

Claims Processing and Management Services for Montana's Program for Automating and Transforming Healthcare (MPATH)

RESPONSE TO DPHHS-RFP-2020-0254T

February 18, 2020
2:00 p.m., Mountain Time



3.10 Detailed Scope of Work

3.10.1 Technical and Information Architecture

Submitted electronically to:

Tia Snyder
Procurement Officer
Phone: (406) 444-3315
Fax: (406) 444-2529
E-mail: tsnyder@mt.gov

Submitted by:



2277 Research Blvd.
Rockville, MD 20850
(301) 634-4600

Table of Contents

3.10 Detailed Scope of Work..... 45

 3.10.1 Technical and Information Architecture Requirements 47

 3.10.1.1 Compliance 62

 3.10.1.2 Security 79

 3.10.1.3 Hosting and Environments..... 155

 3.10.1.4 Integration..... 169

 3.10.1.5 Data Management 210

 3.10.1.6 Interfaces..... 273

 3.10.1.7 Business Rule..... 282

 3.10.1.8 Correspondence Management..... 301

 3.10.1.9 Enterprise Content Management..... 307

 3.10.1.10 Workflow 317

3.10 Detailed Scope of Work

The Department of Public Health and Human Services (DPHHS) defined the scope of work stated in the Requirements Response Matrix which is included as Attachment F of this RFP. 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 Scope of Work, unless otherwise noted, shall apply throughout the life of the Contract. Additionally, the Contractor's scope of work must be performed within the Offeror's proposed cost for each project phase as defined in Attachment G – Pricing Schedules, Schedule B – DDI Payment Milestones.

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 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 described in respective sections our approach to successfully delivering the desired services for DPHHS specifically and other NASPO participating states. 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 Claims Processing and Management Services (CPMS) implementation and is uniquely positioned to deliver the services with the only true modular MMIS solution in the market that has been successfully deployed in multiple states.

Team CNSI has led the way in multi-state Medicaid Enterprise implementations with our projects in Michigan and Illinois and have developed an extensive set of reusable and proactive best practices purposely focused on the implementation of modular MMIS solutions. 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. Furthermore, we recognize the dynamic nature of the healthcare industry at both the Federal and State levels and we actively monitor for any regulatory or policy changes that will impact how our solutions functions are implemented. Change is a natural component of any Health IT environment, and we have incorporated change management as a core element of our delivery approach to allow us to rapidly and flexibly adjust and develop the solution as needed and authorized. Team CNSI's evoBrix X platform architecture is dynamic and flexible, allowing us to incorporate change or new regulations, policies, and standards through maintenance updates and roll-out these updates across any of the states using our platform. Team CNSI's successful track record implementing evoBrix X as a SaaS solution in multiple states in multi-vendor environments provides DPHHS and the other NASPO participating states a low-risk and repeatable option for evolving their current environments to a fully modular, flexible, and configurable enterprise solution.

Key highlights of the evoBrix X platform include:

- Highly flexible, dynamically configurable, modular solution components built upon a loosely coupled Service Oriented Architecture (SOA) architecture using SOAP and REST APIs to enable easy integration with the MPATH Integration Platform and other modules in the DPHHS ecosystem
- Powerful and easy-to-use RulesIT rules engine that leverage a user-friendly interface to achieve streamlined business outcomes by flexibly configuring rules, workflows, and evaluations to meet State and CMS requirements today, and in the future.
- Deployed in a secure, scalable, and highly available FISMA-Moderate Amazon Web Services (AWS) cloud environment
- Proven alignment with CMS MITA and MECT requirements including achieving certification in other states on the first pass with no findings

- evoBrix X HealthBeat® provides an automated, configurable dashboard that presents a centralized enterprise service view of real-time performance metrics and statistics. Leveraging the tool's alert engine and graphic dashboard, stakeholders can make informed decisions based upon real-time data.
- Supports member and provider self-service through MyHealthButton®, our mobile patient-provider tool that allows authorized users to review benefits and claims, obtain eligibility information, search for approved care providers, and track goals based on health behaviors and measures

Team CNSI has provided detailed responses to all 3.10 subsections to provide DPHHS and other NASPO-participating states with a comprehensive explanation of the technical and architectural elements of our solution. For the functional requirements, we have offered many screenshots of the system to illustrate how our evoBrix X CPMS solution currently addresses these requirements. As a result, the file size of our response has exceeded the 50MB limitation of the eMACS system. Therefore, we have broken our responses into several sections and included them as Supplier Attachments.

3.10.1 Technical and Information Architecture Requirements

The MPATH Integration Platform, implemented by the Systems Integration Services Contractor, will provide an inventory of Application Programming Interfaces (APIs) in addition to performing other systems integration services to support the Technical and Informational Architecture requirements. 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 Response Matrix.

Montana DPHHS is fundamentally transforming its Medicaid operations by implementing the MPATH 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.

Team CNSI proposes evoBrix X, a modular Medicaid platform, to serve as the MT Claims Processing and Management Solution within MPATH. Team CNSI’s solution is fully backed by its solid track record of enabling the states of Michigan, Washington, Illinois, and Utah to successfully run Claims processing and management functions in a multi-vendor implementation environment. evoBrix X 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 X is cloud- and SOA-enabled, positioning it as the most advanced Medicaid platform in the market.

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

- Functionally rich Claims Processing & Management Services (CPMS) 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 CPMS to quickly and cost-effectively adapt to the changing environment of Medicaid
- As a MITA-aligned solution, evoBrix X will enable MT CPMS 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 X 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 X will enable 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.

The Team CNSI Advantage

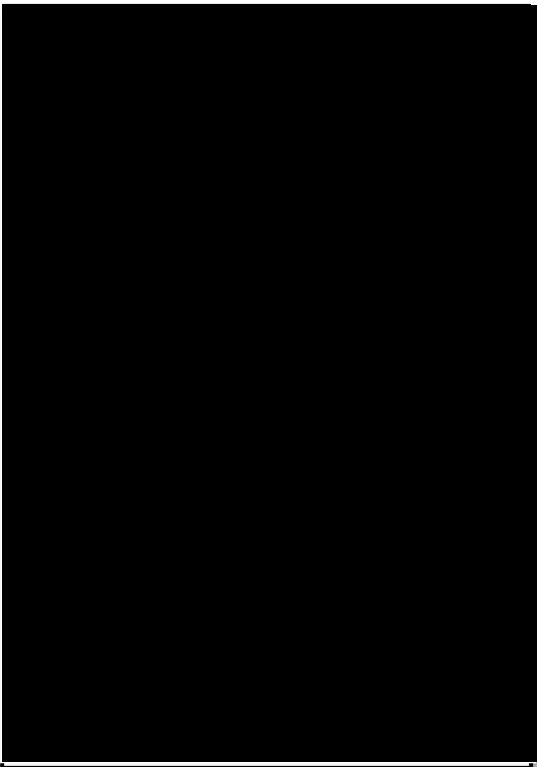
evoBrix X is an industry-leading, low-risk solution for delivering business services to Montana DPHHS.

- Modular and modern platform based on Service Oriented Architecture (SOA) design principles
- Deployed in FedRamp certified AWS GovCloud
- Feature rich functionality based on input from multiple states
- Advanced, real-time monitoring to monitor and measure key performance indicators
- Responsive UI portals compatible with various mobile device sizes

MTCPM-1.2.4-754

Team CNSI’s solution will follow the CNSI standards-based integration approach established through the planned reference technical architecture governed by the State and managed by the system integrator vendor (Deloitte). 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 X is integrated with several COTS solutions to further enrich its functional and technical capabilities. evoBrix X integration architecture and tools will facilitate seamless integration with MPATH Integration Platform. using API, webservices, file exchanges etc. Each module and COTS product was carefully chosen to be part of the evoBrix X CPMS 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 CPMS solution. Montana DPHHS will greatly benefit from the proven, innovative evoBrix X 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 - Eight independent modules that offer DPHHS and other NASPO-participating states with maximum flexibility to implement their modular Medicaid enterprise - Eliminates vendor lock-in by providing easy integration with third party modular components
Interoperability	- Enhanced interoperability allows for increased information exchange among trading partners and other agencies - Industry standard integration elements such as SOAP and REST APIs
Configurability	Rules-based architecture enables changes to business rules through configuration
Accessibility	- Ensure enterprise-wide access to services through various access channels - Role-based access controls to allow each enterprise to tailor the accessibility needs to meet their enterprise security definitions and roles
Adaptability and Extensibility	- Agility to adapt to changes in DPHHS business and regulatory environment - CMMI Level 3 Development practices are aligned with Agile and DevOps principles - 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	• Software-as-a-Service solution hosted in FedRamp certified AWS GovCloud • Elastic scalability to meet business demands and support outyear fluctuations
Alignment to Industry Standards	• Leverage business process improvement opportunities through MITA business process maturity • Solution is based on industry standard and proven tools and technologies • Processes align with industry best practices and standards including CMMI, ITIL, and PMBOK

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

Modularity

evoBrix X'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 X'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.

Cloud-Platform

Team CNSI will host the MT CPMS solution in AWS Federal Risk and Authorization Management Program (FedRAMP) certified Cloud. The primary data center and the Disaster Recovery (DR) Data Center will be in different Availability Zones to ensure continuous operations. These data centers use a robust and redundant infrastructure architecture to provide maximum uptime for critical data, applications, and technologies. Team CNSI's cloud model is elastic and scalable to allow for both short-term capacity spikes as well as long-term growth as needs evolve. Key capabilities include:

- 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 certified and FedRAMP certified data centers.
- The hosting platform is built on a robust security framework comprising multiple security and encryption features. These security and encryption features are based on the Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) models.

Interoperability

The key interoperability capabilities of the MT CPMS 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 X 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 X UI responsive layout for creating an engaging user experience aligned to usability standards including W3C and ADA (level A & AA) 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 (Option B implementation)

Adaptability & Extensibility

evoBrix X adaptability and extensibility capabilities will allow MT CPMS 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 X 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 X security framework will be responsible for ensuring secure access to information, information exchange, secure communication, protection of privacy, and data security. Figure 3.10.1-2 illustrates key security capabilities of evoBrix X:

Feature Type	Capability of the evoBrix X Solution
Protection of health information	- Controlled access to data - Secure communication - Security controls for existing/emerging threats and vulnerabilities
Application security	- Authentication controls including single sign on. - Separation of web layer and application layer via secure deployment - Data security in transit via validation and encryption
Authorization controls	- RBAC (to data element level) - User account audit - Audit trail and history.
Data security	- Encryption of data at rest and in-transit - SAN encryption - Data de-identification (masking).
Infrastructure security	- Hardware separation via a secure, zone-based architecture - Multi-zone architecture to protect the MT CPMS solution from vulnerabilities - Optimized resource utilization - Expandable infrastructure on demand.

Figure 3.10.1-2. evoBrix X Security Features. evoBrix X provides security across multiple architectural and data layers.

Scalability

The evoBrix X architecture provides application-level as well as infrastructure-level scalability capabilities to support business growth. Team CNSI will host evoBrix X Solution AWS FedRamp Certified cloud which 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: Figure 3.10.1-3 provides information on the key capabilities of our cloud solution:

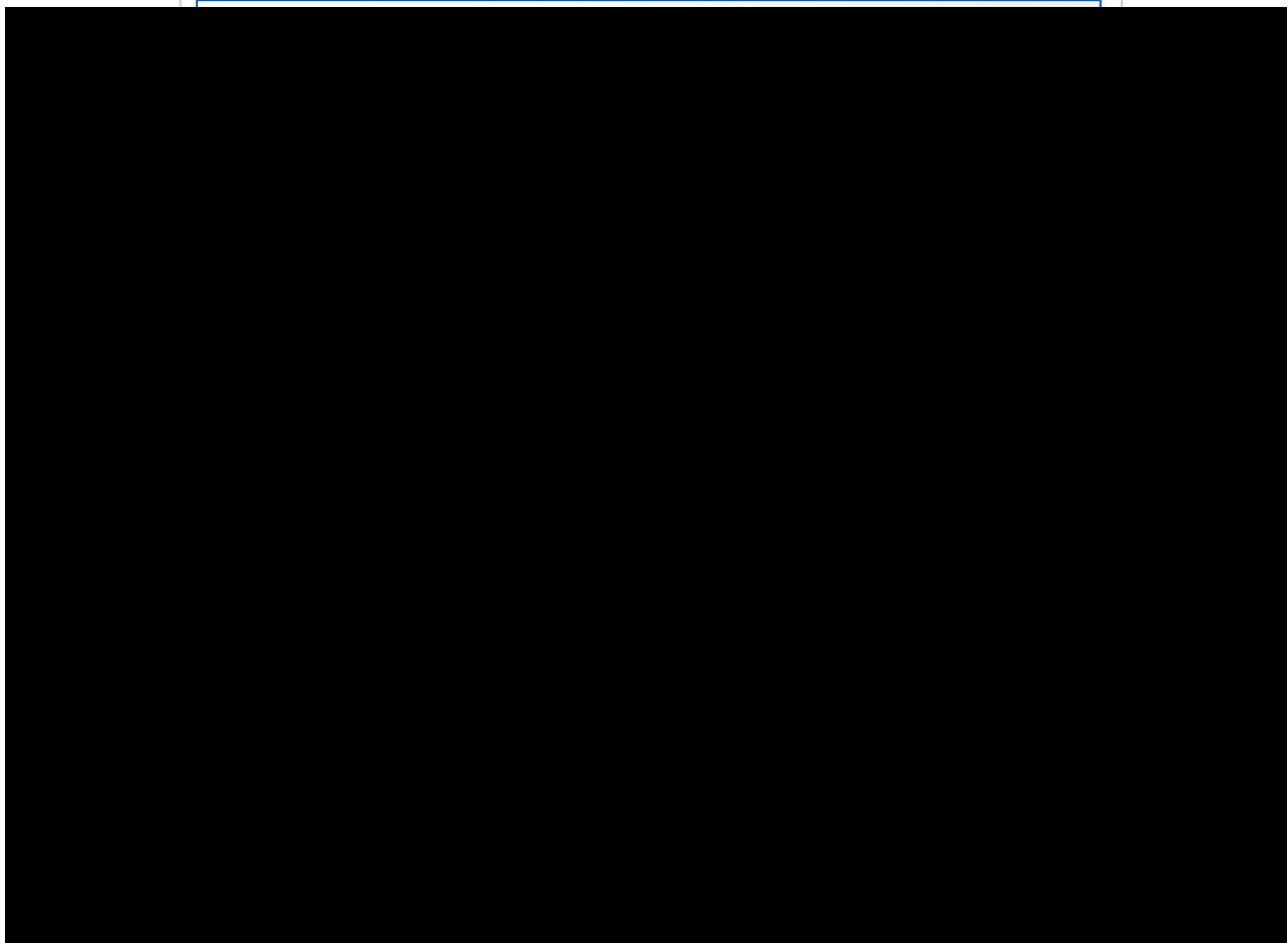
Feature Type	Capabilities of the evoBrix X Solution
Vertical Scalability.	- Dynamic reconfiguration of app servers to add or remove VPUs, RAM, or I/O devices without requiring a reboot - Dynamic expansion capability of database servers
Horizontal Scalability	- Dynamic addition of new and powerful app servers - Addition of supercluster racks for enhanced database server scalability - 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.
Provisioning	- Live migration and reconfiguration between servers - Consolidation of application via monitoring components that manage virtual infrastructure
Availability	- Removal of single point of failure dependencies - Minimal downtime during maintenance - Compression and deployment options that ensure high-efficiency

Figure 3.10.1-3. evoBrix X Cloud Features. Team CNSI's cloud solution leverages AWS GovCloud reliability and scalability to support the current and future needs of the program.

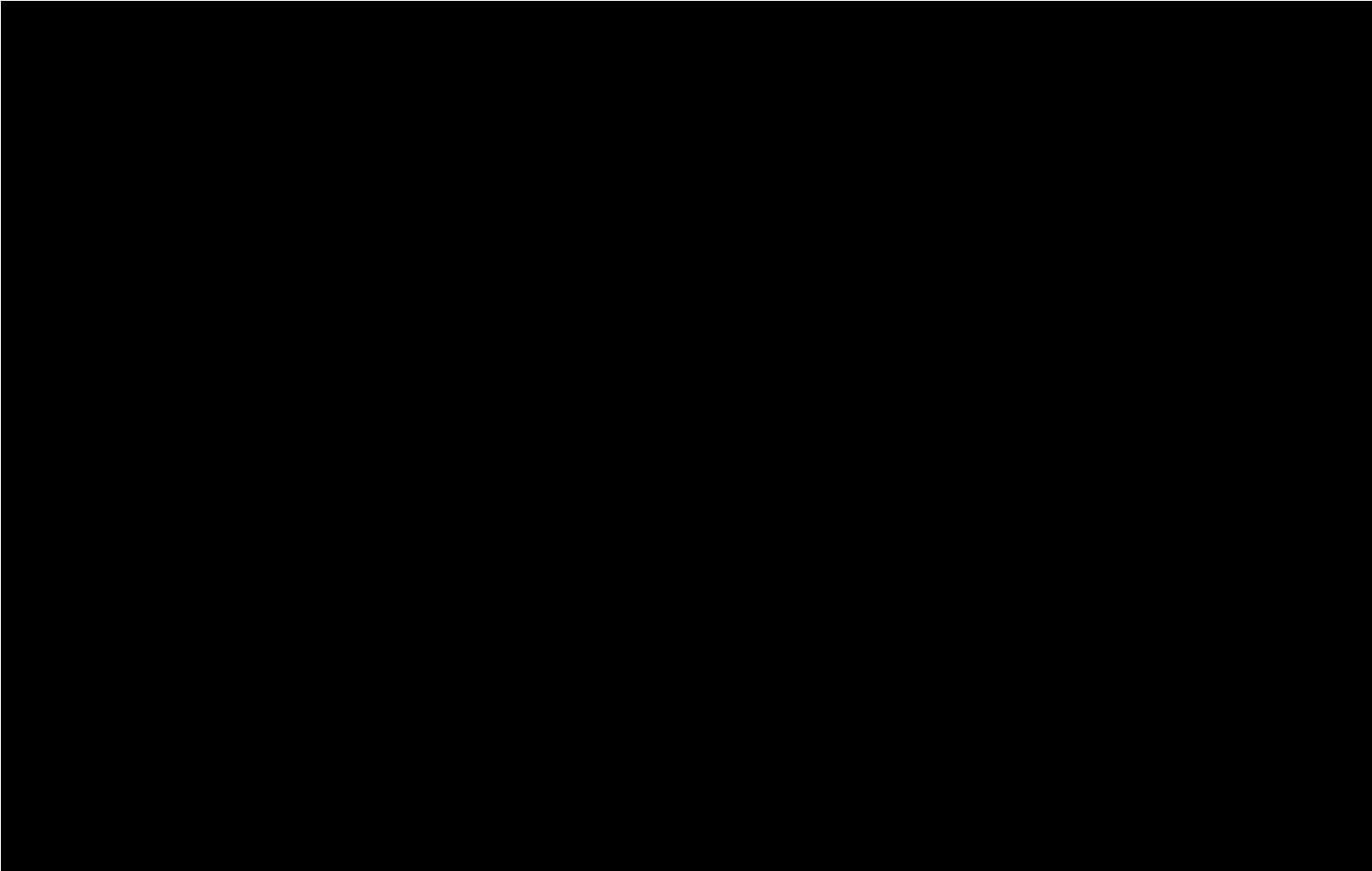
Team CNSI continues to participate in MITA, HL7 standards, and other standards-related forums to promote and adopt standards. We regularly review current standards and any updates or changes are prioritized on our product development roadmap to ensure that standards are met in a timely fashion. The evoBrix X solution is currently aligned to industry and regulatory standards at the time of this submission, 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 derived from our successful deployments of our precursor eCAMS product in the states of Washington and Michigan and the Department of Veterans Affairs. evoBrix X leveraged the existing product functionality and engineered its modular framework 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. Figure 3.10.1-5 illustrates our architectural design.



The technical architecture capabilities of the proposed solution will allow for interoperability between the evoBrix X 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 3.10.1-6.

