processes are carefully followed and no steps are overlooked. By adding the entry of information to the financial systems to these procedures, Team CNSI will know that staff have the necessary materials required to support their information entry. Team CNSI conducts productivity and accuracy monitoring on all staff to make sure staff are completing the amount of work expected without sacrificing the quality of their work. In additions, as a quality step, data entry of financial information will be double checked by another team member. This consistent review of quality ensures that work is completed correctly.

Using Automation to Meet and Exceed SLAs

Team CNSI facilitates quality and timely staff performance using advanced technology which is built into our systems. In the call center, controls built into our CRM tool work together with our knowledgeable and skilled staff to assign each request to the most qualified CSR. As shown in Figure 3.10.14-51, Team CNSI's CRM solution can be configured to automatically route service requests and activities using CRM Assignment Manager.

©2017 CNSI | Option B-74

The CRM Assignment Manager routes work items, such as enrollment inquiries, to the most appropriate candidates by enforcing business rules. Assignment Manager accomplishes this function by matching candidates (staff members, positions, and organizations) to predefined and user-configurable assignment objects. To assign the most qualified candidate to each object, Assignment Manager applies rules that are defined for each candidate. This blend of Team CNSI's experienced, skilled staff and advanced routing technology helps to transfer the request to the right person and deliver the response to the provider within the required time.

Evidence of the success in using this assignment routing technology can be seen in Noridian twice being awarded the CMS Provider Customer Service Program (PCSP) of the Year award, in addition to consistent praise by the providers served. Noridian currently boasts a 97% rate of first call resolution in its call center, and will use the experiences and processes developed there to support a high rate of first call resolution for DPHHS and other NASPO states.

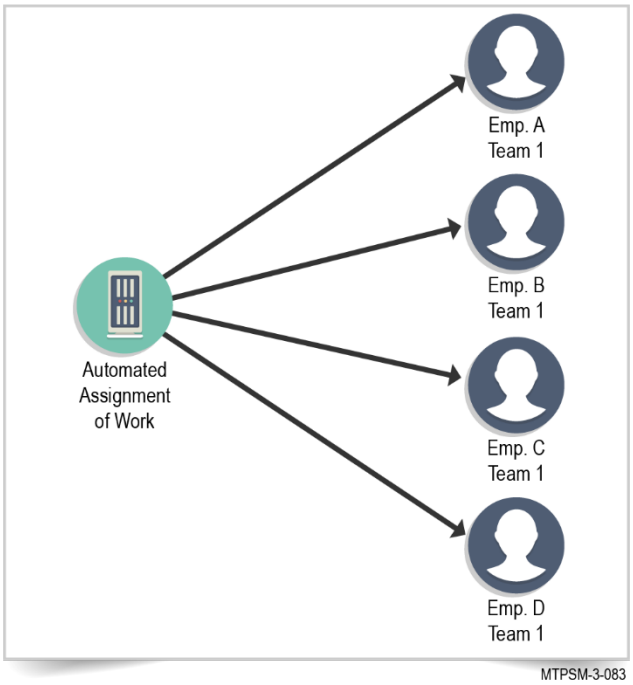


Figure 3.10.14-51. CRM Assignment Manager. Team CNSI ensures the inquiry goes to the most qualified staff member, resulting in fewer escalations and more timely resolution.

To support timeliness requirements, the CRM workflows can be tailored to monitor the due date on a documented provider inquiry through a service request. When the service request is nearing the due date, both the owner and the supervisor will receive notification emails. The screen that provides for these alerts is shown in Figure 3.10.14-52.