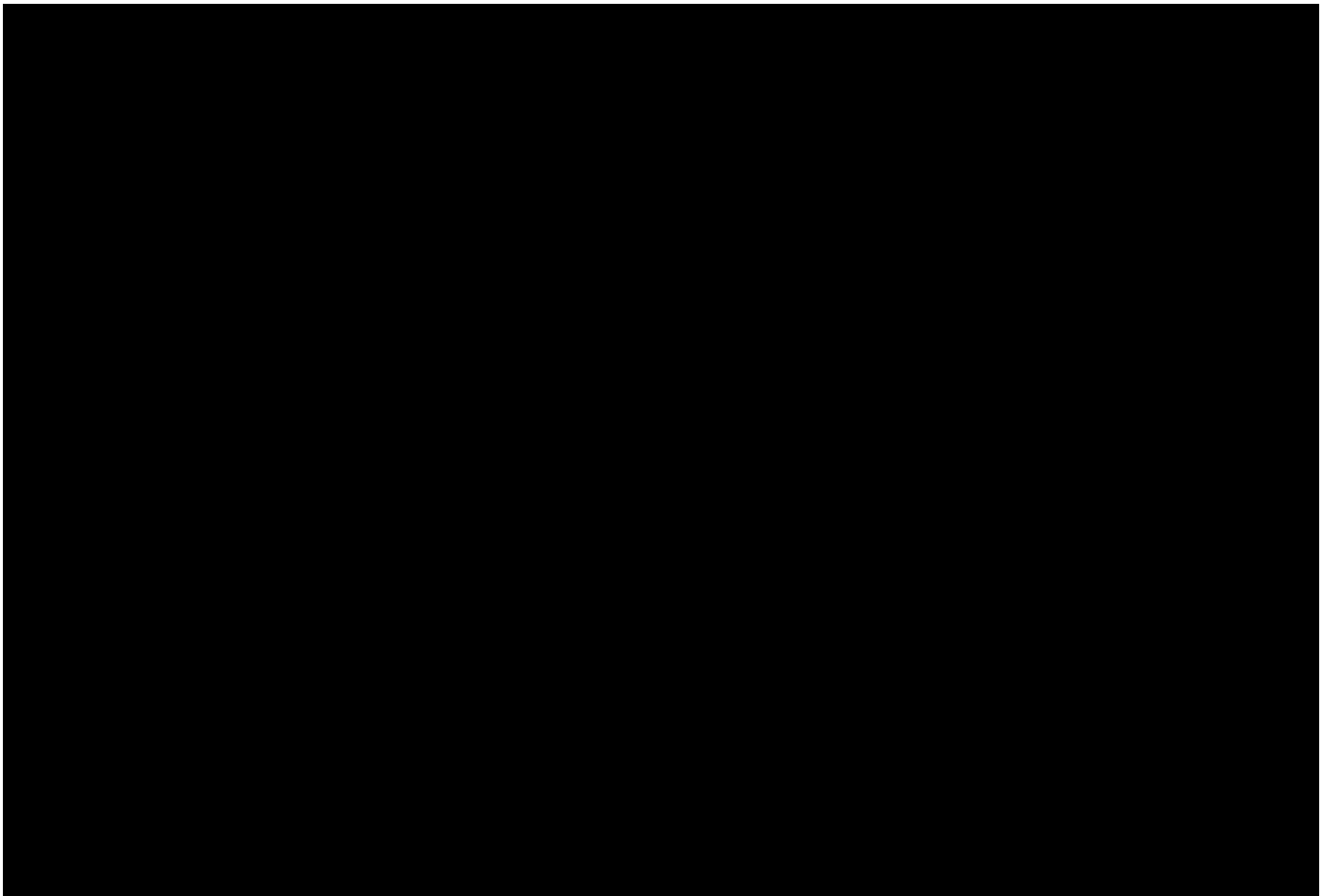
Services	Service Description
Accessibility Services	■ Includes services that enable user access to various users of the MPATH solution via web portals and mobile devices ■ Responsive UI technology for multi-device, multi-browser support ■ Compliant to web and ADA standards ■ Multi-channel support including web, mobile, Computer Telephony Interface (CTI)

Services	Service Description
Integration Services	Set of Integration services, Integration gateway, and SOA mediator for enabling service-oriented integration between MT CPMS and other systems in the DPHHS Enterprise environment through the MPATH system integrator.
Technical Services	Set of services leveraged across the evoBrix X 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 3.10.1-6. evoBrix X Service Layers. evoBrix X service layers encapsulate a modular and integrated solution stack.

Option A with Core System (Claims Processing & Management Services)

Effective and timely claims processing is dependent upon accurate and reliable receipt of claims. Providers have varying needs and technical abilities for submitting claims. Team CNSI provides a full spectrum of capabilities to enable all providers to submit claims efficiently based on their circumstances and preferences (SFTP, Claim uploads, Direct Data Entry & Paper Claims).



evoBrix X 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 X will offer the core business services, which are functionally rich, aligned to MITA, and federally compliant. Each functional module in evoBrix X 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 X, 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.

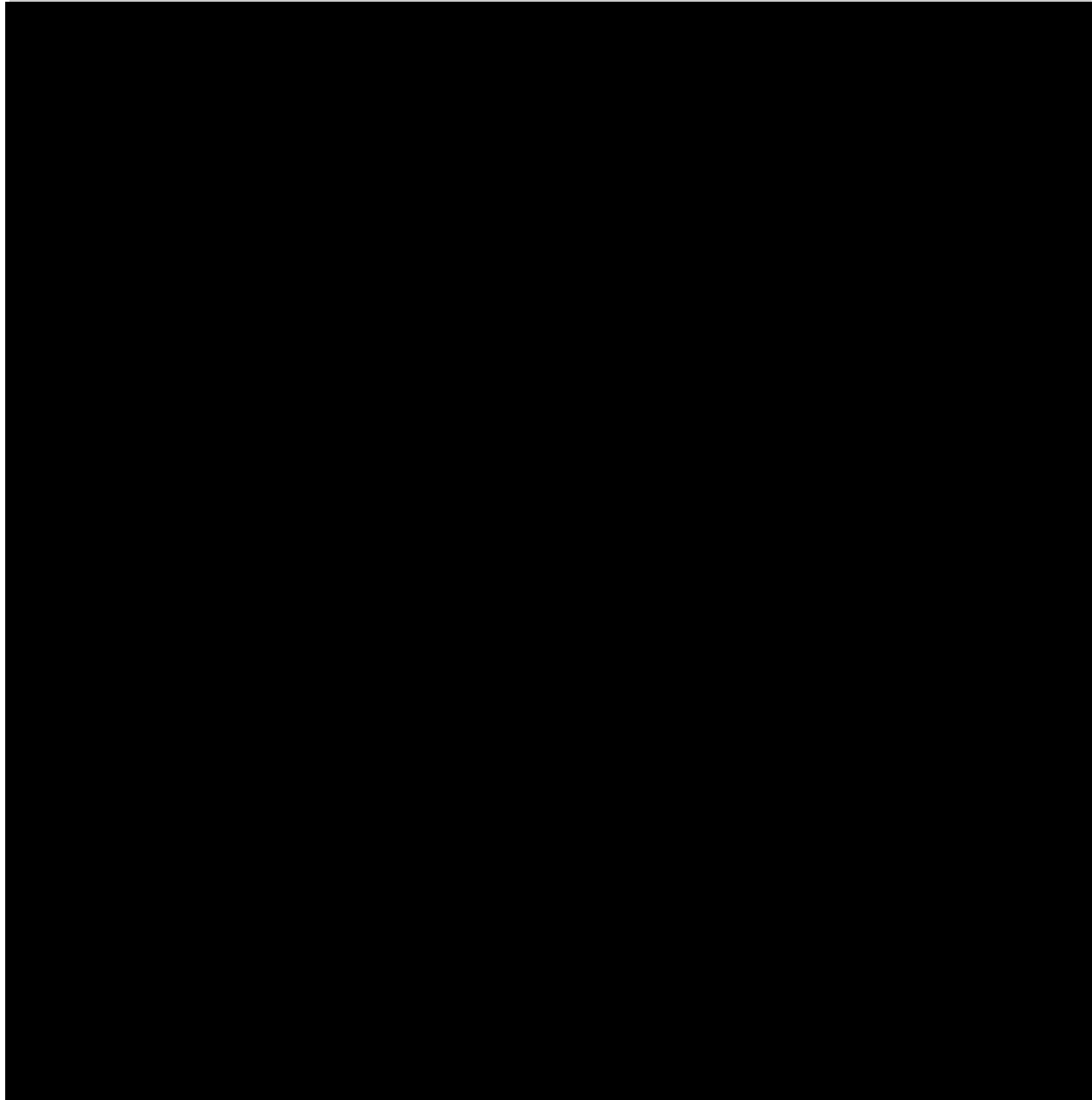
evoBrix X CPMS solution provides user-friendly interfaces and supporting business operations for claims submitted in the evoBrix X CPMS Core Claims portal through:

- Direct data entry (DDE) and 837 file
- Individual uploads
- Paper claims submission
- Batch submission through the electronic data interchange (EDI) Gateway

evoBrix X CPMS solution claims intake solution has been operational in several states for over a decade. It has been designed to receive, store, process, and pay institutional and professional claims in the Medicaid environment, regardless of the input method applied. Receipts are monitored and reported daily, allowing us to track the successful processing of all claims through to completion. Team CNSI has received and adjudicated over 300 million claims annually. Today, we collect claims submitted by 25,000 unique trading partners, representing roughly 290,000 providers across many lines of business. Throughout our decades of EDI support experience, we have tailored EDI processes that reduce implementation risk and improve provider satisfaction. We have done so by:

- Including an EDI testing phase prior to Operational go-live;
- Enabling providers and their trading partners to confirm file errors prior to submission; and
- Ensuring providers experience no disruption in payment receipt.

[REDACTED]



Team CNSI understands the State's requirements for a user-friendly, convenient, dynamic, feature-rich portal with extensive self-service functionality for claims management activities. evoBrix X provides a rich set of MITA-aligned features for Claims Processing and Management Services functions that will serve to address the State's requirements. The solution combines a full-featured, secure, self-service portal with a comprehensive administrative framework to intake & process claims. 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 a browser-based and interactive system supporting the day-to-day business needs of the providers and DPHHS user communities.

evoBrix X supports the processes identified in the MITA's Claims Processing & Management Services 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.

evoBrix X CPMS 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 X CPMS solution also provides functionality that allows State staff to request for security profiles based on their job duties.

evoBrix X CPMS 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 X CPMS 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.

Option B (CRM & IVR)

Our Customer Relationship Management (CRM) system, ConnectionPoint, is built on industry-leading technology that promotes innovative approaches to service delivery. ConnectionPoint is a Software as a Service (SaaS) offering that is built on a microservices architecture supported by a rich Platform as a Service (PaaS) infrastructure for optimal configurability, flexibility, and scalability. ConnectionPoint includes complete contact record, interaction tracking capability, and a link to all correspondence and claims documentation for access from within case records.

Our system includes all of the core functionality required for an Enterprise Member and Provider Call Center. ConnectionPoint will provide the Agency with:

- **Configurability: Built-in configurability through analyst level options and workflow creation capability**
- **Flexibility:** We implement the features and services designed to meet specific State needs
- **Ease of change management:** Application changes can be implemented independently at a modular level to minimize system downtime and service interruption
- **High availability:** Independent microservices configuration prevents an issue impacting one service from causing an entire system outage
- **Scalability:** On-demand elasticity through cloud hosting seamlessly supports open enrollment surges as well as potential longer-term volume changes
- **Reliability:** ConnectionPoint is hosted in the AWS cloud for best-in-class reliability
- **Full History by Provider or Member:** Quick access to the provider or member’s complete contact history allows us to provide better, more personalized customer service

ConnectionPoint provides all contact tracking, case activity, documents received and sent, complaint records, and configurable action codes for each contact and activity. For example, a provider claim

inquiry would be attached to a provider case record for full provider inquiry history—allowing management, the Agency, and the assisting CSR to easily see that the provider has inquired previously about the same claim and submitted, or failed to submit, follow-up documentation regarding that claim. We can also see if the provider has pursued similar issues on previous claim inquiries across patients.

Option C (Federal Reporting)

Team CNSI is a leader in innovative healthcare solutions and brings a proven technology to implement a federal reporting solution. Team CNSI’s evoBrix X Medicaid Reporting solution, as shown in Figure 3.10.1-9, is based on state-of-the-art technologies and approaches for data management and reporting. Our solution is purpose built to solve the State’s need for Federal reporting and provide operational insights for managing the Medicaid enterprise. Team CNSI’s evoBrix X Medicaid Reporting solution provides the necessary strategic framework for the NASPO State customers to report on both traditional and nontraditional programs. Team CNSI’s offering provides the necessary framework and analytical tools for the State to manage the key objectives including the ability to:

- Analyze Medicaid program costs and trends
- Evaluate Financial performance
- Monitor program payments
- Analyze provider performance
- Maintain an efficient and effective management reporting process
- Meet the Federal reporting mandates
- Meet State defined quality measures
- Meet operational reporting needs

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]



3.10.1.1 Compliance

This section addresses requirements to ensure compliance with state and federal statutes, policy, mandates as well as industry standards required for the Contractor's Scope of work. Offerors must describe in detail how their solution, services and operational approach meet each of the Compliance requirements in Attachment F – Requirements Response Matrix. In addition, the Contractor is required to demonstrate that their hosting solution is Statement on Standards for Attestation Engagements (SSAE-18) SOC 2 Type II compliant. The Offeror simply repeating the RFP requirements does not qualify as a good response as defined in Section 6.1.1 of this RFP.

Team CNSI’s evoBrix X CPMS solution provides a rich set of MITA-aligned features for claims intake, management, processing, payment, and tracking to meet all of the requirements of the CPMS solicitation and serve as a core element of the MPATH enterprise. Team CNSI’s evoBrix X CPMS solution combines a full-featured, secure, web portal with a comprehensive administrative framework to manage all elements of claims processing and support. The solution provides State staff, providers, and members with a full range of online, real-time inquiry and update functions with intuitive web-based data entry screens. The solution maximizes the opportunity to collect valid and complete information throughout the provider’s association with the DPHHS. Team CNSI’s solution for the Base requirements delivers a 100 percent browser-based, interactive, and modular claims processing platform to support the business needs of the State, providers, members and other DPHHS user communities. The solution is fully MITA-aligned, and elements of the solution have previously been certified with CMS in multiple states including Washington, Michigan, and Illinois. Team CNSI’s approach ensures continuous alignment of the system with the latest State and Federal regulatory status, policies, and mandates as well as industry standards as they evolve.

The Team CNSI Advantage

The evoBrix X CPMS 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.

MTCPM-1.2.4-310

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, which provides 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.

Team CNSI’s Solution, Configuration, and Implementation (SCI) methodology builds CMS certification preparation into every step. Our team focuses on requirements traceability to map, analyze, and implement CMS certification checklist criteria to requirements and our solution components. CMS certification preparation begins on day one given the criticality of this milestone for the state to receive matching funds. We have proven our approach successfully with the states of Washington and Michigan. The state of Washington's ProviderOne received CMS certification in July 2011 – the first with no findings based on the then-newly released CMS Medicaid Enterprise Certification Toolkit (MECT). The state of Michigan's CHAMPS followed the next month in August 2011 – also with no findings. We have an archive of certification documentation such as checklist criteria, state responses, and evidence to the criteria from evoBrix X modules which provides a foundation for the completion of all eight (8) checklists identified as applicable under the current MECT version 2.3. Team CNSI continually conducts research and analysis of regulatory and policy changes that impact Medicaid solutions. We also participate in industry conferences to monitor trends and to engage in discussions with state and CMS staff.

The evoBrix X CPMS solution and Team CNSI meet all applicable State and Federal requirements for regulatory policy compliance, audit compliance, and security. Our 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's solution meets all elements of the MITA initiative. The evoBrix X platform aligns with the Seven Conditions and Standards inherently and by design. It is not only aligned to the architectural requirements but also to 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.

DPHHS desires a MITA-aligned solution, enabling the State 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 X CPMS base design documentation, which includes a crosswalk of CPMS functionality to MITA business areas and business processes. This is updated throughout the solution analysis and solution modeling sessions where needed. The CPMS-to-MITA crosswalk is an essential part our approach to support rapid achievement of CMS certification.

CMP30

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

Team CNSI will retain each collection of personally identifiable information (PII) for the time period to fulfill the purpose(s) identified in the records retention schedule;

Team CNSI retains audit records for at least monthly to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements as well as State.

Team CNSI will handle and retain information within the information system and information output from the system in accordance with applicable State laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. We shall ensure that all data is retained in accordance with timeframes as defined in the requirements and with all applicable records retention laws and regulations, unless otherwise mutually agreed to.

CMP32

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

Team CNSI employs sanitization mechanisms consistent with guidance provided in NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization.

The organization finely shreds hard-copy documents using approved equipment, techniques, and procedures, and with a minimum of cross-cut shredding.

Authorized employees of the receiving entity must be responsible for securing magnetic tapes and cartridges before, during, and after processing; and they must ensure that the proper acknowledgement form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies:

- Date received
- Reel/cartridge control number contents
- Movement, and
- If disposed of, the date and method of disposition

Surplus equipment is stored securely while not in use and then disposed of or sanitized in accordance with NIST SP 800-88 revision 1 when no longer required. Required by HIPAA Security Rule: [164.310(d)(1), 164.310(d)(2)(i), 164.310(d)(2)(ii)].

These sanitization mechanisms is based on the policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information.

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 will work collaboratively with the State to ensure that all documentations in its custody are account for by providing data transferred records in a way and manner preferred by the State.

Team CNSI physically controls and securely stores all media that contains PHI or PII and will be stored in a secure facility. We store media in our data center that is not in systems within locked cabinets until final disposition. We maintain logs for storage cabinets storing sensitive media. Any removal of media from storage is documented, citing the location to which the media was relocated.

If media is being decommissioned, it will be destroyed or sanitized using approved equipment, techniques, and procedures. The decommissioning will be logged and signed off by a minimum of two persons from Team CNSI. Understanding that the State is the proprietary owner of any MPATH program-related records and data for which Team CNSI has custody, we comply with requests from the State to transfer or destroy such documentation. To ensure a seamless transfer of such documentation, we ensure that all program records and data are provided in the format specified or 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 provide the state with all documentation on any suspected fraudulent activities as well as abuse and will assist in its investigations. The timely reporting of suspected fraud or abuse supports rapid responses to /remediations of such suspected occurrences, helping ensure paid claims are valid; our system generates written notifications that we review and forward to the State within five (5) business days. Our solution tracks and monitors all claims and enables users to review information through regular and ad-hoc reports and near real-time dashboards. In the event that any suspected fraud or abuse is detected, the claim information is tagged and escalated to our claims analysts who provide additional review and analysis.

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's solution is fully aligned with MITA, which will enable the agency to secure Federal funds for implementation and ongoing maintenance. Our proposed evoBrix X CPMS solution's alignment to MITA maximizes enhanced FFP for the State and provides flexible procurement options to leverage the best-fit solution.

Team CNSI's evoBrix X 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 X CPMS solution base design documentation which includes a crosswalk of CPMS functionality to MITA business areas and business processes. This is updated throughout the solution analysis and solution modeling sessions where needed. The CPMS to MITA crosswalk is an essential part of our strategy to support CMS certification of Team CNSI’s MT CPMS solution.

Figure 3.10.1-10 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 X aligns with that condition/standard.



Figure 3.10.1-10. evoBrix X CPMS solution alignment with Seven Conditions and Standards. evoBrix X 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 meet all data requirements cited in 45 CFR 164.316 and Administrative Rule 37.85.414. As a standard practice, we retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system for 10 years or in

accordance with Administering Entity organizational requirements, whichever is more restrictive to support business needs.

Team CNSI will handle and retain information within the information system and information output from the system in accordance with applicable State laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Team CNSI will maintain all processed data necessary to satisfy State data retention requirements and the needs of other business functions for a time period specified by the State.

CMP06

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

Team CNSI’s has written Privacy and Security policies and procedures to 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 PMO includes a Contracts Manager, Ms. Linda Mras, who 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.

Ms. Mras will ensure that all solicitation documents, SOWs, and applicable contract documentation 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 do so in accordance with NIST Special Publication (SP) 800-35, Guide to Information Technology Security Services.

Once a year, 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,” 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 compliance policies and procedures ensure that all personnel have equal access to goods, services, and communication. This compliance effort is in accordance with Section 508 Of the ADA specific that to federal government agencies and services. The ADA is a broader law that covers all entities, organizations, public, private, and not-for-profit; excluding federal agencies. The ADA Standards require equal access to all goods, services, information, and communication.

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 actively monitors all State and Federal Statutes, CIO Promulgated Rules, State IT policies, rules, and standards to ensure that our solution meets all minimum requirements. For the MT CPMS solution we specifically reviewed the State of Montana IT Strategic Plan, IT Environment, IT Policies and Approved Enterprise Software List (requested and received during the proposal process). We also reviewed all of the technical, architectural, functional, and procedural information provided as part of the procurement library for this solicitation. We perform regular review of all Federal requirements and mandates to ensure continued compliance with any updates or changes. Our senior management team includes policy experts who remain in close communication with State and Federal counterparts to ensure that our solutions continue to map to and align with the latest regulations and mandates. Our technical managers participate in industry technology talks, forums, and other events to ensure that we remain up-to-date on the latest hardware and software technologies and changes.

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 X 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” vision of the MITA 3.0 Standards and Conditions – MITA Condition and has been built with the MITA vision in view.

Our CPMS solution comes with a cross walk from evoBrix X CPMS 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 X CPMS 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 X CPMS solution is a SOA-based system. Facilitated by evoBrix X 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 X Integrator Services enable the evoBrix X CPMS 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 X 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’s MT CPMS solution is built upon standards and components that not only have been previously certified by CMS, but also aligned with MITA 3.0 and the Seven Conditions and Standards from their very inception. By focusing on architecture and standards from day one, our team has been able to lead the industry with modularity and cloud services purposefully built for the Medicaid enterprise. Moreover, our solution isn't based on a theoretical blueprint -- it is based on practical, real-world experience gained from working with multiple states, collaborating with CMS, and participating in MITA work groups.

Specifically, in relation the MITA 3.0 Standards and Conditions – Business Results Condition, our solution provides:

- Proven, Medicaid-based rules engine
- Configuration of adjudication and work management rule
- Centralized rules repository that houses fee for service and cross over claims
- Continuous flow processing of claims
- Customer service through multiple channels focused on providers, consumers, and state staff
- Performance standards and testing
- Adherence to performance standards
- HealthBeat, dashboard tool for transparency and visibility into Medicaid operations, allowing for performance monitoring and triggering performance improvement actions or corrective action plans

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’s MT CPMS solution is built upon standards and components that not only have been previously certified by CMS, but also aligned with MITA 3.0 and the Seven Conditions and Standards from their very inception. By focusing on architecture and standards from day one, our team has been able to lead the industry with modularity and cloud services purposefully built for the Medicaid enterprise. Moreover, our solution isn't based on a theoretical blueprint -- it is based on practical, real-world experience gained from working with multiple states, collaborating with CMS, and participating in MITA work groups.

Specifically, in relation the MITA 3.0 Standards and Conditions – Interoperability Condition, our solution provides:

- Seamless coordination and integration with the exchange leveraging current integration and interoperability technologies (for example SOAP and REST APIs)
- Interaction with other internal entities as well as external agencies
- Open, standards-based interfaces
- Standards-based integration architecture that enables integration and removal of data sources

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 X solution is close alignment with the key principles of service-oriented design. 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 X 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 CPMS solution’s alignment with MITA provides services that enable better and more efficient business processes. Through this framework, these services enable the evoBrix X solution to provide access to business process areas, to functions within the overall MMIS application, and to external components via evoBrix X 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 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.

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

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 similar Medicaid information system solutions in Michigan, Washington, Illinois, and Utah.

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 Amazon Compute 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.

Team 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, Team CNSI's and our customer's confidential information. Team 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 as provided by law, no information in the possession of our team about any individual will 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 has Information Security procedure that establishes a framework to support a strong, multi-faceted security program, and to instill and support a culture of security protection throughout the Company. Team CNSI is committed to having sufficient policies and procedures in place to support a culture of security, and the CNSI employees and independent contractors (Team CNSI users) that work within the Team CNSI culture. This document provides the security requirements that will be followed in the configuration and use of Team CNSI information and information systems by all individuals who have access including, but not limited to system owners, administrators, security personnel and users.

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.

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 evoBrix X solution will handle and retain information within the information system and information output from the system in accordance with applicable federal and State laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Per Team CNSI's Corporate Document Retention Plan team CNSI will maintain all processed data necessary to satisfy Federal and State data retention requirements and the needs of other evoBrix X CPMS business functions for a time period specified by the State in this case for fifteen (15) calendar days period.

MAXIMUS will store the original, received paper copies of all documents and correspondence for 15 calendar days from the received date stamp, post scanning and indexing, allowing for the complete claims process and necessary quality control prior to destroying the documents. The MAXIMUS document processing steps confirm the image quality and content prior to providing the documents for claims review, but will keep the documents as required for easy retrieval if necessary.

MAXIMUS will destroy all original documents which have not been requested for re-scanning using an approved secure shredding service. As we will store the documents in batches by date, we will complete a daily processing of logging the destroyed materials and placing them in the secure, locked shredder service box for pick-up.

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 will ensure all software is used according to licensing and contract agreements and copyright laws. All open-source software usage will be within the constraints of the copyright restrictions for that particular software according to the developer or publisher. We track all software licensing and monitor software usage using configuration management processes and procedures.

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 maintain compliance with Sections 1104 and 1561 of the Affordable Care Act, with standards to ensure accessibility, as well as with security and privacy standards consistent with federal and State laws, in the following areas:

- HIPAA Transaction Standards that ensures IT projects undertaken by states in support of the Affordable Care Act should comply with all relevant HIPAA standards, including protection of personal health information.
- Additional Transaction Standards in the Affordable Care Act which develop interoperable and secure standards and protocols for enrollment.
- Standards for Accessibility, enrollment and eligibility systems should be designed to meet the diverse needs of users (e.g., consumers, state personnel, other third-party assisters) without barriers or diminished function or quality.
- Security and Privacy, Information systems containing individually identifiable information (PII) and/or protected health information (PHI) are required to implement adequate protections (Security Controls) to ensure the protection of sensitive data. The HIPAA Privacy and Security Rules specify privacy and security requirements that HIPAA covered entities must follow. In designing their information systems, agencies should also be aware of State laws that impose additional restrictions on the sharing of sensitive health information.

CMP37

The Contractor's Information Technology Equipment and Software purchased and licensed with monies under this Contract for use by departmental employees, program participants, or members of the public must provide, as required by 18-5-604, MCA, blind or visually impaired persons with access, including interactive use of the equipment and services, that is equivalent to that provided to persons who are not blind or visually impaired.

Team CNSI affirms and agrees that procurement requirement meet the technology access clause.

The nonvisual access standards developed pursuant to subsection (1) must include specifications that are necessary to fulfill the assurances contained in 18-5-603 and must include the following minimum specifications:

- (a) Effective, interactive control and use of the technology, including the operating system, applications programs, and format of the data presented, are readily adaptable to nonvisual means.
- (b) (The technology equipped for nonvisual access must be compatible with information technology used by other individuals with whom the blind or visually impaired individual may interact or exchange electronic information.
- (c) Nonvisual access technology must be integrated into networks used to share communications among employees, program participants, and the public.
- (d) The technology for nonvisual access must have the capability of providing equivalent access by nonvisual means to telecommunications or other interconnected network services used by persons who are not blind or visually impaired.

CMP39

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 be compatible with standard browsers without requiring specialized or proprietary plug-ins..

Team CNSI's evoBrix X solution has multi-browser capabilities including compatibility with multiple versions of including Firefox, Google Chrome, and Internet Explorer. No additional, specialized, or proprietary plug-ins are needed.

CMP40

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 in support of the business results condition to accurately and timely adjudicate claims.

Team CNSI performs continuous training to ensure they are current on the latest development of various Compliance changes and development. These trainings are mandatory for all the employee to get trained and be knowledgeable to support the various businesses accurately and timely manner.

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. The Offeror simply repeating the RFP requirements does not qualify as a good response as defined in Section 6.1.1 of this RFP.

Team CNSI has implemented a robust security framework for ensuring Confidentiality, Integrity, and Availability – known as the CIA Triad. This framework provides multiple layers of external and internal security to protect sensitive and confidential information. The CIA 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:

- 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

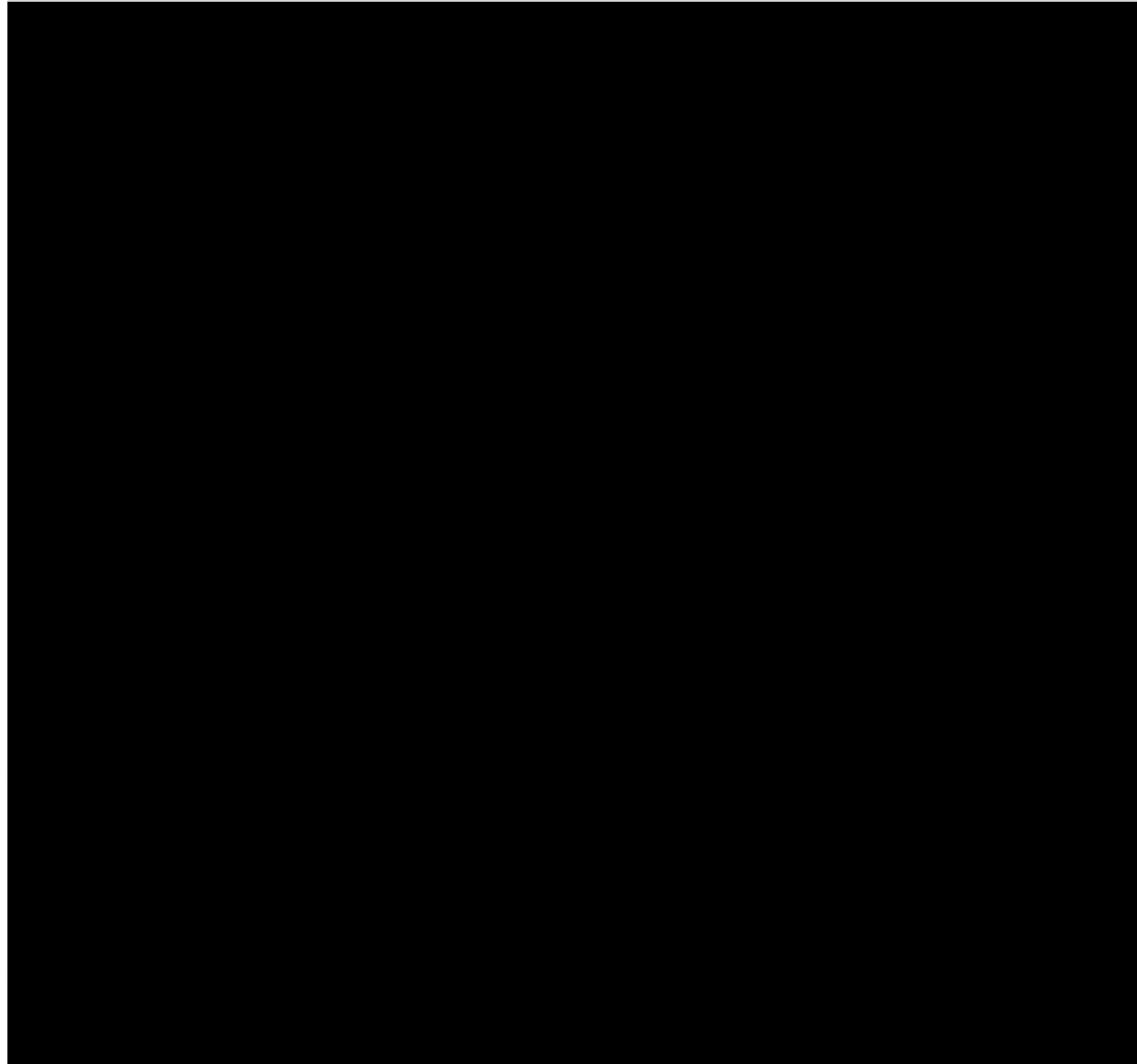
Team CNSI's hosting platform is built on a robust security framework comprising of multiple security and encryption features. These security and encryption features are built using Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) services. Figure 3.10.1-11 provides an overview of the various PaaS and IaaS security services that forms the building blocks of Team CNSI's evoBrix X CPMS solution.

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-certified and HIPAA-certified AWS
- Three-tier application security architecture
- Complaint 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

MTCPM-1.2.4-331



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's approach to developing security controls and procedures for the DPHHS CPMS 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.

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 X CPMS solution to help drive the secure design and implementation of all solution components, including IT infrastructure, systems, and application components.

Due to the maturity of our security practice and the experience we have gained during the past 18 years, Team CNSI is accustomed to performing 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 DOD customers.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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.

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[illegible]

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 Jira Insight 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.

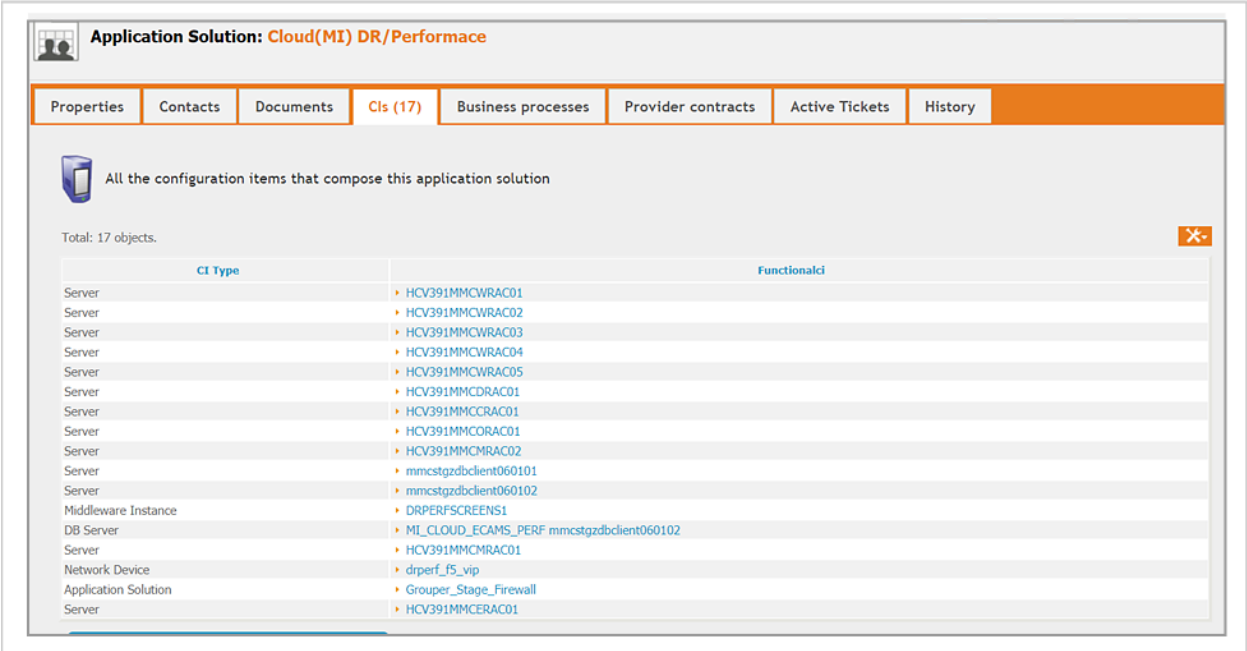
Based on their usage, any unneeded hardware, software and licenses can be decommissioned by going through the Change Control Board (CCB) process. Direction is determined through gaining consensus of all organizations represented at the CCB including, at a minimum, personnel from Team CNSI and DPHHS PMO. 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 CCB:

- 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 X CPMS solution and it is listed in iTOP CMDB maintained by Team CNSI personnel. Figure 3.10.1-14 presents a snapshot of a list of hardware CIs available in the CMDB.



MTCPM-1.2.4-334

Figure 3.10.1-14. Jira Insight CMDB. Through use of this tool, Team CNSI accurately tracks 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 3.10.1-15. The tool records the time and action to provide an audit trail of changes made to a CI.

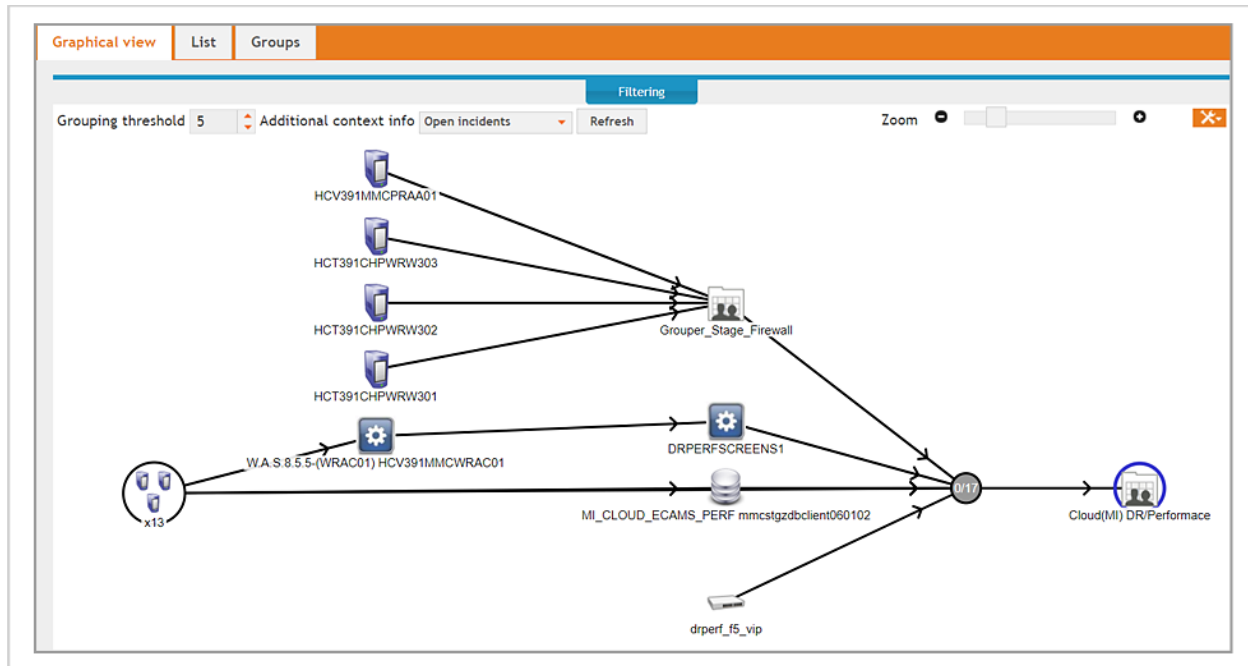
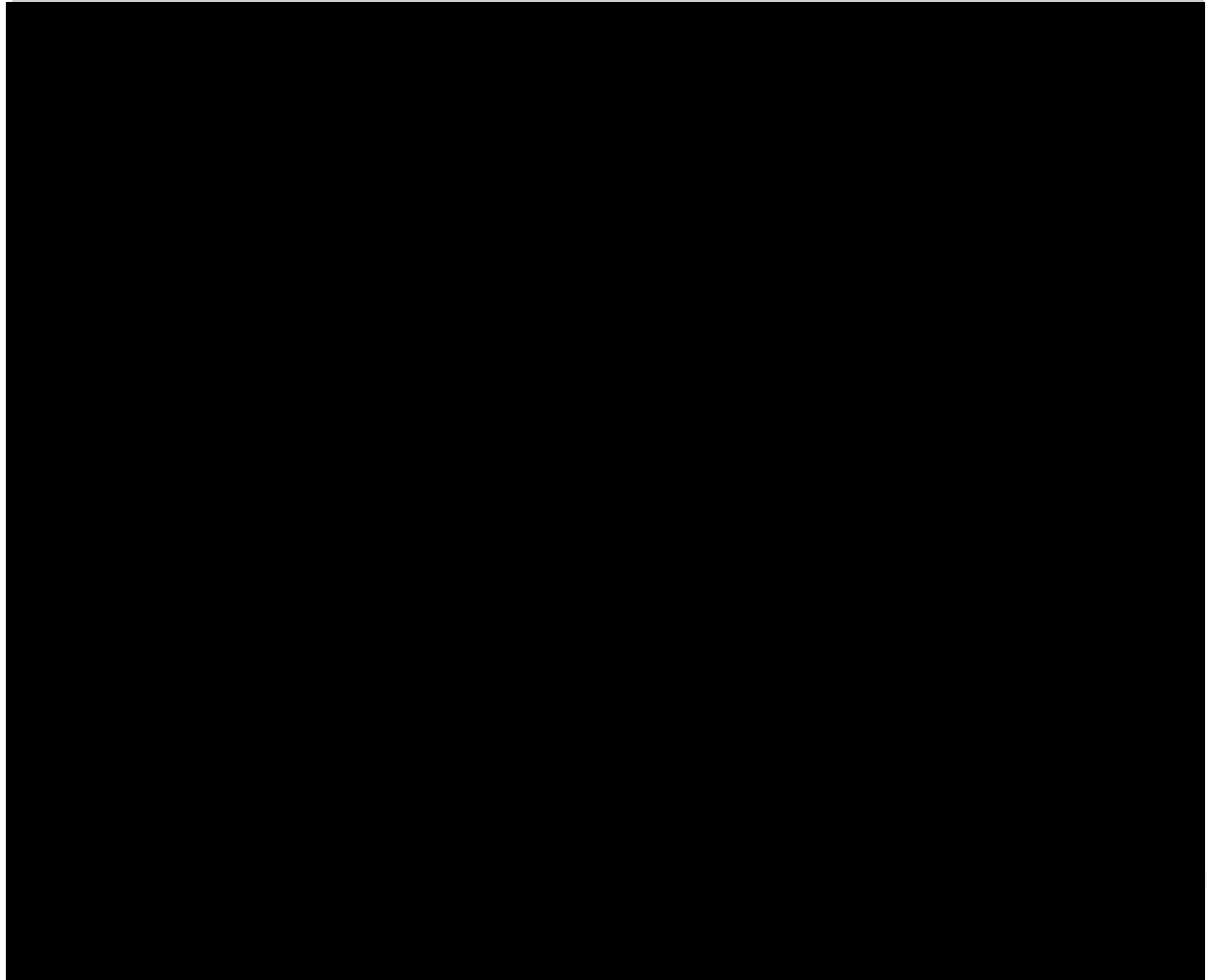


Figure 3.10.1-15. Graphical Representation of Hardware CIs Constituting a Logical Environment. Our MT CPMS solution helps plan for maintenance, availability, and system health of a given logical environment.