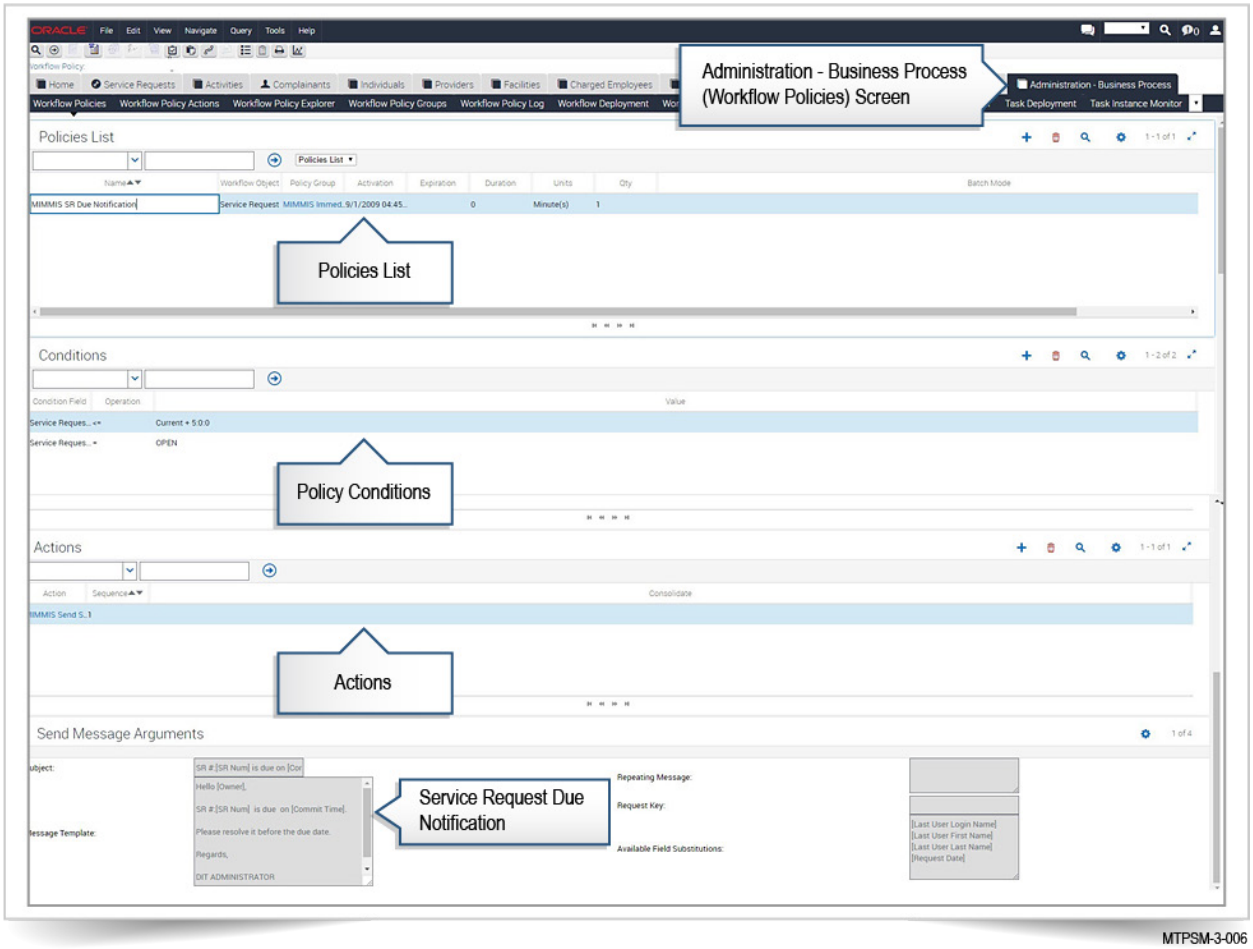


Figure 3.10.14-52. CRM Notification Email. Team CNSI's CRM solution provides automatic escalation to ensure SLAs are met.