SEC04

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

Team CNSI's public cloud is hosted in the AWS FedRAMP public Cloud. Figure 3.10.1-16 describes a multi-layered security approach that protects the backend client data from unauthorized access. The Team CNSI evoBrix X CPMS 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 users are authenticated into the system with which they are interfacing, the presentation tier provides access to the site.

Application/Services Tier

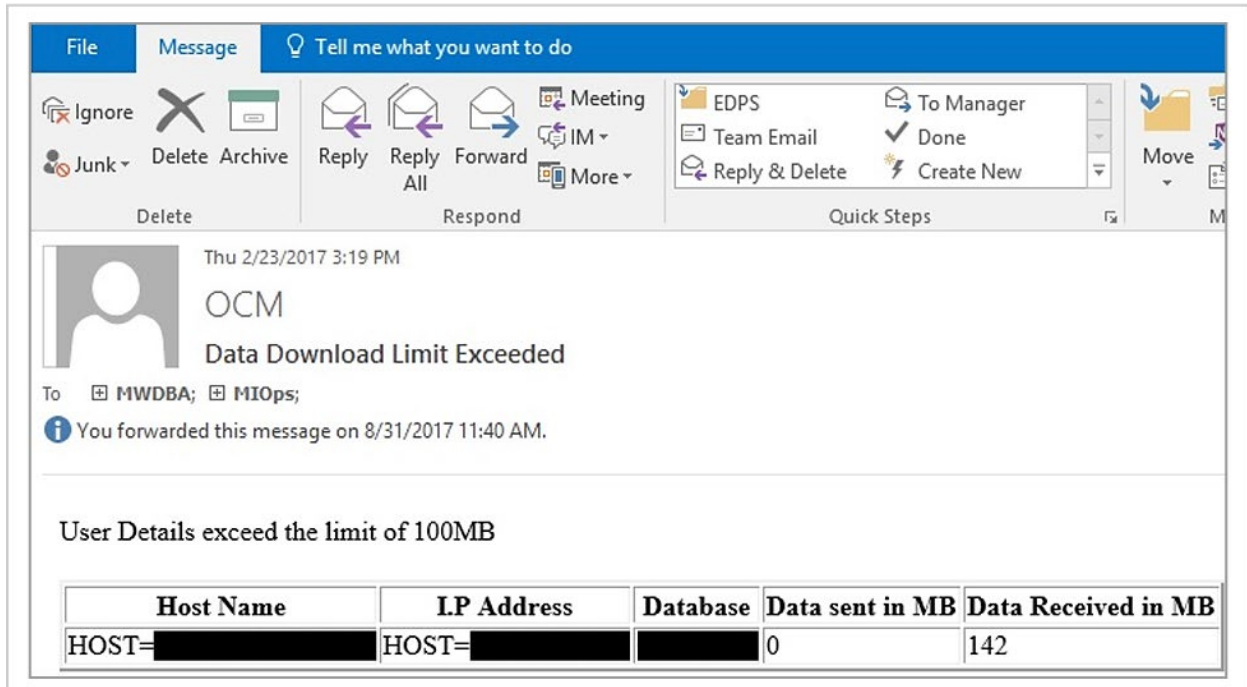
The presentation tier servers interact with the application/services tier. The user does not have any direct access to the application/services tier. The applications then access the data tier. Each tier is protected from the others using firewalls to protect the more sensitive environments from the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

[REDACTED]

[REDACTED]



MTCPM-1.2.4-337

Figure 3.10.1-17. 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 X CPMS solution streamlines electronic transactions by requiring an electronic signature from providers during the claim process to ensure that their intent to accept the terms of the agreement is captured against their claims 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 claim steps, the provider is presented with the terms and conditions they need to review and acknowledge as shown in Figure 3.10.1-18. These screens will be configured to include any specific terms, conditions and/or usage requirements for the state of Montana.

Agreement

Account, Password, and Security

To open an account, you must complete the registration process by providing us with current, complete, and accurate information as prompted by the Registration Form. You will then choose a password. You are entirely responsible for maintaining the confidentiality of your password and account. Furthermore, you are entirely responsible for any and all activities that occur under your account. You agree to notify State of Michigan (SOM) immediately of any unauthorized use of your account or any other breach of security. Do not give out your password or allow it to be seen, or used, by anyone else. If someone else learns your password, they might use this Application to get private information about you without your knowledge that we cannot stop until you change your password.

Use of the Application

☐ I ACCEPT

< Back ✓ Submit Cancel

MTCPM-1.2.4-338

Figure 3.10.1-18. Electronic Signature - Terms and Conditions Screen. Team CNSI's evoBrix X solution supports electronic signatures thus making the electronic transactions compliant with HIPAA and other State and federal mandates.

Team CNSI's evoBrix X CPMS solution will integrate with the State's existing IAM infrastructure to provide a seamless IAM experience for internal and external users across the MPATH system.

Trading Partner Agreements will drive the ability to submit HIPAA transactions and where applicable the app will provide ability to electronically sign.

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.



[REDACTED]

[REDACTED]

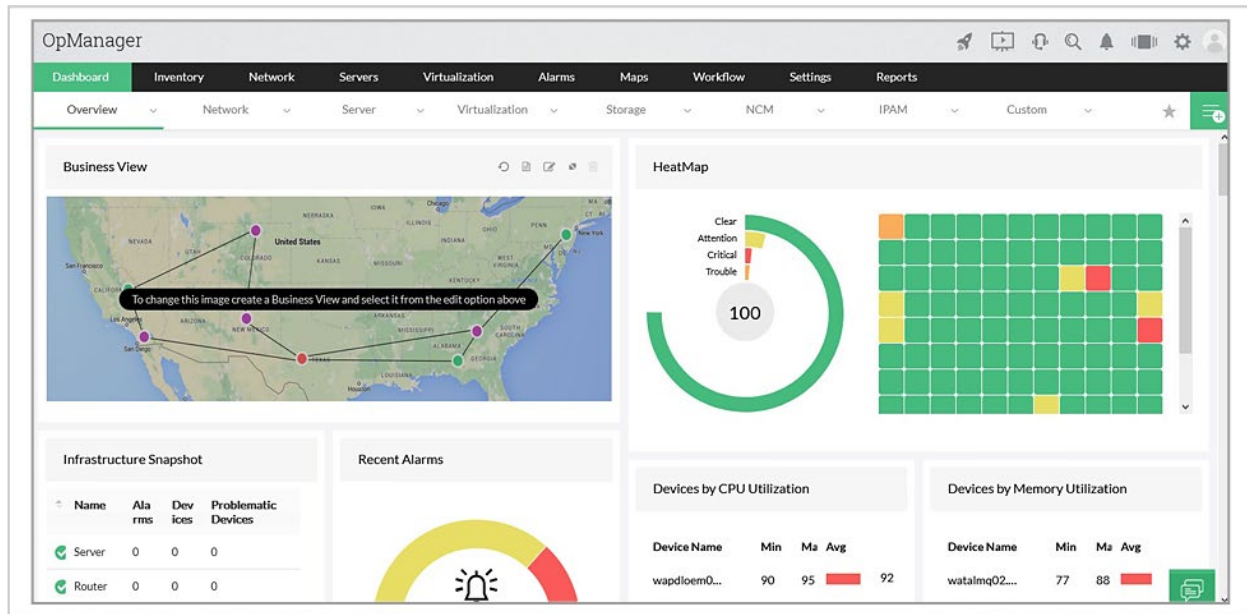
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

example, Figure 3.10.1-20), which provides threat context along with remediation recommendations to form an effective response and help prevent attackers from completing their mission.

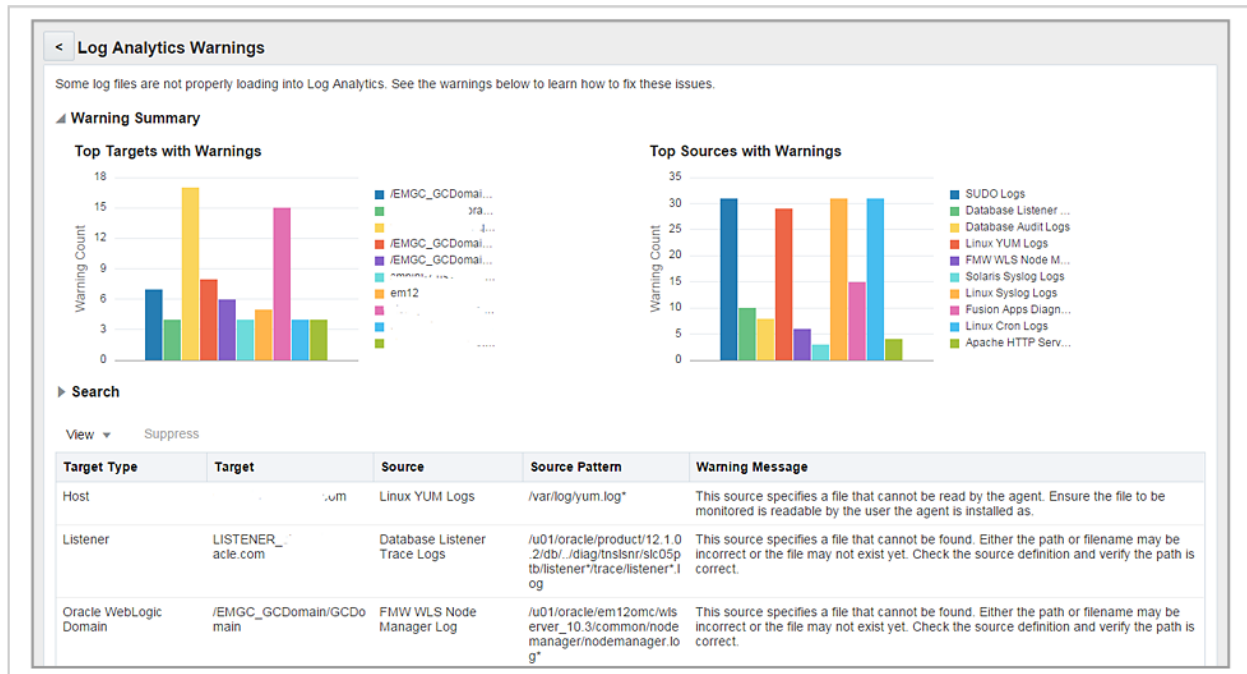


MTCPM-1.2.4-574

Figure 3.10.1-20. OpManager Dashboard. Through this dashboard, Team CNSI can provide integrated SIEM and UEBA capabilities built on machine learning, user session awareness, and up-to-date threat intelligence context.

[REDACTED]

[REDACTED]



MTCPM-1.2.4-341

Figure 3.10.1-21. Oracle Log Analytics Cloud Service Dashboard. Team CNSI can use the Oracle Log Analytics Cloud Service to monitor, aggregate, index, and analyze all log data from multiple sources to detect system anomalies.



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 X CPMS solution includes a robust and comprehensive auditing solution that is used to record both data changes and data access. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]
■ [REDACTED]
■ [REDACTED]

[REDACTED]

[REDACTED]

Application Audit Framework

Team CNSI's evoBrix X CPMS solution has a comprehensive data model that supports record level history/ versioning and audit capability. evoBrix X 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 CPMS in the next interface run.

Team CNSI's evoBrix X CPMS solution for MT CPMS 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 X CPMS 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 X CPMS solution includes a robust and comprehensive auditing solution covering database, network, and application layers. [REDACTED]

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 (View Only, Regular, Super, and Administrator), each with a different security role, and all levels of user access are audited and monitored by the Application Security Framework.

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 CPMS. 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 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 policies are defined in the databases across multiple users covering different SQL types (SELECTs, DDLs, DMLs) and the audit records generated from this database auditing are 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.



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 X CPMS solution is hosted on FedRAMP and HIPAA compliant data centers in AWS FedRAMP Public Cloud. Additionally, Team CNSI's evoBrix X CPMS 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 X CPMS solution is compliant with all these HITECH audit standards – compliance factors for these standards are explained in detail in Figure 3.10.1-22.

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 X CPMS 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 X CPMS 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 X CPMS 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 X CPMS 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 Response Plan (IRP) 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 X CPMS 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 X CPMS 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 X CPMS 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, AWS CloudWatch, AWS CloudTrail, Fire eye Helix, OpManager 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:	SEC07

Audit Standard	Compliance Factor	Proposal Section
	■ 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	

Figure 3.10.1-22. Compliance with HITECH Audit Standards. Team CNSI's evoBrix X CPMS solution is compliant with HITECH audit standards based on these compliance factors.

SEC11

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 will conduct risk assessment of our evoBrix X CPMS solution, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system and the information and data it processes, stores, or transmits. The results will be documented and reviewed at least annually. The risk assessment will be updated at least annually or whenever there are significant changes to evoBrix X or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Team CNSI's evoBrix X CPMS solution 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 3.10.1-23 provides a sample dashboard of NNT Change Tracker's dashboard.

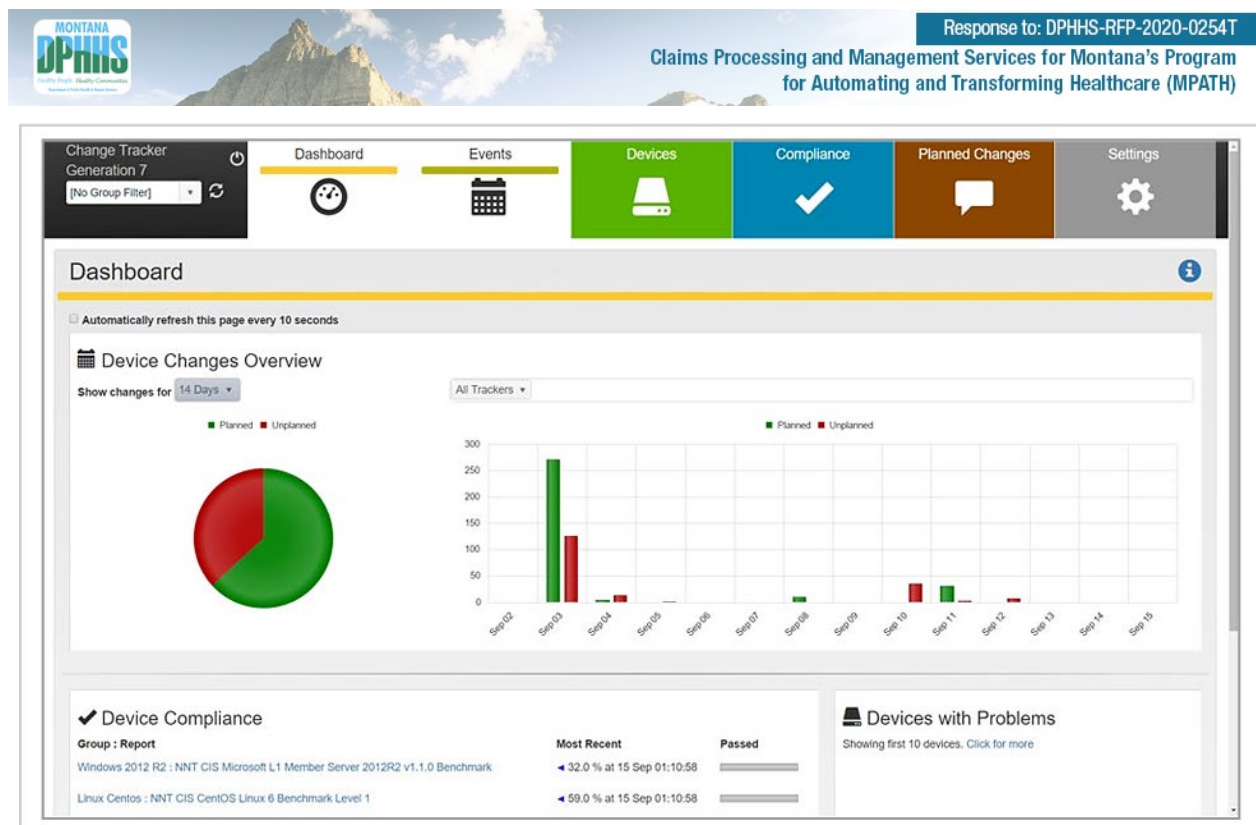


Figure 3.10.1-23. NNT Change Tracker Sample Dashboard. Team CNSI uses NNT Change Tracker to perform risk assessments based on NIST 800-53 rev4 standards.

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. System security is maintained per the system security plan with regular system audits. Team CNSI's evoBrix X CPMS solution is monitored and protected by different PaaS services within the security suite of the AWS Cloud. These PaaS services help to identify usage anomalies and system misuse. The solution suite includes AWS CloudWatch, AWS CloudTrail and OpManager. 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.

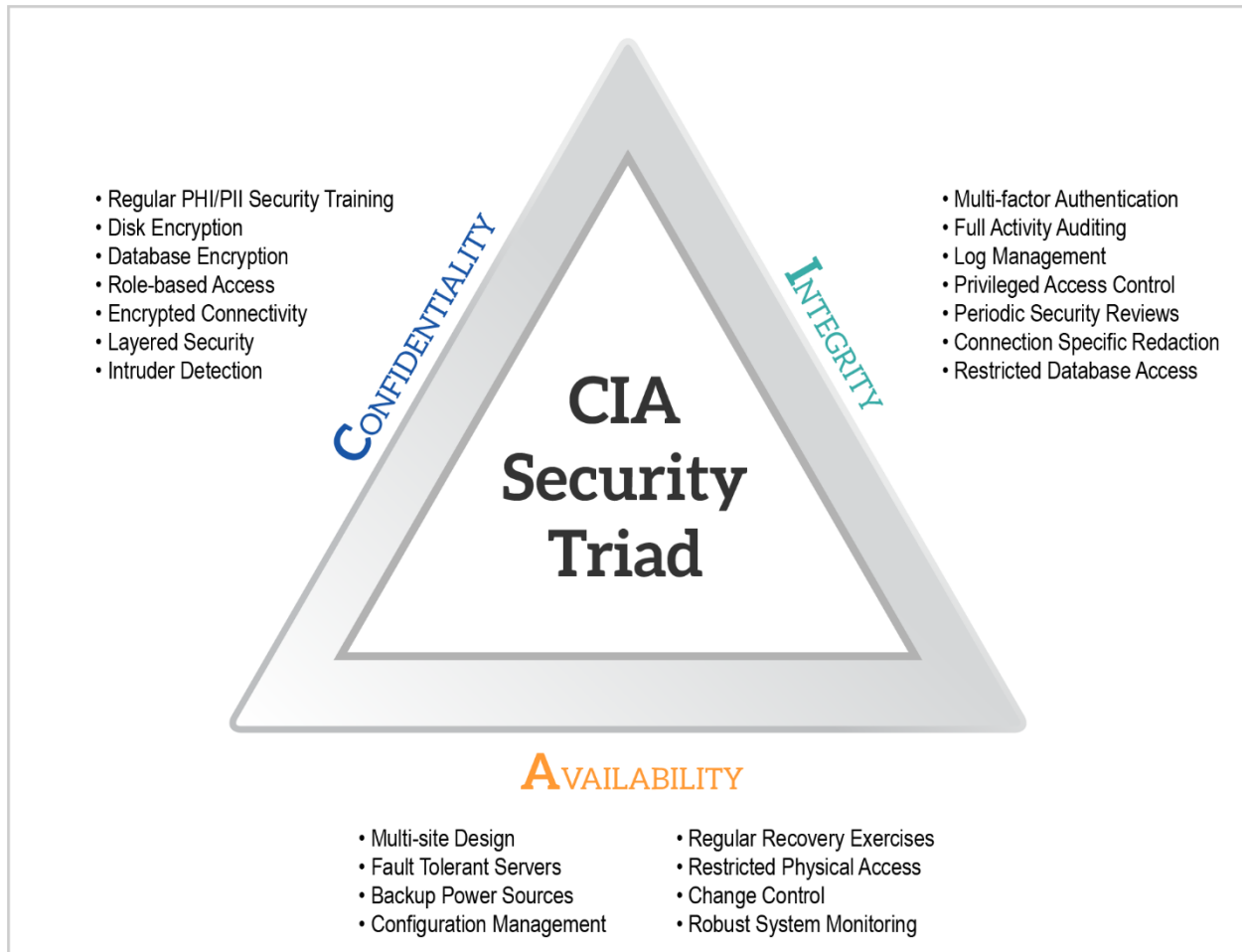
The use of the RBAC model in the system ensures full confidentiality of PHI and PII information. Users of the system can only access a limited set of data based on their authorization in the system. The system facilitates easy removal of people from the list of those who are authorized to view information. 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 X CPMS solution 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 leveraging best practices of the CIA Triad (Confidentiality, Integrity, and Availability) that provides multiple layers of security to protect sensitive or 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 uphold 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 3.10.1-24 provides an overview of the CIA Triad which enforces that Confidentiality, Integrity and Availability is the forefront for Team CNSI's system security design



MTGPM-1.2.4-343

Figure 3.10.1-24. 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 X CPMS solution only after authenticating to the MT CPMS 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. 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 CPMS solution will not include any code of unknown origin. The evoBrix X CPMS 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 3.10.1-25 lists the 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
Hardware	Servers and routers that help implement the project activities

Figure 3.10.1-25. Types of CIs. Various types of CIs are tracked in Team CNSI's evoBrix X CPMS.

Figure 3.10.1-26 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	JIRA Insight/Wiki	Initiation of the Project

Figure 3.10.1-26. Items Under Configuration Management. Team CNSI can list each type of CI, within a repository where they are stored, and identify 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 X CPMS 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:

- Scan the source code using Rogue Wave
- Identify and resolve any discovered issues
- Perform license review
- Perform architectural review
- 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 X CPMS 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 X CPMS solution will be hosted in AWS public Cloud. In the AWS public 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 six 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.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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 three distinct 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 X CPMS 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 AWS public 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 X CPMS 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, AWS Cloudwatch Cloud Service and it is applicable for all users including administrators.
- Usage anomalies: Team CNSI's evoBrix X CPMS solution is monitored and protected by various IaaS services within the security suite of the AWS Cloud. These IaaS services help to identify usage anomalies and system misuse. The solution suite includes AWS Cloudwatch and AWS Cloudtrail. 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 X CPMS 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.

Team CNSI shall provide staff necessary for 24x7x365 support and ongoing maintenance to infrastructure to ensure the availability of the managed environments.

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 X CPMS solution includes a comprehensive and complete system monitoring and reporting framework.

Figure 3.10.1-27 provides a classification of monitoring tools and their respective infrastructure modules

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 3.10.1-28 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

Tier	Team CNSI Area(s)	Details	Availability	Response
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 3.10.1-28. Team CNSI's System Support Model. We establish 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 X CPMS 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.

[illegible]

SEC20

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

Team CNSI evoBrix X CPMS solution for MPATH 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.

- [REDACTED]
- [REDACTED]
- [REDACTED]

Physical Transmission

Team CNSI's evoBrix X CPMS solution does not normally require physical transmission of data using disks or disk partitions. However, when a need arises, then [REDACTED]

[REDACTED]

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 X CPMS 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 X CPMS solution is hosted in the AWS public 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 X CPMS 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. Our 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 at the Federal and State level including for the states of Washington, Michigan and Utah. These state-specific security plan implementations demonstrate Team CNSI's extensive experience 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 X CPMS 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 X CPMS 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 X CPMS 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 X

CPMS 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 the State of Montana's security and privacy control requirements and our proposed evoBrix X CPMS solution complies with these security processes.

The Team CNSI evoBrix X CPMS, hosted in AWS public 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 response to SEC22, page 108 of this section.

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 our response to SEC72 (pages 150-151).

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 X CPMS 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 X CPMS 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 X CPMS 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 incorporates 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 X applications is a critical security activity. Each security level and account follow our evoBrix X 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 3.10.1-30 provides an overview of different compliance factors that are built into the Team CNSI's evoBrix X solution to enforces the below required security controls.

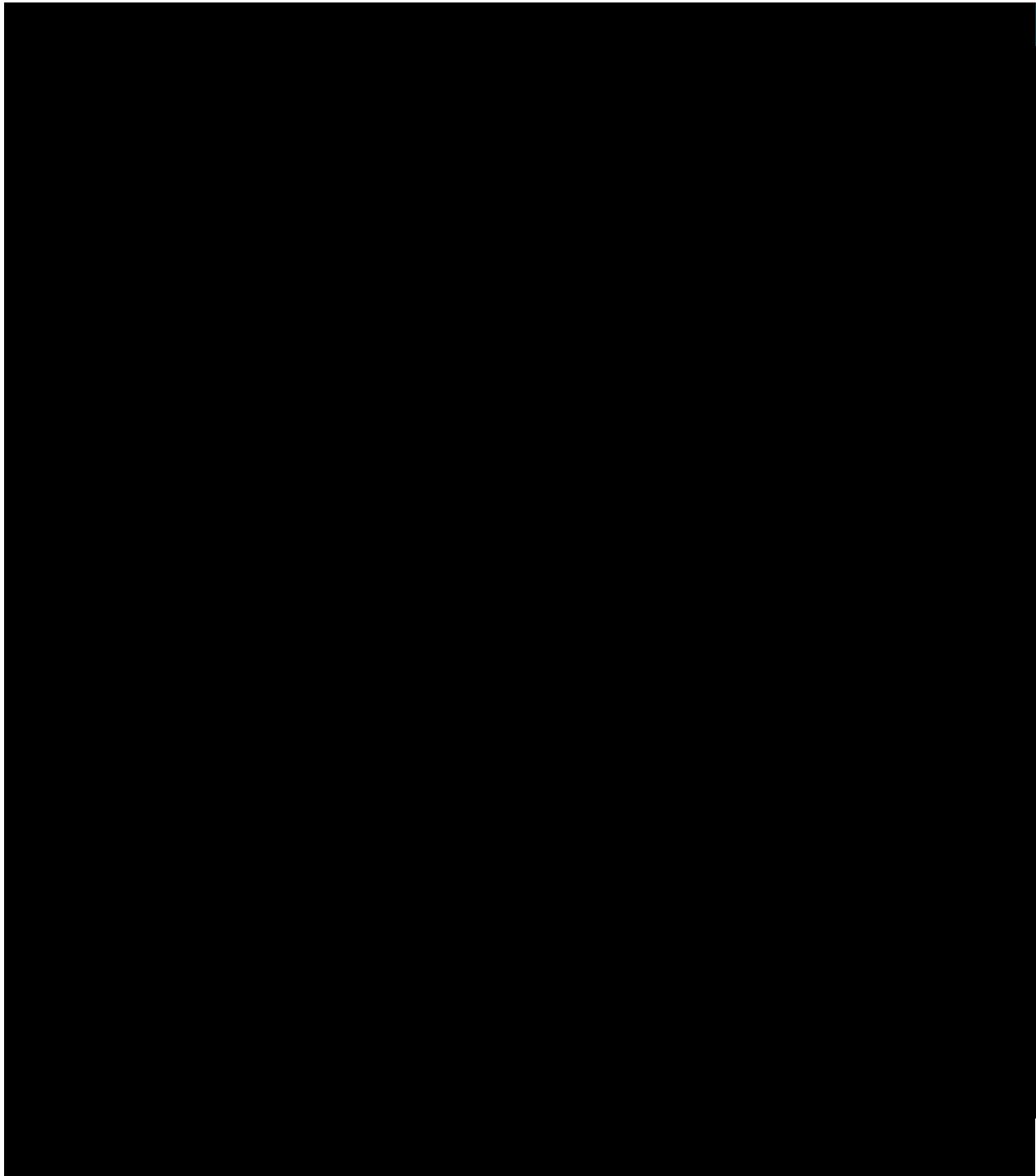
Security Control	Compliance Factors
Requires a unique sign-on (ID and password)	Each system administration account/password is unique. Each end user account/password is unique.
Supports a user security profile that controls user access rights to data categories and system functions	Team CNSI evoBrix X CPMS 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 X CPMS solution notifies the systems team via email of potential risks and violations detected by our automated systems tools.

Figure 3.10.1-30. 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 X CPMS. 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 3.10.1-31.



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 X CPMS 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 X Security Framework is implemented through the conceptual network of user accounts, domains, profiles, roles, pages, and page controls. Each user within the evoBrix X CPMS 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 X CPMS 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 public cloud is hosted in AWS's FedRAMP Public Cloud. Access to Team CNSI's cloud infrastructure is tightly controlled and it is strictly limited to AWS 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 AWS FedRAMP and HIPAA complaint 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 X CPMS solution includes security and privacy controls that are compliant with the most current version of FISMA and NIST standards. Team CNSI's evoBrix X CPMS 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 X CPMS 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 CPMS. Team CNSI's evoBrix X CPMS solution has a comprehensive data model that supports record level history/versioning and audit capability. evoBrix X 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 CPMS in the next interface run.

Data De-identification

Team CNSI ensures that data in all development and system test environments for MT CPMS 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,

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 uses the Fortify 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 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.

[illegible]

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
- Tenable 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).



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 X CPMS 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 environment. 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 use Amazon Cognito 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, page 81.

SEC42

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

Due to our prior relevant 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. This data security audit includes auditing multiple systems and processes within Team CNSI's evoBrix X CPMS and these systems and processes are described below.

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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 CPMS. 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 3.10.1-34 provides an overview of all the network vulnerabilities areas and the audit security solutions that are implemented in Team CNSI's evoBrix X CPMS solution.

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

Network Vulnerability Area	Scope	Audit Security Solutions
Availability	Lost connectivity in networks could cause business interruption.	■ Team CNSI's hosting platform in AWS Public 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 (AWS Cloudwatch, AWS Cloudtrail, Fireeye Helix 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 3.10.1-34. Audit Security Solutions for Network Vulnerabilities. Team CNSI's evoBrix X CPMS solution offers Audit Security features to address network vulnerabilities.

SEC43

The Contractor shall provide, configure, support, maintain and manage a federated identity and access management solution that will perform user authentication and authorization through single sign-on for all module components.

Team CNSI user accounts will be provisioned based on federated system account information sent from the provisioned Single Sign-On (SSO) login. System user accounts will be provisioned within an internal directory and used solely for enforcing authorization to the application.

Database administrator accounts are stored within the Oracle database system. These accounts are managed by the Oracle database team.

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 X CPMS does comply with these security processes.

Team CNSI's evoBrix X CPMS solution undergoes risk assessment covering NIST SP 800-53 Rev 4

[REDACTED]

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 X CPMS 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.

[illegible]

[illegible]

Incident Management

Team CNSI operational teams use Atlassian Jira 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 24x7x365 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 3.10.1-35 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 (via a Production Incident Report shown in Figure 3.10.1-35). Follow up reviews of the actions are conducted to make sure they are properly alleviating the issue and to determine whether there is a more efficient way of correcting or preventing the problem.



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

MTCPM-1.2.4.344

Figure 3.10.1-35. 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 X CPMS solution is monitored and protected by different PaaS services within the security suite of the AWS Cloud. These PaaS services help to identify usage anomalies and system misuse.

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, page 88.

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 Fortify 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, page 115.

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

The evoBrix X CPMS solution will integrate with the MPATH 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 3.10.1-36 provides a complete list of access standards and the equivalent compliance features that are built into the evoBrix X CPMS 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 X 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 (p. 81) SEC48 (p. 127)
Authenticates the receiving entity prior to a system-initiated session, such as transmitting responses to case inquiries.	■ Team CNSI's evoBrix X CPMS 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 CPMS and other state agencies. ■ This establishes a 256bit SSL encrypted tunnel.	SEC01 (p. 81)
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 (p. 127)
Identity verification information, and an indicator of employee versus contractor.	■ Team CNSI's OMP product tracks and records this information.	SEC48 (p. 127)
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 (p. 98) SEC01 (p. 81)
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 (p. 82)
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 (p. 82)
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 (p. 82)
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 (p. 143)

Access Standards	Compliance Features	Proposal Section
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 (p. 143)
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. [REDACTED] These tools enable rapid detection, investigation, and remediation of the broadest range of security threats across Team CNSI's cloud IT assets.	SEC06 (p. 88)

Figure 3.10.1-36. Compliance to Access Standards. evoBrix X CPMS solution includes built-in access standards and the equivalent compliance features.

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:

- Team CNSI personnel logs into OMP and creates a ticket for Named User Access.
- 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.
- 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.
- The ticket is then approved by the Project Manager, which is the second level of approval.
- Finally, the ticket is approved by the Operations Manager, which is the third level of approval.
- 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.
- Once the ticket is approved, it is then submitted to the respective Admin team.
- 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 3.10.1-37. 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 [REDACTED]

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,PRDMMISMV_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
BHR	12-30-2011 16:52:03	OPEN	USER_PROFILE	PRDMMIS_MC_534,MIEHRPROD_READ,AUDIT_SYS_PRIVS,CONNECT,PRDMMIS_READ
BHU	01-25-2016 11:11:50	OPEN	USER_PROFILE	AUDIT_SYS_PRIVS,PRDMMISIR_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,PRDMMISIR_READ
CHA	03-02-2015 15:08:06	OPEN	USER_PROFILE	PRDCNVSTG_READ,CONNECT,PRDMMIS_READ,AUDIT_SYS_PRIVS
CHA	06-03-2015 14:00:15	EXPIRED(GRACE)	USER_PROFILE	DBA,AUDIT_SYS_PRIVS,CONNECT,MIEHRPROD_READ
CHE	09-13-2012 11:13:59	OPEN	USER_PROFILE	PRDMMISIR_READ,PRDMMISIR_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,PRDMMISIR_READ,AUDIT_SYS_PRIVS,PRDMMIS_READ,PRDMMISIR_READ

MTCPM-1.2.4-345

Figure 3.10.1-37. 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 3.10.1-38. 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 [REDACTED]

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_CATEGORY3	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
MIEHRPRODISR_READ	DW_EHR_LOOKUP_TARGET5	MIEHRPRODISR	SELECT

MTCPM-1.2.4-346

Figure 3.10.1-38. Roles and Privilege Report. Team CNSI can provide a report that contains the list of roles present in the system along with the list of objects and type of privileges.

Team CNSI's evoBrix X CPMS 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 3.10.1-39.

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 3.10.1-39. evoBrix X CPMS' Profiles. The evoBrix X CPMS solution features multiple profiles that 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 X CPMS 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 AWS public Cloud. These PaaS services help to identify usage anomalies and system misuse, report security incidents and mitigate the same.

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

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 X CPMS in AWS public 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.

Country	Year	Population (millions)	Population (millions)
Algeria	2010	34.0	34.0
Algeria	2011	34.5	34.5
Algeria	2012	35.0	35.0
Algeria	2013	35.5	35.5
Algeria	2014	36.0	36.0
Algeria	2015	36.5	36.5
Algeria	2016	37.0	37.0
Algeria	2017	37.5	37.5
Algeria	2018	38.0	38.0
Algeria	2019	38.5	38.5
Algeria	2020	39.0	39.0
Algeria	2021	39.5	39.5
Algeria	2022	40.0	40.0
Algeria	2023	40.5	40.5
Algeria	2024	41.0	41.0
Algeria	2025	41.5	41.5
Algeria	2026	42.0	42.0
Algeria	2027	42.5	42.5
Algeria	2028	43.0	43.0
Algeria	2029	43.5	43.5
Algeria	2030	44.0	44.0
Algeria	2031	44.5	44.5
Algeria	2032	45.0	45.0
Algeria	2033	45.5	45.5
Algeria	2034	46.0	46.0
Algeria	2035	46.5	46.5
Algeria	2036	47.0	47.0
Algeria	2037	47.5	47.5
Algeria	2038	48.0	48.0
Algeria	2039	48.5	48.5
Algeria	2040	49.0	49.0
Algeria	2041	49.5	49.5
Algeria	2042	50.0	50.0
Algeria	2043	50.5	50.5
Algeria	2044	51.0	51.0
Algeria	2045	51.5	51.5
Algeria	2046	52.0	52.0
Algeria	2047	52.5	52.5
Algeria	2048	53.0	53.0
Algeria	2049	53.5	53.5
Algeria	2050	54.0	54.0
Algeria	2051	54.5	54.5
Algeria	2052	55.0	55.0
Algeria	2053	55.5	55.5
Algeria	2054	56.0	56.0
Algeria	2055	56.5	56.5
Algeria	2056	57.0	57.0
Algeria	2057	57.5	57.5
Algeria	2058	58.0	58.0
Algeria	2059	58.5	58.5
Algeria	2060	59.0	59.0
Algeria	2061	59.5	59.5
Algeria	2062	60.0	60.0
Algeria	2063	60.5	60.5
Algeria	2064	61.0	61.0
Algeria	2065	61.5	61.5
Algeria	2066	62.0	62.0
Algeria	2067	62.5	62.5
Algeria	2068	63.0	63.0
Algeria	2069	63.5	63.5
Algeria	2070	64.0	64.0
Algeria	2071	64.5	64.5
Algeria	2072	65.0	65.0
Algeria	2073	65.5	65.5
Algeria	2074	66.0	66.0
Algeria	2075	66.5	66.5
Algeria	2076	67.0	67.0
Algeria	2077	67.5	67.5
Algeria	2078	68.0	68.0
Algeria	2079	68.5	68.5
Algeria	2080	69.0	69.0
Algeria	2081	69.5	69.5
Algeria	2082	70.0	70.0
Algeria	2083	70.5	70.5
Algeria	2084	71.0	71.0
Algeria	2085	71.5	71.5
Algeria	2086	72.0	72.0
Algeria	2087	72.5	72.5
Algeria	2088	73.0	73.0
Algeria	2089	73.5	73.5
Algeria	2090	74.0	74.0
Algeria	2091	74.5	74.5
Algeria	2092	75.0	75.0
Algeria	2093	75.5	75.5
Algeria	2094	76.0	76.0
Algeria	2095	76.5	76.5
Algeria	2096	77.0	77.0
Algeria	2097	77.5	77.

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, page 115.

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 X CPMS solution understands the importance of maintaining data integrity during transit. All connections to the DPHHS CPMS 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 X CPMS 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 X CPMS 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 X CPMS 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 compliant with the Harmonized Security and Privacy Framework - Exchange Reference Architecture Supplement Version 1.0.

Team CNSI's evoBrix X CPMS solution is compliant with the following security and privacy controls that are related to Harmonized Security and Privacy Framework. Figure 3.10.1-42 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 (p. 82)
Identify, Credential and Access Management	■ Identify Proofing ■ Authorization	SEC01 (p. 81)
Secure Infrastructure and Managed Services Computing	■ Data Encryption Solutions ■ Data protection/audit Methods ■ Infrastructure Monitoring Framework	SEC02 (p. 82) SEC07 (p. 91) SEC18 (p. 104)
Data Encryption	■ Data Encryption at Rest ■ Data Encryption in Transit	SEC02 (p. 82)
Audit Trails	■ Data protection/audit Methods	SEC07 (p. 91)

Control Name	Key Compliance Factors	Proposal Location/ Security Requirement #
Continuity of Operations and Disaster Recovery	Disaster Recovery Process	SEC16 (p. 101)
Compliance Oversight	- Risk Assessment and Management - Penetration Testing - Protection against Vulnerabilities - Continuous Monitoring and Reporting	SEC55 (p. 133) SEC15 (p. 101) SEC38 (p. 115) SEC18 (p. 104)
Privacy	- Accessibility - Data Integrity - Accountability	SEC64 (p. 141) SEC61 (p. 138) SEC06 (p. 88)
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 (p. 97)

Figure 3.10.1-42. Harmonized Security and Privacy Framework. Team CNSI's evoBrix X CPMS solution provides 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 Specifications to build secure web services to implement message content integrity and confidentiality.



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 X CPMS 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 3.10.1-43.

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 3.10.1-43. POA&M Template Header Information Description. Our solution displays POA&M Template Header and 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 3.10.1-44.

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.

Column	Details
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 3.10.1-44. POA&M Template Column Information Description. We provide detailed information containing corrective action plans 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 X CPMS is hosted in an AWS Public 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 X CPMS 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 X CPMS 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 X CPMS 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 X CPMS 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 X CPMS 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 guidelines within HIPAA is to develop emergency access procedures, so that we are compliant with Security Rule safeguard standards and Team CNSI's evoBrix X CPMS 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 X CPMS solution. Team CNSI tests the Contingency Plan every 12 months including the backup media testing. If testing reveals that the Contingency Plan will be 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 and disaster recovery in different availability zones of one of AWS region. 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 X CPMS 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:

- AWS Cloud Backup Service: All the systems are backed up using Oracle's Database Backup Service and AWS Cloud Infrastructure Object and Archive Storage Service. All data running in the environment is backed up in its native format and stored on off-device storage appliances.
 - AWS Cloud Infrastructure Object Storage– Storage for both structured and unstructured data including backups supported by enterprise-class data protection, resilience, and elastic scalability
 - AWS Cloud Infrastructure Archive Storage – 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

AWS EBS backup Volume 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 X CPMS 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 X CPMS 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 X CPMS 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.
- [REDACTED]
- [REDACTED]
- Oracle Database Backups are validated on a weekly basis to ensure that backup data is not altered or destroyed during transit.