For provider enrollment activities, Team CNSI's winning combination of provider enrollment experience and proven technology delivers high-quality service and low-risk enrollment operations services for Montana and its providers, fully encompassing the enrollment activities detailed in RFP Attachment F, STF01. Team CNSI is proposing a federally compliant PMIS that is implemented and operational in the states of Michigan, Washington, Illinois, and Utah. The evoBrix PMIS module has been leveraged successfully in enrolling providers for many years, and has been enhanced over time. Montana and other participating states' Medicaid providers will be the beneficiaries of these enhancements. Team CNSI's evoBrix PMIS has been shown to decrease provider enrollment backlogs from 30-60 days down to one day. Functionality, such as automated screening of providers' criminal background, sanctions, debarments, and other records, allows Team CNSI to expedite the review and finalization of enrollment applications, often in minutes rather than hours or days.

In managing provider enrollment and provider change request workflow using Lean management principles, we carefully develop time expectations for each task, and we use specific workload monitoring and reporting tools to gather and present data on staff productivity and efficiency.

Team CNSI's SiteVisitPro (SVP) is another tool we use to automate processes, improving performance and efficiency. SVP is Team CNSI's site visit solution, a portable application designed to meet Affordable Care Act (ACA) mandates for use with mobile devices. The SVP application allows business operations staff to perform site visits and capture the results in real time, eliminating the need to transfer

©2017 CNSI | Option B-76

data from paper forms. This application supports our staff by using up-to-the-minute provider information directly from the Medicaid provider enrollment system, thereby eliminating redundant data entry. SVP can be accessed from anywhere with a wireless connection. The application offers the following benefits:

- Streamlines Site visit processing using a real-time system, eliminating paper
- Eliminates periods of no activity on the site visits through alerts to the appropriate business operations staff
- Decreases the time it takes to approve or reject a provider's application for enrollment
- Eliminates redundant data entry and manual updates to the PMIS
- Sends systematic notification of the site visit results to the evoBrix PMIS module to enable reporting of the scheduled site visits versus those completed

Monitoring and Reporting on SLAs

Many vendors promise ***transparency into performance,*** but Team CNSI has a proven track record of making it a reality. It is such a vital ingredient to establishing trust that we present SLAs, metrics, and other measures directly, in a near real-time manner, using our HealthBeat system. HealthBeat is a business-driven, enterprise-wide framework that provides value by automating the extraction, analysis, and visualization of data on the performance of mission-critical business and information technology (IT) processes. HealthBeat kiosks are currently operating at Medicaid facilities and at high levels of the state of Michigan's Governor's organization. HealthBeat is in production at the CMS operations center for Marketplace operations and in the states of Washington and Utah, providing timely views into daily business operations.

> *...I would like to have all states adopt the [HealthBeat] dashboard as a sign of full transparency into the Medicaid program and if possible I would like to have one myself!*
>
> — CMS Official

MTPSM-3-067

We intend to deliver this same level of insight and visibility of performance measurements to Montana and the other NASPO states. HealthBeat provides a performance monitoring system that is aligned to Medicaid Information Technology Architecture (MITA) business areas. Its capabilities include enterprise dashboards that transform raw data into transparent, actionable measures of performance used to improve process maturity, performance results, and proactive management of potential issues. HealthBeat's data visualization capabilities accelerate the assessment of many key data points and make insights clearer for important business processes. HealthBeat is flexible enough to enable users to track MITA core business process performance and IT processes. We monitor performance and performance trends across all operational areas using daily, weekly, and monthly measures.

A HealthBeat graph showing call center status is shown in Figure 3.10.14-53.



Figure 3.10.14-53. HealthBeat Call Distribution by Status. HealthBeat automates the extraction, analysis, and visualization of data to provide easy to understand dashboards and reports.

In managing provider enrollment activities using Lean management principles, we carefully develop time expectations for each task, and we use specific workload monitoring and reporting tools to gather and present data on staff productivity and efficiency. Management holds each enrollment representative accountable for completing assigned work, and management can readily identify workload priorities and assignments to make sure timeliness metrics are met efficiently. DPHHS and providers will experience responsiveness and a well-coordinated organization that meets their needs.