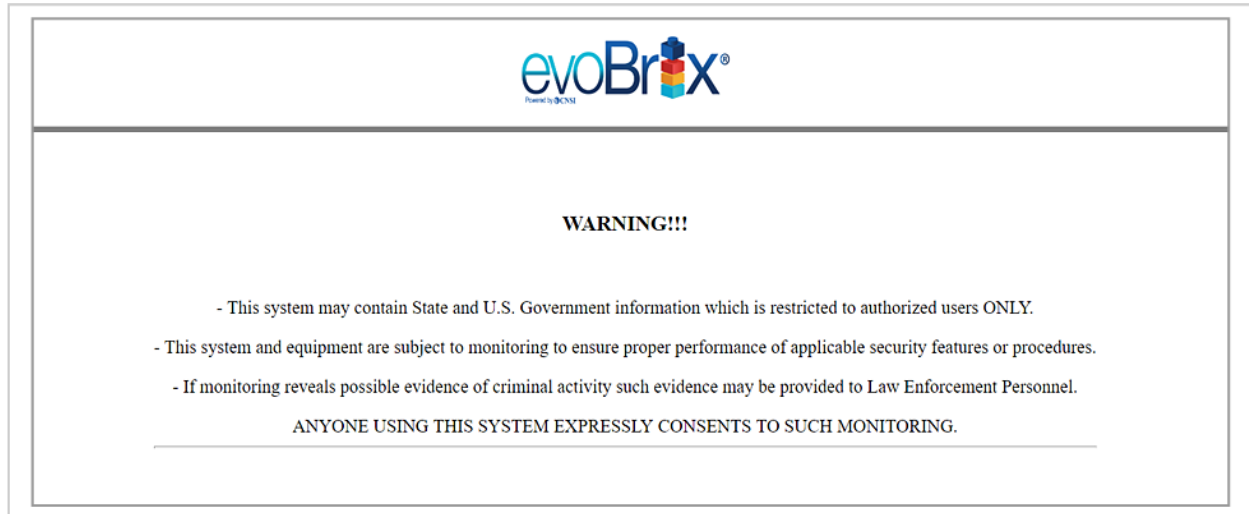
Additionally, all access to data is monitored, logged, and recorded to show who accesses data, and what they do. Access to Team CNSI's solution is monitored and protected by different PaaS services within the security suite of the AWS Cloud. These PaaS services help to identify usage anomalies and system misuse. [REDACTED]

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 X CPMS includes appropriate security warning banners. Additionally, login screens for access to backend systems by systems administrators display appropriate security warning banners that are prominently displayed on login. These banner messages are illustrated in Figure 3.10.1-45 and Figure 3.10.1-46.



MTCPM-1.2.4-347

Figure 3.10.1-45. Application Usage Banner Message. Team CNSI's evoBrix X CPMS Application includes a security warning banner when logging in.

WARNING

-This system may contain State and U.S. Government information which is restricted to authorized users ONLY.

-Unauthorized access use misuse or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18 United States Code Section 1030 and may subject the individual to Criminal and Civil penalties pursuant to Title 26 United States Code Sections 7213 7213A.

-This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures.

-Such monitoring may result in the acquisition recording and analysis of all data being communicated transmitted processed or stored in this system by a user.

-If monitoring reveals possible evidence of criminal activity such evidence may be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

Using keyboard-interactive authentication.
Password:

MTCPM-1.2.4-348

Figure 3.10.1-46. Backend System Access Banner Message. A security warning banner is shown when accessing backend systems in Team CNSI's evoBrix X CPMS 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 AWS Public Cloud Platform, which 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

AWS IaaS 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 AWS 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, AWS 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 AWS 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 AWS 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

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 3.10.1-48, 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 [REDACTED]				
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,PRDMMISMV_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
BHN	12/30/2011 16:52:03	OPEN	USER_PROFILE	PRDMMIS_MC_334,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

MTCPM-1.24-345

Figure 3.10.1-48. 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

- An automated report called “User Access Report” is scheduled every quarter
- 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
- Figure 64-1 describes a sample “User Access Report”
- This report gets delivered to the Operations Support Team, every quarter
- Operations Support Team reviews the user list
- During this review process, Operations Support Team raises tickets in OMP, if any of the below conditions are true
- If a user left the company or the user is no longer working on the current project
- A user’s role or responsibilities changed
- 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 3.10.1-49 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 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 3.10.1-49. 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 X CPMS 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 CPMS, 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 X CPMS 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 X CPMS 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:

- Team CNSI personnel logs into OMP and creates a ticket for Named User Access.
- 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.
- 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.
- The ticket is then approved by the Project Manager, which is the second level of approval.
- Finally, the ticket is approved by the Operations Manager, which is the third level of approval.
- 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.
- Once the ticket is approved, it is then submitted to the respective admin team.
- 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 consolidate 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 X CPMS 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 3.10.1-50.

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 X CPMS solution has robust and multi-tier audit system with a centralized repository to store and preserve the audit data	SEC07 (p. 91)
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 X CPMS solution includes appropriate security warning banners including banners for application access as well as for backend system access	SEC62 (p. 139)
Involve application and system owners, when appropriate, to determine what user activities should trigger an entry in the audit trails.	Team CNSI's evoBrix X CPMS 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 (p. 88)
Determine how random audits will be conducted as well as the frequency of those audits.	Team CNSI's evoBrix X CPMS includes periodic risk-based assessments based on NIST SP 800-53 rev4 standards and periodic penetration testing.	SEC55 (p. 133)
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 (p. 121)
Determine what audit tools will be used for automatic monitoring and reporting	Team CNSI's evoBrix X CPMS solution includes a robust and comprehensive auditing solution that is used to record both data changes and data access.	SEC07 (p. 91)
Determine what to Audit	Team CNSI's evoBrix X CPMS 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 (p. 91)

Audit Standard	Compliance Factor	Proposal Section
Implementing Audit Tools	Team CNSI's evoBrix X CPMS 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 (p. 91) SEC06 (p. 88)
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 (p. 91)

Figure 3.10.1-50. Compliance with HITECH Audit Standards. Team CNSI's evoBrix X CPMS 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 X CPMS 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 CPMS 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.

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 CPMS 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 3.10.1-51 to support the masking/de-identification needs for MT CPMS.

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 X CPMS solution.	Greatly reduces the risk of a privacy data breach because the MT CPMS project staff would only have access to de-identified data in the non-Production environments such as Development and System Test.

Features	Benefits
■ 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 CPMS 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.	■ 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 known about the data, the better the outcome. ■ Drives key operational, analytical, and strategic initiatives.

Figure 3.10.1-51. 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 CPMS.

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.

- Names
- Geographic subdivisions smaller than a state
- 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)
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- 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 X CPMS 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 X CPMS 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 X CPMS 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 X CPMS 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 CCB and its change control process. Direction is determined by consensus of all organizations represented at the CCB including, at a minimum, personnel from Team CNSI, the MPATH Project Manager, MPATH Program Management Office, and other stakeholders as identified and approved by DPHHS. 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 CCB 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

SEC82

The Contractor's transmission security shall use, at a minimum, TLS 1.2, SHA 2 with a minimum of a 2048 bit key, or a more advanced industry standard transmission security protocol.

Team CNSI system protects the confidentiality and integrity of transmitted information over internal and external network. Team CNSI uses federal approved FIPS 140-2(Federal Information Processing Standard-2) standards to store and transmit all data.

All communication and transmission of DPHHS data uses private IPsec VPN tunnel or HTTPS web connections. IPsec VPN tunnel and Web session connections always use HTTPS (TLS 1.2) and SHA 2 encrypted secured hash encryption algorithms.

Cornerstone MFT uses cryptographic standards that are compliant with FIPS 140-2, NIST and HHSC standards for encryption. Cornerstone MFT server enables interface data is encrypted both in transit and at rest using PGP RSA (512, 1024, 2048 or 4096 bits) encryption standard.

SEC83

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 ninety (90) 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 ninety (90) 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 in detail their approach to solutions and services that meet State and federal regulations and each of the Hosting requirements detailed in Attachment F – Requirements Response Matrix. The Offeror simply repeating the RFP requirements does not qualify as a good response as defined in Section 6.1.1 of this RFP.

Cloud-based hosting of the claims processing and management module enables the State to maintain information system flexibility, scalability, cost-efficiency and enhanced integration capabilities. Team CNSI offers a cloud hosting solution, hosted in the AWS FedRAMP Moderate-compliant public cloud and Statement on Standards for Attestation Engagements (SSAE-16) SOC 1 Type 2 and SOC 2 Type 2 compliant. The information in this section applies to the Core Solution, Option A, Option B, and Option C.

The Team CNSI Advantage

Team CNSI's cloud solution provides high availability and reliability in a secure, scalable, and flexible FedRamp certified environment.

- Hosted in AWS FedRAMP certified and HIPAA certified Cloud
- A multi-tier secure Software-as-a-Service (SaaS) solution fully compliant with federal standards and mandates
- Dynamic elastic scalability enables rapid provisioning of additional compute and memory resources to meet current and future needs
- Redundant Disaster Recovery platform supported by a comprehensive Business Continuity plan

MTCPM-1.2.4-073

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 X CPMS solution is hosted in AWS's FedRAMP and HIPAA compliant public cloud. This hosting platform has all the cloud features built in 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 Infrastructure as a Service (IaaS) services, or Software as a Service (SaaS) services, thereby creating a highly flexible and elastic environment. Additional IaaS services in Team CNSI's public cloud can be subscribed to or cancelled, on an ad hoc basis, using the "Pay as you go" subscription model. CNSI's AWS cloud hosting platform architecture is flexible to integrate AWS-hosted core claims module with any on-premise or private cloud

platforms. CNSI has successfully integrated AWS and other cloud hosting platforms with on-premise hosting platforms in some other implementations.

Team CNSI's hosting platform leverages AWS cloud bursting technique for effective usage of AWS resources. Leveraging the cloud bursting technique makes CNSI's platform as a cost-effective solution since 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 a monthly job is run that requires additional computing power, 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). In our cloud implementation in Washington, nearly 30% in costs related to hosting were saved by migrating to AWS cloud and leveraging its Cloud Bursting technology.

ENV06

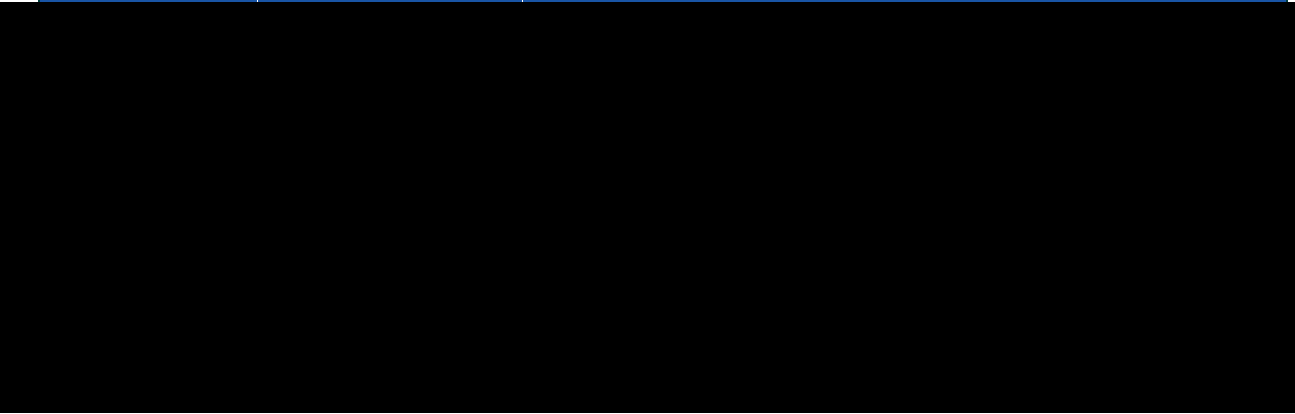
The Contractor shall provide the ability to run multiple sessions /environments/applications/areas/views simultaneously. This includes providing sufficient environments and configurations (e.g., multiple environments, multiple application layers, hub architecture) necessary to perform all required functions (e.g., testing, training, production operations, modeling, disaster recovery).

Team CNSI's evoBrix X CPMS 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 X CPMS 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. [REDACTED]

Category	Sub-category	Value
Category 1	Sub-category 1.1	Value 1.1.1
	Sub-category 1.2	Value 1.2.1
Category 2	Sub-category 2.1	Value 2.1.1
	Sub-category 2.2	Value 2.2.1
	Sub-category 2.3	Value 2.3.1
	Sub-category 2.4	Value 2.4.1
	Sub-category 2.5	Value 2.5.1
	Sub-category 2.6	Value 2.6.1
Category 3	Sub-category 3.1	Value 3.1.1



Every environment in Team CNSI's evoBrix X CPMS 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 3.10.1-53.

Team CNSI's evoBrix X CPMS solution will integrate with the DPHHS' Enterprise Service Bus (ESB) hub, as mandated by DPHHS's security requirements. A handshake is established first with the exchange of certificates between the evoBrix X platform 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 X CPMS solution upon a successful authentication and authorization.

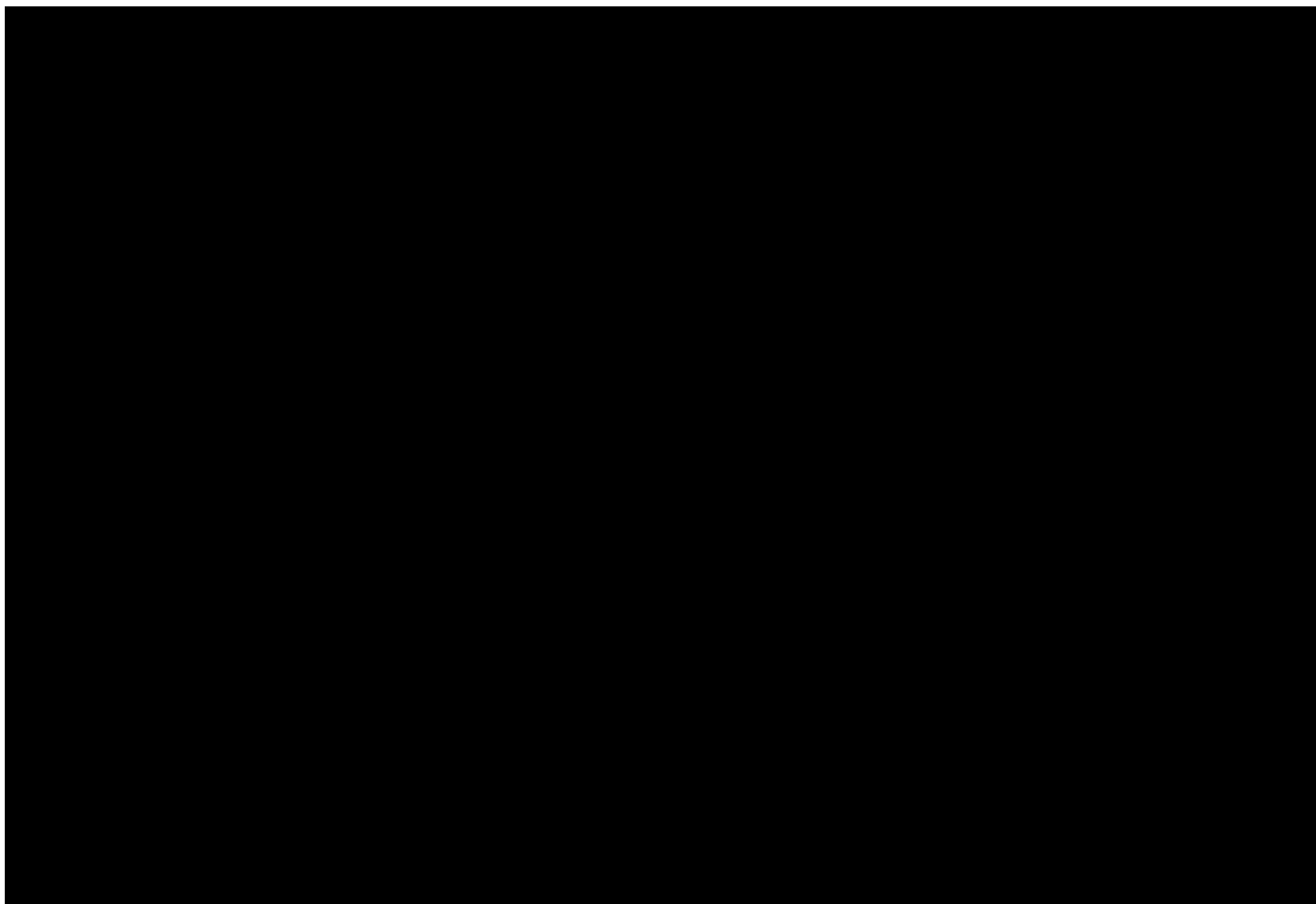


Figure 3.10.1-53. Deployment Topology Diagram. Interaction between different applications and areas present in a logical environment in Team CNSI's evoBrix X CPMS solution.

Category	Sub-category	Item	Value
Category 1	Sub-category 1	Item 1	Value 1
Category 1	Sub-category 1	Item 2	Value 2
Category 1	Sub-category 1	Item 3	Value 3
Category 1	Sub-category 1	Item 4	Value 4
Category 1	Sub-category 1	Item 5	Value 5
Category 1	Sub-category 1	Item 6	Value 6
Category 1	Sub-category 1	Item 7	Value 7
Category 1	Sub-category 1	Item 8	Value 8
Category 1	Sub-category 1	Item 9	Value 9
Category 1	Sub-category 1	Item 10	Value 10
Category 1	Sub-category 1	Item 11	Value 11
Category 1	Sub-category 1	Item 12	Value 12
Category 1	Sub-category 1	Item 13	Value 13
Category 1	Sub-category 1	Item 14	Value 14
Category 1	Sub-category 1	Item 15	Value 15
Category 1	Sub-category 1	Item 16	Value 16
Category 1	Sub-category 1	Item 17	Value 17
Category 1	Sub-category 1	Item 18	Value 18
Category 1	Sub-category 1	Item 19	Value 19
Category 1	Sub-category 1	Item 20	Value 20

Configuration Management – Views and Areas

Team CNSI's robust Software Configuration Management system supports 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 X CPM platform and components to meet the MT CPMS solution implementation and operational needs.

This approach will allow the following for evoBrix X CPMS 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 CPMS 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 X CPMS solution.

Cloud Infrastructure Change Management

This section describes the functions of Change Control Board (CCB) as it relates to the management of Cloud infrastructure changes for the evoBrix X CPMS solution. All Configuration Items (CIs) related to

Cloud infrastructure and Software License Asset Management are identified, documented, and tracked in the Configuration Management Data Base (CMDB). Team CNSI uses Atlassian Insight as the CMDB tool for Hardware and Software Asset Management. Additional details about Insight and Team CNSI's CMDB solution is provided in SEC03 requirement, page 84.

The CCB represents the interests of project management by ensuring that a structured process is used to consider purchases or upgrades or decommission of Cloud infrastructure and supporting the installation of the infrastructure 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 CCB:

- Requests that impact analysis of proposed Cloud infrastructure changes be performed
- Reviews the Cloud infrastructure changes
- Makes decisions regarding Cloud infrastructure
- Monitors progress of the Cloud infrastructure installation
- Communicates decisions made to affected groups and individuals

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.

ENV09

The Contractor's environments (e.g., development, testing, training and production) 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's evoBrix X CPMS solution is highly scalable and supports multiple environments such as Development, System Test, UAT, Regression, Conversion, Training/Outreach, Performance, Disaster Recovery (DR), B2B/Parallel and Production. These environments will be available for users to access it twenty-four (24) hours a day, seven (7) days a week, with the exception of planned downtime due to system upgrades or routine maintenance. Team CNSI will communicate and coordinate all planned downtime and maintenance outages with the Agency and agreed to by the Agency, at least five 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

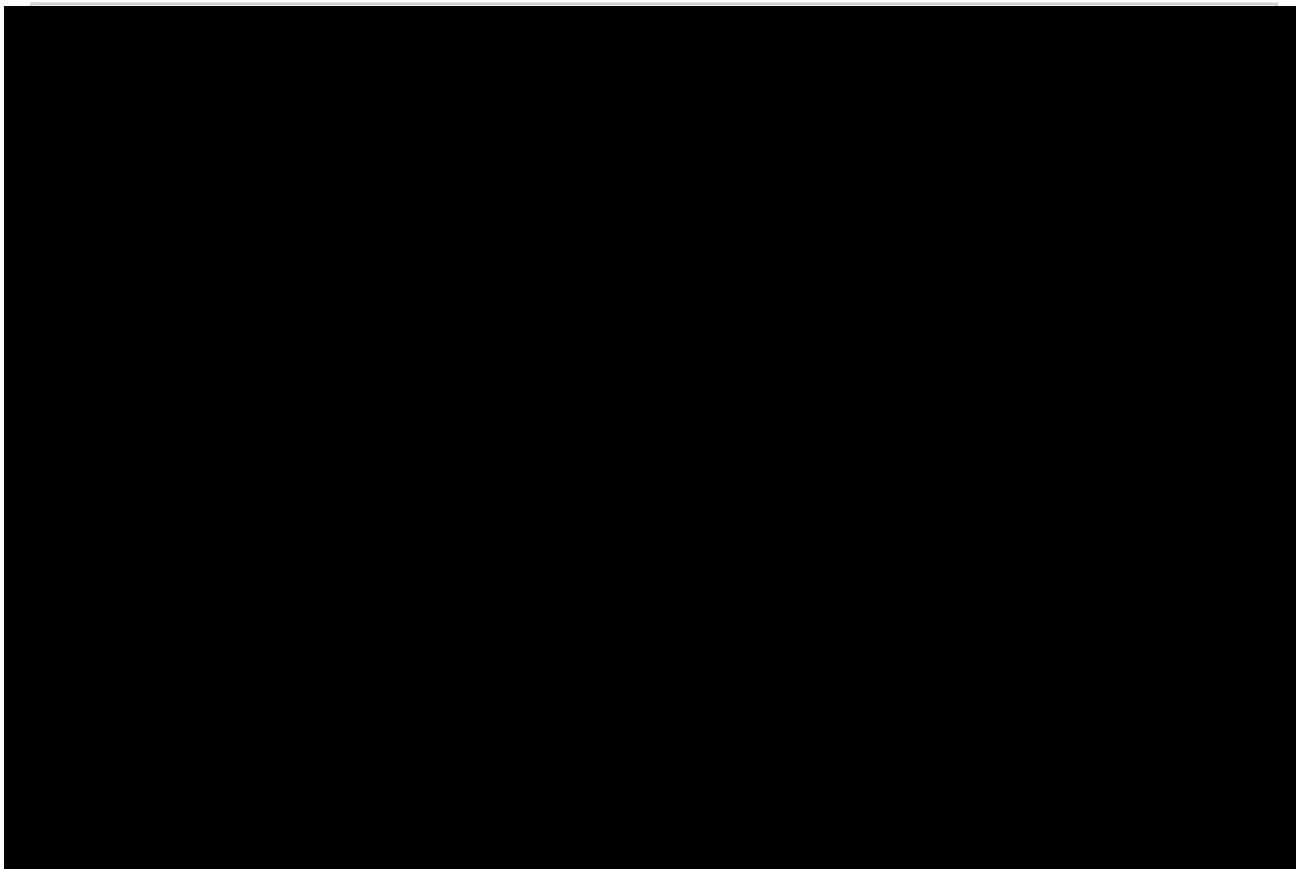
Team CNSI's evoBrix X CPMS solution addresses challenges related to additional volumes and new programs anticipated for the future, as well as issues related to performance, maintenance, and

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. In our current similar implementation in WA ProviderOne and CMS EDPS CNSI has successfully maintaining system availability of 99.9%.

Team CNSI's high-availability architecture includes:

- AWS Cloud server with high available AWS robust architecture
- Application server cluster with load balancing
- Web server load balancing
- 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 3.10.1-55 depicts the high-level availability architecture covering clustering at the application server and database server level as well as web server load balancing.



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 3.10.1-56 contains a list of components that provide redundancy and scalability needed to support the system 24x7x365.

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 Database Backups and Data Guard Replication ensures high availability for databases

Figure 3.10.1-56. 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.

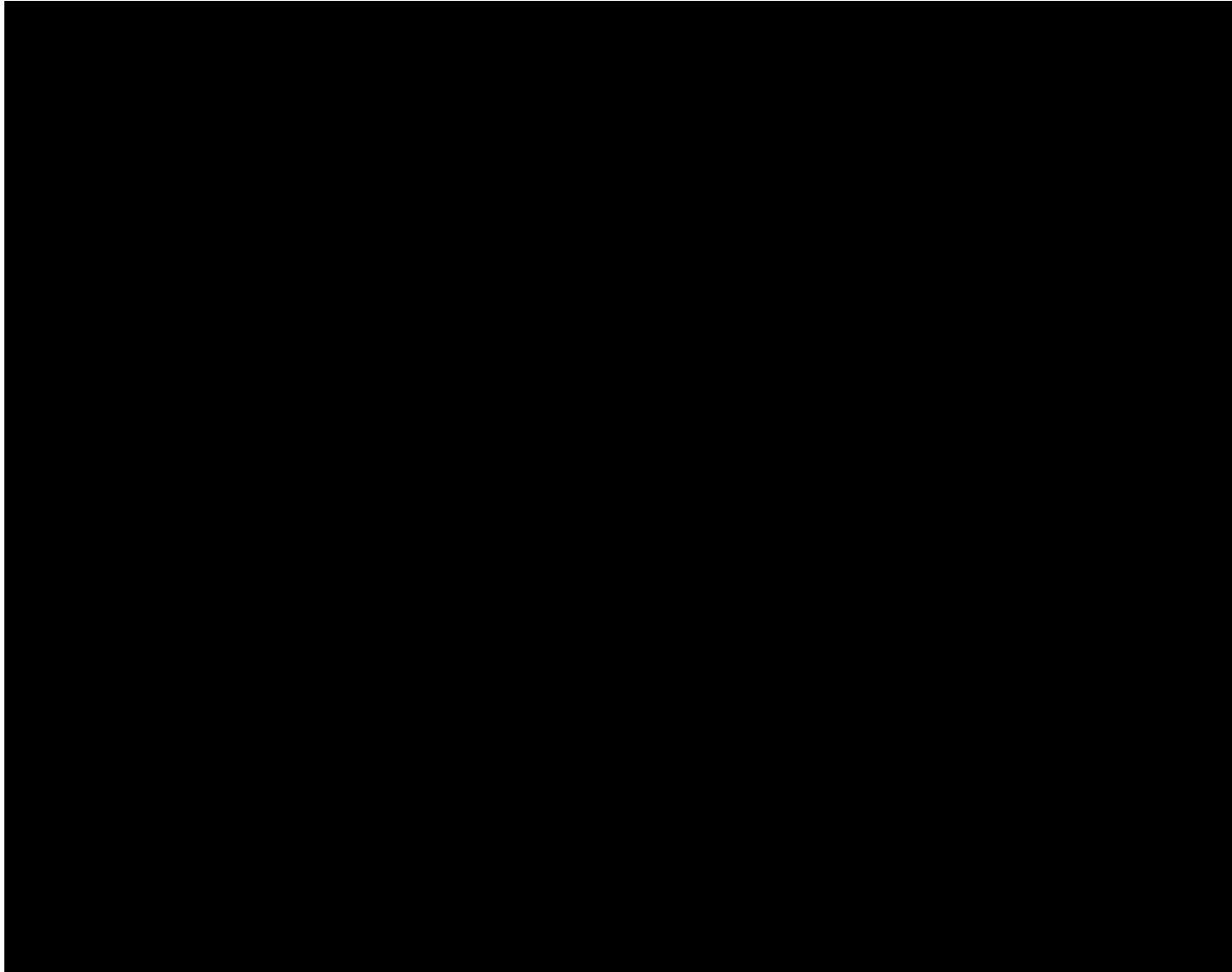
Unscheduled Maintenance

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 X CPMS 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, and AWS Infrastructure Management portal and AWS Cloudwatch and AWS Cloudtrail 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.



[REDACTED]

[REDACTED]

[REDACTED]

ENV10

The Contractor shall provide hosting services that shall meet all functional and non-functional requirements defined in the RFP.

Team CNSI's hosting solution meets all State requirements outlined in Attachment F and other sections of the RFP.

[REDACTED]

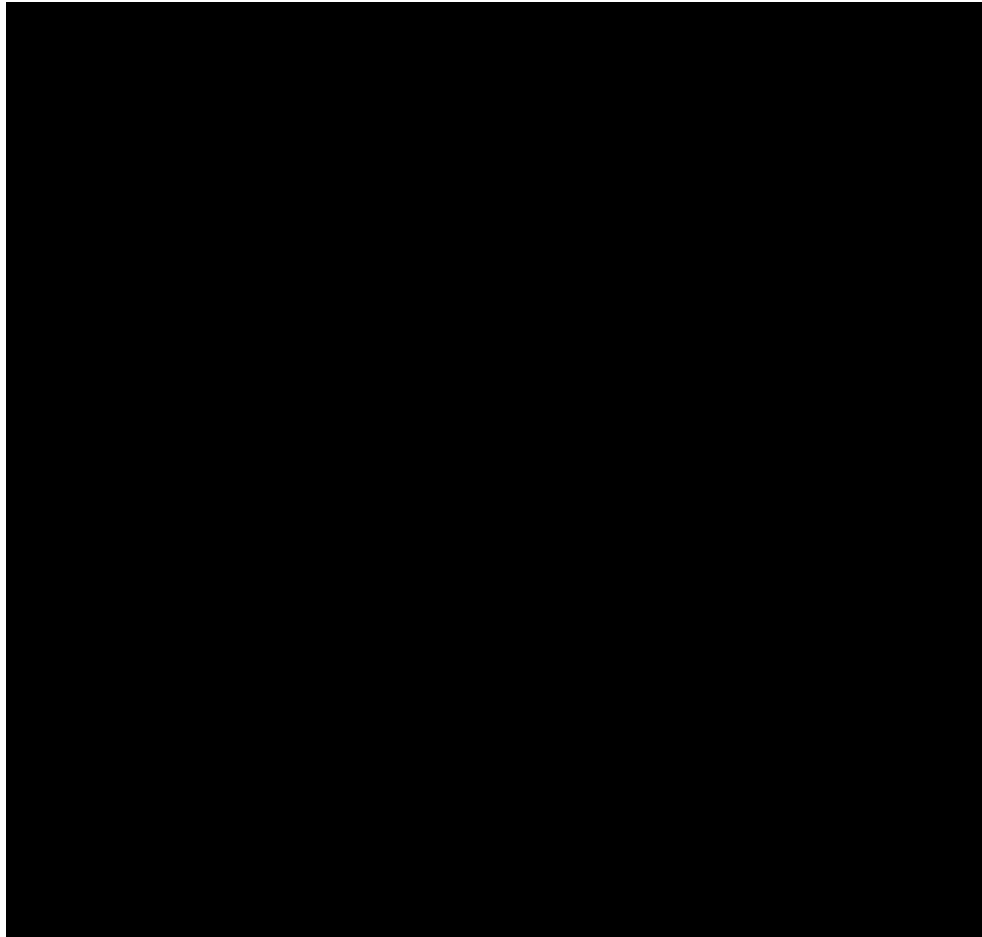


Figure 3.10.1-60. Hosting Platform Topology. Team CNSI uses high efficiency, highly redundant and effective plans while building the servers from firewalls to SAN.

Managed Services and Key Features of Hosting Platform

Team CNSI's evoBrix X CPMS solution includes managed services at the data center level covering security services, data services, network services, and infrastructure services. 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 3.10.1-61 provides an overview of the various PaaS, IaaS, encryption and security services that form the building blocks of Team CNSI's evoBrix X CPMS 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.

This data centers utilize a robust and redundant infrastructure architecture to provide maximum uptime for critical data, applications, and technologies. Access to Team CNSI's cloud infrastructure is tightly controlled and it is strictly limited to AWS 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.

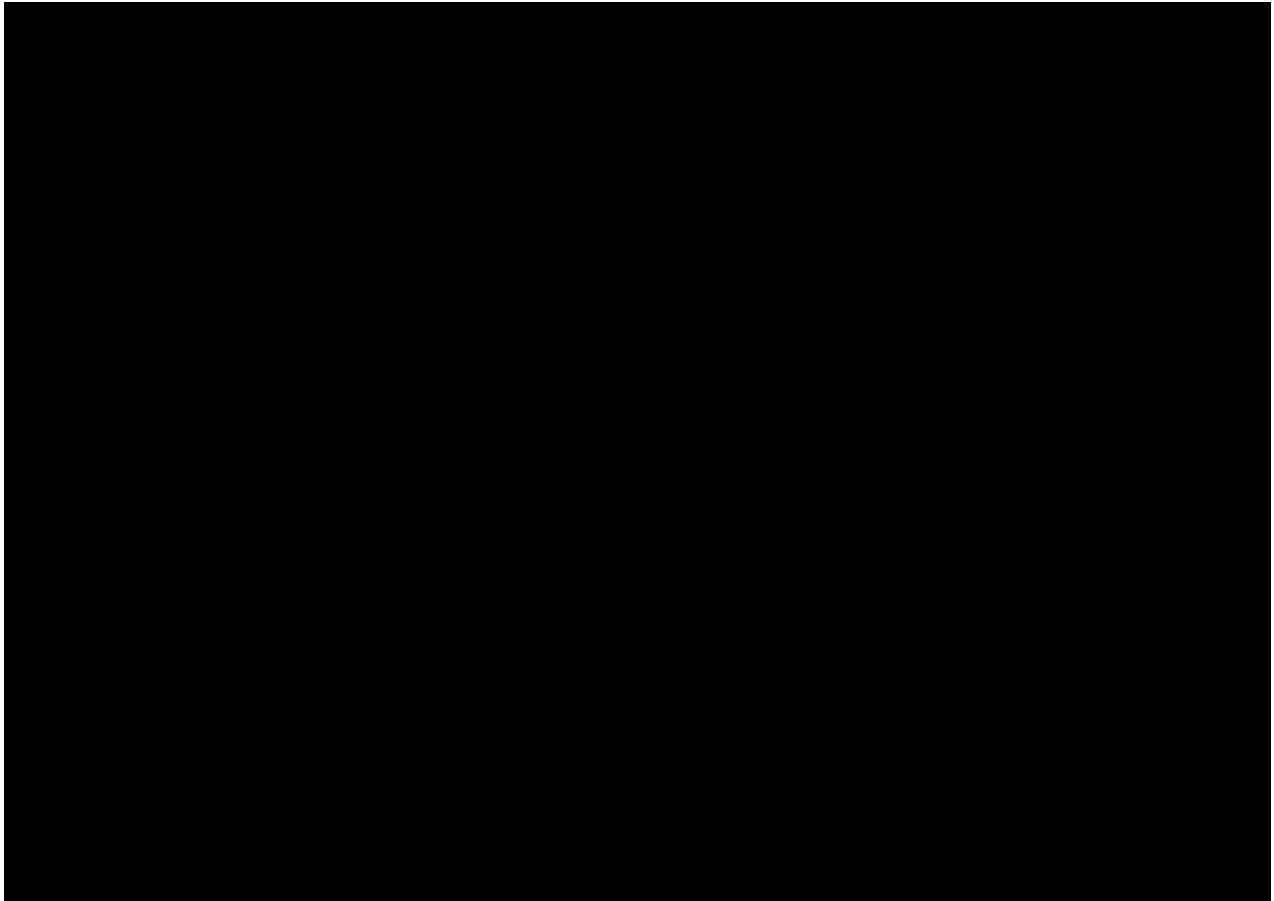
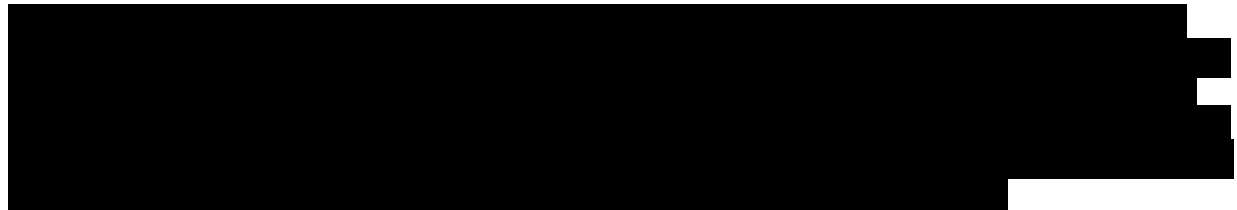


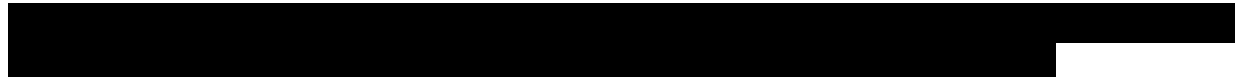
Figure 3.10.1-61. Building Blocks. evoBrix X uses PaaS, IaaS, encryption and security services that form the building blocks.

ENV11

The Contractor shall identify the physical location(s) where the Contractor's solution is installed and operating. In the event the Contractor is utilizing a SaaS or PaaS-based service the Contractor shall provide the State with sufficient identifying characteristics of the physical location(s) and allow the State to independently verify the security of said location(s). To the extent possible, the State must have transparent access to this location(s)..

Team CNSI's evoBrix X CPMS solution is hosted in AWS's FedRAMP and HIPAA compliant public cloud. This hosting platform has all the cloud features built in to support any future expansion based on workloads.





Team CNSI has provided detailed design and architectural details of the hosting solution in response to requirements ENV06 (pages 154 to 158), ENV09 (pages 158 to 162) and ENV10 (pages 163 to 165).

3.10.1.4 Integration

This section addresses integration requirements. The Claims Processing and Management Services solution will be required to integrate with the MPATH Integration Platform. The MPATH Integration Platform, administered by the Systems Integration Services Contractor, will enable interactions between MPATH modules via MPATH Integration Platform enterprise messaging services, bidirectional interfaces, data imports and data exports. The Claims Processing and Management Services Solution Contractor must ensure all service endpoints/APIs are clearly defined, exposed to the MPATH Integration Platform and be able to receive and submit messages through the MPATH Integration Platform to facilitate standardized data exchanges. The Offeror must describe their approach in detail to meet each of the integration requirements in Attachment F – Requirements Response Matrix. The Contractor's solution shall include all integrations/interfaces listed in Attachment F - Requirements Response Matrix in their overall fixed price. The Offeror simply repeating the RFP requirements does not qualify as a good response as defined in Section 6.1.1 of this RFP.

3.10.1.4.1 Integration Service Type Definition

Integration Service Type definitions are critical to defining the various types of integrations that the Claims Processing and Management Services Contractor will be required to perform throughout the life of the Contract. These integration service type definitions will also serve as the basis for the fixed hour amounts that the Department will require each Offeror to provide for each Integration Service Type definition (see Attachment G – Pricing Schedules, Schedule J – Integration Service Types).

The Department has outlined five discrete Integration Service Types below, to describe the distinct types/levels of integration services required to support module integration. The Contractor will use the Integration Service Type definitions below to provide a fixed number of hours (i.e. level of effort) for each Integration Service Type. For each unique integration service required to support MPATH integration needs (e.g., the integration of a module, Montana Healthcare Enterprise component, or outside entities) the Department and the Contractor will mutually agree on the appropriate Integration Service Type category for each unique integration service request. The Department will require the Contractor to identify the hour breakdown for each Integration Service Type by resource type necessary to implement services in Attachment G – Pricing Schedules.

The following sections define each integration service type.

3.10.1.4.1.1 Major Integration Service

A major integration service involves some combination of significant data transformation/translation development, complex orchestration, frequent communications, high number of business process steps, significant performance requirements, multiple shared data stores, extensive data transformation conformance requirements, or significant failure handling requirements.

3.10.1.4.1.2 Complex Integration Service

A complex integration service involves some combination of simple data transformation/translation development or difficult transformations, detailed orchestration, frequent communications, a moderately high number of business process steps, significant performance requirements, multiple shared data stores, technical conformance requirements, or significant failure handling requirements.

3.10.1.4.1.3 Standard Integration Service

A standard integration service involves some combination of moderate transformation development, simple orchestration, regular interval communications, a moderate number of business process steps, performance requirements, several shared data stores, well defined and supported technical conformance requirements, or limited failure handling requirements.

3.10.1.4.1.4 Simple Integration Service

A simple integration service involves some combination of simple transformation development, simple orchestration, infrequent communications, a small number of business process steps, straight forward performance requirements, few shared data stores, well defined and supported technical conformance requirements, or limited failure handling requirements.

3.10.1.4.1.5 Onboarding Integration Service

An onboarding integration service involves the setup of a connection of a new system, component, or module including the setup/coordination (e.g., security settings, interface testing, training) to an existing claims module integration/interface. Reuses existing integration/interface without the need for any changes to the interfaces themselves such as the creation of any additional adaptors, changes to the data format, changes to transmission

method, etc. in order to set up the integration/interface with the new system. Outside of planning, configuration, testing and training, no labor is required for modifications to the existing interface being reused.