Along with HealthBeat and the Lean management principles described above, Team CNSI's call center solution provides extensive metric capture and reporting capabilities. The Avaya application plays a major role in managing, tracking, and reporting call center performance. Using the call tracking system effectively helps the call center business run smoothly and with improved performance by providing managers with real-time views into workload and staff performance. Avaya, as part of Team CNSI's call center solution, is designed to minimize the average hold time. Skill-based routing, along with call tracking in the CRM, plays a key role in reducing the average hold time.

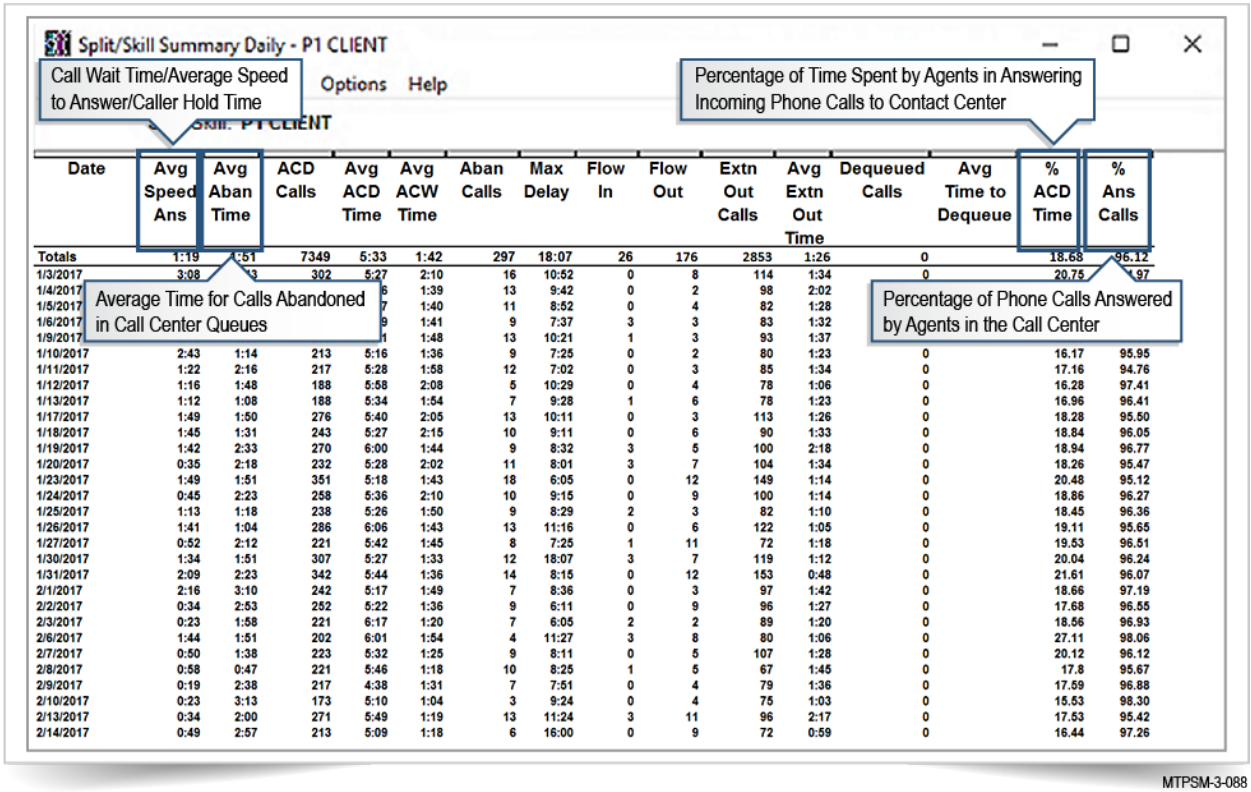
Team CNSI's Siebel CRM solution supports interactive logging of all transactions and the comprehensive ability to report call statistics. The available reports can be broadly categorized into three types, as described in Figure 3.10.14-54. These reports provide a 360-degree view of call center performance.

Report Type	Description	Report Names
Avaya Call Management System Call Center Reports	Provide details on the overall functioning of the call center. Avaya Call Management System reports can be real-time reports, historical reports, or integrated (combination of real-time and historical) reports. Additional reports can be configured as defined during solutioning activities.	■ Skill Status Report ■ Agent Group Report ■ Daily Summary Report ■ Agent Graphical Information Report ■ Skill Comparison Report

Report Type	Description	Report Names
Avaya Aura Experience portal/Interactive Voice Response (IVR) Reports	Provide details on all the transactions that are performed during IVR calls and overall performance of the IVR systems. These reports can be generated on a pre-defined schedule or on demand.	■ Application Summary Report ■ Application Detail Report ■ Call Summary Report ■ Call Detail Report ■ Session Detail Report ■ Performance Report ■ Active IVR Calls Report ■ System Monitor Report
HealthBeat Reports	HealthBeat provides a robust, automated framework to extract, analyze, and report data from diverse business processes into a centralized enterprise service view. It allows near real-time access to business and system performance metrics and provides transparency to information technology operations management and the enterprise-wide business.	■ Average Call Waiting Time ■ Distribution of Abandoned Calls by Percentage ■ Call Distribution by Helpline ■ Call Distribution by Status

Figure 3.10.14-54. Call Center Reporting. Team CNSI's call center reporting provides a 360-degree view of the call center performance allowing for full transparency into our performance.

As another aid to managing workload, the system generates a real-time display of available agents, average online time, average talk time, average hold time, average speed of answer, calls in queue, total calls offered, total calls answered, service level percentage, and total time the agent was available to take calls. Call center management use this call center tool to monitor SLA metrics and overall performance reporting, as well as to handle call center workload management. This information is accumulated throughout the day to produce summary reports such as the one shown in Figure 3.10.14-55.



Date	Avg Speed Ans	Avg Aban Time	ACD Calls	Avg ACD Time	Avg ACW Time	Aban Calls	Max Delay	Flow In	Flow Out	Extn Out Calls	Avg Extn Out Time	Dequeued Calls	Avg Time to Dequeue	% ACD Time	% Ans Calls
Totals	1:19	:51	7349	5:33	1:42	297	18:07	26	176	2853	1:26	0		18.68	96.12
1/3/2017	3:08	:3	302	5:27	2:10	16	10:52	0	8	114	1:34	0		20.75	97
1/4/2017		:6			1:39	13	9:42	0	2	98	2:02				
1/5/2017		:7			1:40	11	8:52	0	4	82	1:28				
1/6/2017		:9			1:41	9	7:37	3	3	83	1:32				
1/9/2017		:1			1:48	13	10:21	1	3	93	1:37				
1/10/2017	2:43	1:14	213	5:16	1:36	9	7:25	0	2	80	1:23	0	16.17	95.95	
1/11/2017	1:22	2:16	217	5:28	1:58	12	7:02	0	3	85	1:34	0	17.16	94.76	
1/12/2017	1:16	1:48	188	5:58	2:08	5	10:29	0	4	78	1:06	0	16.28	97.41	
1/13/2017	1:12	1:08	188	5:34	1:54	7	9:28	1	6	78	1:23	0	16.96	96.41	
1/17/2017	1:49	1:50	276	5:40	2:05	13	10:11	0	3	113	1:26	0	18.28	95.50	
1/18/2017	1:45	1:31	243	5:27	2:15	10	9:11	0	6	90	1:33	0	18.84	96.05	
1/19/2017	1:42	2:33	270	6:00	1:44	9	8:32	3	5	100	2:18	0	18.94	96.77	
1/20/2017	0:35	2:18	232	5:28	2:02	11	8:01	3	7	104	1:34	0	18.26	95.47	
1/23/2017	1:49	1:51	351	5:18	1:43	18	6:05	0	12	149	1:14	0	20.48	95.12	
1/24/2017	0:45	2:23	258	5:36	2:10	10	9:15	0	9	100	1:14	0	18.86	96.27	
1/25/2017	1:13	1:18	238	5:26	1:50	9	8:29	2	3	82	1:10	0	18.45	96.36	
1/26/2017	1:41	1:04	286	6:06	1:43	13	11:16	0	6	122	1:05	0	19.11	95.65	
1/27/2017	0:52	2:12	221	5:42	1:45	8	7:25	1	11	72	1:18	0	19.53	96.51	
1/30/2017	1:34	1:51	307	5:27	1:33	12	18:07	3	7	119	1:12	0	20.04	96.24	
1/31/2017	2:09	2:23	342	5:44	1:36	14	8:15	0	12	153	0:48	0	21.61	96.07	
2/1/2017	2:16	3:10	242	5:17	1:49	7	8:36	0	3	97	1:42	0	18.66	97.19	
2/2/2017	0:34	2:53	252	5:22	1:36	9	6:11	0	9	96	1:27	0	17.68	96.55	
2/3/2017	0:23	1:58	221	6:17	1:20	7	6:05	2	2	89	1:20	0	18.56	96.93	
2/6/2017	1:44	1:51	202	6:01	1:54	4	11:27	3	8	80	1:06	0	27.11	98.06	
2/7/2017	0:50	1:38	223	5:32	1:25	9	8:11	0	5	107	1:28	0	20.12	96.12	
2/8/2017	0:58	0:47	221	5:46	1:18	10	8:25	1	5	67	1:45	0	17.8	95.67	
2/9/2017	0:19	2:38	217	4:38	1:31	7	7:51	0	4	79	1:36	0	17.59	96.88	
2/10/2017	0:23	3:13	173	5:10	1:04	3	9:24	0	4	75	1:03	0	15.53	98.30	
2/13/2017	0:34	2:00	271	5:49	1:19	13	11:24	3	11	96	2:17	0	17.53	95.42	
2/14/2017	0:49	2:57	213	5:09	1:18	6	16:00	0	9	72	0:59	0	16.44	97.26	

Figure 3.10.14-55. Daily Summary Report. This report provides a compilation of statistics collected during the day and can be organized by different categories.

Process Improvements

Team CNSI's overall performance focus is continuous process improvement that is measured, in part, by improvements in enrollment application/revalidation/change processing, first call resolution, call/correspondence accuracy and timeliness, and customer service survey scores. Team CNSI will incorporate Lean principles in the MT PSM solution. As process improvements are identified or changes to workflows are needed, the quality processes described in the sections above are invoked to make the improvement. Team CNSI provides open and transparent access to our performance and to our continuous process improvement initiatives. Evidence of our commitment to, and our success in realizing, high levels of customer service can be found in the metrics we achieve for current customers,

Team CNSI will work with DPHSS and/or the other NASPO cooperative states to apply a process improvement review procedure at regularly scheduled points during the operations phase of the project. The frequency of these process improvement reviews will be determined with input from each state. To facilitate these reviews, we will:

- Use a structured, documented methodology to conduct these reviews
- Verify that results and recommendations resulting from the reviews are documented and distributed to the appropriate parties
- Implement meetings with the appropriate operational area supervisors, managers, and state personnel to discuss opportunities for process improvements
- Use lessons learned from improvements in other operational areas or other contracts to help determine possible improvements in the process

Team CNSI's overall management approach is conducive to problem solving and out-of-the-box thinking which has led, and continues to lead, to Team CNSI's adaptive nature. It is not happenstance that Team CNSI has been on the leading edge of adopting new technology, deploying process improvements, and introducing innovative customer service solutions. Team CNSI has evolved and will continue to evolve to meet the changing Medicaid program and environment.