3.10.1.4.2 Integration Service Dimensions and Scoring

To determine the appropriate integration service type of a particular interface, the following table provides nine complexity dimensions (see Table 3.10.1.4.2.1 Integration Service Dimension and Scoring). For each dimension, a score of “low,” “medium,” or “high” will be determined based on the description of the dimension. Each score has a point allocation, which will be added together to determine the appropriate integration service type category using scoring ranges in Table 3.10.1.4.2.2 Integration Complexity Definition and Scoring Ranges.

Table 3.10.1.4.2.1 Integration Service Dimension and Scoring

Interface Complexity Dimensions		Low (score=1)	Medium (score=5)	High (score=10)	Example Scoring
Data Transformation	Provide a score related to the volume of and complexity of data transformations and translations that will be required to support the interface. The module's internal representation of data may be different from the exact formats required to implement the interface.	None or minimal. Data stored by the module closely resembles the data formats exchanged by the service.	Moderate. Data stored by the module differs from the data formats exchanged by the interface for multiple, but not all, data elements or data properties.	Extensive. Data stored by the module significantly differs from the data formats exchanged by the interface. Specifically, data schemas, relations, structures and entities do not resemble interface formats and necessitate significant additional implementation effort to support the interface.	1
Orchestration	Provide a score related to the volume of and complexity of service orchestration that will be required to support the interface. Service orchestration is the process of integrating two or more services and/or applications together to provide a response or to synchronize data in real-time. Additionally, the service may need to be part of a broader enterprise-wide orchestration of services, necessitating additional design and testing	None or minimal. Simple point-to-point internal integration for the interface, no complex orchestration.	Moderate Some orchestration dependencies exist and need to be accounted for and implemented by the module vendor for this interface. (2-5 orchestration related sub-processes).	Extensive Extensive orchestration dependencies exist and need to be accounted for and implemented by the module vendor for this interface. (5+ orchestration related sub-processes).	1

Interface Complexity Dimensions		Low (score=1)	Medium (score=5)	High (score=10)	Example Scoring
	coordination with multiple parties.				
Frequency	Provide a score for the expected frequency for which the interface will be invoked/used.	Frequency is on the order of monthly, weekly or once or a few times daily.	Frequency is once or more hourly.	Frequency is multiple times per minute, per second or even more frequent.	1
Business Process Logic	Provide a score related to the volume of and complexity of business process logic steps that will need to be implemented to support the interface. The interface may need to implement a complex set business logic before providing a response or while processing incoming data. Additionally, a higher level of effort to support automated testing and production of synthetic testing data may be required.	Basic. A minor volume of business process steps or logic involved. Business logic is simple (e.g. basic search or look up).	Moderate to High. A moderate to high volume of business process steps or logic involved, but the logic is primarily ordered step-by-step with only a few branches in logic or conditional directions (e.g., a claim posts an edit that identifies TPL on the claim that doesn't exist on the member's record; therefore, a work item is sent to the TPL component to perform insurance verification).	Extensive and complex. This interface encapsulates and requires implementation of an extensive volume of complex business logic. Logic for the business processes has multiple steps, multiple conditional/decision pathways, dynamic input conditions, rollback conditions, numerous possible result outputs/actions, etc. (e.g. claim submission flow is a complex process with many steps and sub-processes that may require interactions between modules and the IP or other modules).	1

Interface Complexity Dimensions		Low (score=1)	Medium (score=5)	High (score=10)	Example Scoring
Performance Requirements	Provide a score associated to enhanced performance requirements for the interface. The interface may need to perform in real-time with specified response time limits.	None or minimal. Asynchronous batch processes.	Moderate. Synchronous interfaces without significant response time constraints (e.g. delayed response or retry attempts not noticeable to the end user).	Extensive. Synchronous interfaces with strict response time constraints (e.g. items that are impacting the UI response time / performance).	1
Number of Data Sources Involved	Provide a score for an increased number of disparate data sources that the interface will need to interact with. The interface may need to retrieve or update data from/to multiple internal module sources and from/to external systems before providing a response or when processing incoming data.	Only the module's internal data store(s) will be utilized by the implemented service.	The module will need to synchronize (update, retrieve) data with the Agency's Operational Data Store in order to implement the interface.	The module will need to synchronize (update, retrieve, send notification) data directly with other modules' data stores in order to implement the interface.	1
Size of Data	Provide a score for the expected size of data, on average, that the interface will transmit or receive.	Low to no payload data transmitted via this interface, size within ~KB range.	Medium amount of payload data transmitted via this interface, size within ~MB range.	Large amount payload data transmitted via this interface, size approaching 1GB and larger.	10
Existing Data Standards	Provide a score that describes whether or not the interface will utilize standardize formats and code list values. Specifically, grade how loosely that standard may be followed by all Parties in regards to any additional anticipated level of coordination and agreement required for implementation.	Technical standards exist and are implemented uniformly by vendors. Minimal to no coordination is needed between the module vendor and the rest of the enterprise parties to agree on technical and data specifications for the interface.	Technical standards exist, but may not be implemented uniformly. Some degree of coordination between the module vendor and other enterprise parties is needed to agree on technical and data specifications for the interface.	No technical or data standards available. A high degree of planning and coordination is needed to identify, design and agree on technical and data specifications for the interface.	10

Interface Complexity Dimensions		Low (score=1)	Medium (score=5)	High (score=10)	Example Scoring
Failure Handling	Provide a score related to the volume of and complexity of failure handling processes and procedures that will be required to implement the interface. Upon a failure, the interface may require rollback of predecessor actions and data changes or may trigger specific notification procedures.	Minimal to no steps are needed to be undertaken by the module in the event of an error or failure (e.g. retry, etc.).	Some steps need to be undertaken by the module in the event of an error or failure (e.g. retry and send failure notifications).	Significant steps need to be undertaken by the module in the event of an error or failure (e.g. unrolling dependent actions, restoring the prior database state, etc.).	10
Total Score					36
Interface Complexity Rating					Complex

The definitions of each interface service type are listed below with its respective scoring.

Table 3.10.1.4.2.2 Integration Complexity Definition and Scoring Ranges

Interface Complexity Definitions		Score Range
Major	Involves some combination of significant data transformation/translation development, complex orchestration, frequent communications, high number of business process steps, significant performance requirements, multiple shared data stores, extensive data transformation conformance requirements, or significant failure handling requirements.	"60 - 90"
Complex	Involves some combination of simple data transformation/translation development or difficult transformations, detailed orchestration, frequent communications, a moderately high number of business process steps, significant performance requirements, multiple shared data stores, technical conformance requirements, or significant failure handling requirements.	"33 - 59"
Standard	Involves some combination of moderate transformation development, simple orchestration, regular interval communications, a moderate number of business process steps, performance requirements, several shared data stores, well defined and supported technical conformance requirements, or limited failure handling requirements.	"18 - 32"

Simple	Involves some combination of simple transformation development, simple orchestration, infrequent communications, a small number of business process steps, straight forward performance requirements, few shared data stores, well defined and supported technical conformance requirements, or limited failure handling requirements.	"9 - 17"
---------------	--	-----------------

Examples of each integration service type are found in Attachment O – Integration Service Type Examples.

3.10.1.4.3 DDI Requisitioned Integration Services Pool

The DDI Requisitioned Integration Services Pool is a bucket of hours to be used during the Project's DDI phase to provide integration services to support the exchange of data between modules that is beyond integrations required within the Scope of Work and/or those proposed to be provided by the Offeror in their response. The Offeror shall include all integrations/interfaces listed in Attachment F - Requirements Matrix in their base solution cost. Also, the Offeror shall include the interfaces listed in Attachment L - Technology Matrix Tab L-2, where columns K, L, M and/or N are "Yes" in their base solution and cost. Any interface required by a Participating State that is not explicitly described in Attachment F - Requirements Matrix or that is listed in Attachment L - Technology Matrix Tab L-2 where columns K, L, M, and N are "No" will be implemented using the DDI requisitioned pool hours.

The Offeror will be required to propose a fixed dollar estimate for the hours in the DDI Requisitioned Integration Services Pool in Attachment G – Pricing Schedules.

The DDI Requisitioned Integration Services Pool will provide the Department the hour equivalent of 5 Major Integration Services, 15 Complex Integration Services, 25 Standard integration Services, 35 Simple Integration Services, 10 Onboarding Integration Services. The actual number of integration services to be provided by the DDI Requisitioned Integration Services Pool will be dependent on the composition of integration services and the mutually agreed upon category designation (defined in Sections 3.10.1.4.1.1 through 3.10.1.4.1.5), for each required service integration. The actual composition of services required from the DDI Requisitioned Integration Services Pool will be based on what is required to integrate the actual modules and will likely differ from the predefined Integration Services Type quantities used to establish the pool (e.g., based on the total hours available in the pool, the eventual composition of integrated services may be 7 Major Integration Services, 20 Complex Integration Services, 27 Standard Integration Services, 30 Simple Integration Services and 16 Onboarding Integration Services).

The Claims Processing and Management Services Contractor will develop an interface control document (ICD) for each integration, including base integrations and those that are implemented through the DDI Requisitioned Integration Service Pool. The Department and the Contractor must mutually agree upon the Integration Services Type using an Integration Service Type form. The Integration Service Type form template can be found in the Procurement Library. Development work can begin following the Department's approval of the ICD. Each integration service, once approved for implementation by the Department, will be a deliverable during the DDI phase. Upon delivery and Department acceptance of each unique integration service, the Contractor will be reimbursed the Integration Service category hours for the service at the DDI Requisitioned Integration Services Pool Average Hourly Rate defined in Attachment G – Pricing Schedules, Schedule K – DDI Requisitioned Integration Services Pool Hours and Cost.

The Contractor will not be guaranteed to be paid the DDI Requisitioned Integration Services Pool cost. The Contractor will only be paid for the hours related to completed and approved integration service. If upon completion of the DDI phase, DDI Requisitioned Integration Services Pool hours remain, at the Department's discretion, all unused DDI Requisitioned Integration Services Pool hours and cost for DDI will:

- be rolled over to the System Enhancement Pool for Operations; or
- be reduced from the Contract along with the unused dollars.

Section 5, Cost Proposal, details how the Integration Service Types will be used to develop Attachment G – Pricing Schedules, Schedule K – DDI Requisitioned Integration Services Pool Hours and Cost.

A range of mission-critical technical and business factors drive DPHHS’ focus on implementing the transition toward a more fully integrated MPATH information system platform. Team CNSI’s evoBrix X Integration Gateway architecture provides support to achieve the MPATH Modularity Business Objectives “An enterprise system than integrates data from disparate systems to enable enterprise wide program management” and Guiding Principles “Data Integration and Interoperability” mentioned in the MPATH Claims Processing and Management Services Module RFP document. Our evoBrix X Integration Gateway including an API Gateway and a File/EDI Gateway is built upon a Service Oriented Architecture (SOA)-based architecture in alignment with Medicaid Information Technology Architecture (MITA) principles. For DPHHS, our solution provides inherent flexibility for effective integration with other systems. It includes built-in features to promote interoperability, reuse of functionality and ease of maintenance.

The Team CNSI Advantage

Team CNSI's evoBrix X CPMS solution offers inherent flexibility for ease-of-integration within MPATH's multi-system platform.

- Open technologies (SOAP, REST, Swagger) and Open APIs facilitate MPATH integration requirements
- Our solution's modular system supports State's integration objectives
- Built-in Integration Gateway features
- Demonstrated success in other states (e.g., MI, WA) implementing interface with an Integration Platform designed to facilitate standardized data exchanges

evoBrix X Integration Gateway provides the capability to easily integrate with the MPATH Integration Platform to interoperate with all other MPATH modules. We provide the following components and services to support integration services:

evoBrix X Integration Gateway components

- **File/EDI Gateway** – This component leverages the Oracle SOA MFT to securely receive and send the files to the external systems. This architecture helps us to integrate seamlessly with the MPATH system integrator to enable the loose coupling.
- **API Gateway** – This component leverages the industry leading Oracle SOA tool for producing and consuming the real time webservices with the external systems. This allows for easy integration with the MPATH Integration Platform.

Technical Components

- **Interface Service Repository (ISR)** – This component 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 evoBrix X ISR solution supports scheduling, audit, error logging, and escalation features. The solution also supports detailed reporting on interface execution status, combined with notification modules to track execution of the various interface transactions thus ensuring processing of interfaces within timeframes.
- **EDI Translator and Validator** – This component uses Edifecs to validate and translate all the EDI transactions to ensure all the HIPPA files adhere to the standards.
- **Technical Services - Web Service Framework** – This component support SOAP or REST as a protocol for producing or consuming webservices for the external agencies. In addition, the framework leverages industry standard Apache CXF libraries. The API specification for SOAP services follows the WSDL (Web-Services Definition Language) standards. The REST Open API specification is also called Swagger Specification.

Business Services

Team CNSI brings demonstrated expertise from other similar programs in the 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, 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, reinforces the Medicaid Enterprise commitment to the Seven Standards and Conditions, and supports the technical evolution of SMAs.

- **Pre-existing web services** – Our evoBrix X solution is comprised of a rich portfolio of production-ready, real time services that are optimized for the Medicaid environment. These services 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 supporting Applications APIs (COTS – Commercial Off the Shelf).
- 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.
- Commercial application APIs expose application functionality as internal and external interfaces through standard APIs. Examples include Document Management API, Workflow API and Correspondence 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.

For 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, page 79.



INT01

The Contractor's solution shall have the ability to identify errors in member information and member eligibility transactions and immediately notify the source system of the specific errors including whether the errors have precluded loading and/or using the data.

The evoBrix X CPMS solution requires Member information from the member system for processing the claims. Without accurate member information, the claims cannot be processed correctly. Our solution utilizes the Integration Gateway to integrate with the MPATH Integration Platform to exchange data with the other systems of the MPATH environment. The ISR component will process the member files and validate them against the file format which has been developed and accepted by both Team CNSI and the MPATH member system vendor. Based on the error code and error description defined as part of the design, the ISR component will generate the error and can send the notifications to the source system

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.

The evoBrix X CPMS solution stores the geographic indicators as part of the data collected through claim submission as well as the provider and member data collected from the MPATH modules. The evoBrix X Reporting solution comes with an extensible reporting model comprising of a standard structured set of data elements to accommodate a wide array of geographic indicators such as by state, city, county, geographic regions, zip code, and zip extension that shall support retrieval and reporting of data. The model can be leveraged to configure scheduled or on-demand reports and provide enhanced self-service user experience through ad-hoc reports for the reporting of geographic indicators according to agency requirements.

Additionally, the evoBrix X Reporting solution supports the creation of peer groups by provider classification, member demographic segmentation, service types, and other functional clusters / groups to augment the presentation of data in conjunction with the standard geographic indicators.

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. As part of our Phase 1 Planning processes, Team CNSI will coordinate with DPHHS and the MPATH System Integrator to identify all relevant stakeholders, including other enterprise module vendors, to develop an approach to support system availability. This approach will include methods for coordination among all entities to proactively identify, diagnose, develop work arounds, and resolve system availability issues. 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

INT35

The Contractor shall provide an architecture that has clearly defined service endpoints.

Team CNSI’s API Gateway 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 X solution relies on open standards and standard APIs, such as the Java Business Integration (JBI) standard, for pluggability of third-party communities. The evoBrix X 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 X 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 protocols. Also, evoBrix X can change the various attributes of the service without impacting existing clients. Our OSB component part of evoBrix X Integration Gateway will allow Core MMIS to avoid point-to-point communication between different system components and will streamline flow of all information throughout the MT Core Claims 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.

The IV&V Contractor plays an important role in supplying status and evaluation information to CMS in order to achieve Certification for the MT CPMS 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 Core Claims 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 Core Claims-related MITA mapping. Our Certification Lead, Ms. Katie DeLorensi, will form a collaborative partnership with the IV&V Contractor to establish the Certification Plan for MT CPMS.

INT52

The Contractor shall collaborate with all State enterprise contractors and solutions to accurately collect, process, and distribute applicable HIPAA EDI transactions.

HIPAA EDI transactions play a very important role in the evoBrix X CPMS without the EDI transaction the claims processing and the communication to providers on the errors, claims outcome will be interrupted. evoBrix X solution utilizes the Integration Gateway to integrate with agencies System Integrator to receive the files from the agencies member system. The EDI Translator and Validator

component will process the EDI transactions and validate the core rules and format of the collected files and the EDI transactions generated by the evoBrix X MT CPMS solution that need to be distributed.

INT54

The Contractor's solution shall require (when appropriate), capture, and maintain the 10-digit NPI.

Team CNSI's evoBrix X CPMS solution requires Provider data for processing the claims and assumes that data will be exchanged through the MPATH Integration Platform. Team CNSI will work with the MPATH System Integrator (Deloitte) and the State's provider system vendor (OptumInsight) to define the file format and frequency which is required to receive the provider information. By utilizing the evoBrix X ISR component, the file will be scheduled, processed and loaded to the evoBrix X repository. NPI received along with the provider data will be stored and utilized by our evoBrix X CPMS solution for processing the claims.

INT55

The Contractor's solution shall accept the NPI in all applicable standard electronic transactions mandated under HIPAA.

The evoBrix X CPMS solution stores NPI (billing, rendering, referring, prescribing providers) information received from DPHHS'S provider system as part of the scheduled interface. The same will be leveraged to validate the information submitted via HIPAA transactions.

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.

Establishing and managing consistency of hardware, software and communication components across all the State staff computers is critical 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.

INT61

The Contractor's solution shall allow internal and external stakeholders to upload and view electronically submitted documents.

The evoBrix X CPMS solution offers State 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.

Business user can upload documentation as part of the claim’s submission. When the user(s) invoke the upload functionality, the evoBrix X CPMS solution 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 (page 305) for further details about the Document Management capabilities of the solution.

Any uploaded documents can later be viewed through Core Claims business user 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 3.10.1-62.



Figure 3.10.1-62. 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.

The evoBrix X 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 X and act upon the task. Figure 3.10.1-63 shows a screen shot within the evoBrix X CPMS solution providing event notifications. The framework ensures that all information and event notifications include aggregated and integrated information and are consistent across evoBrix X CPMS solution.

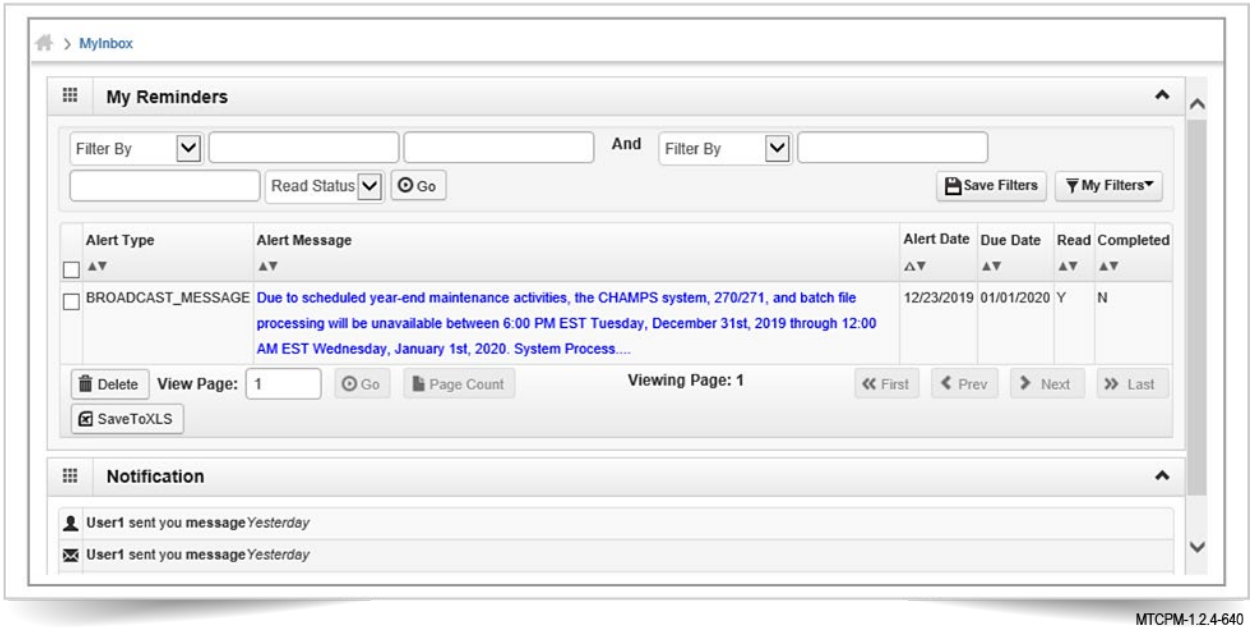


Figure 3.10.1-63. evoBrix X My InBox Screen. evoBrix X Notification framework ensures that information and event notification are consistent across the system.

INT63

The Contractor's solution shall have business process orchestration in an event-driven environment that maximizes process automation.

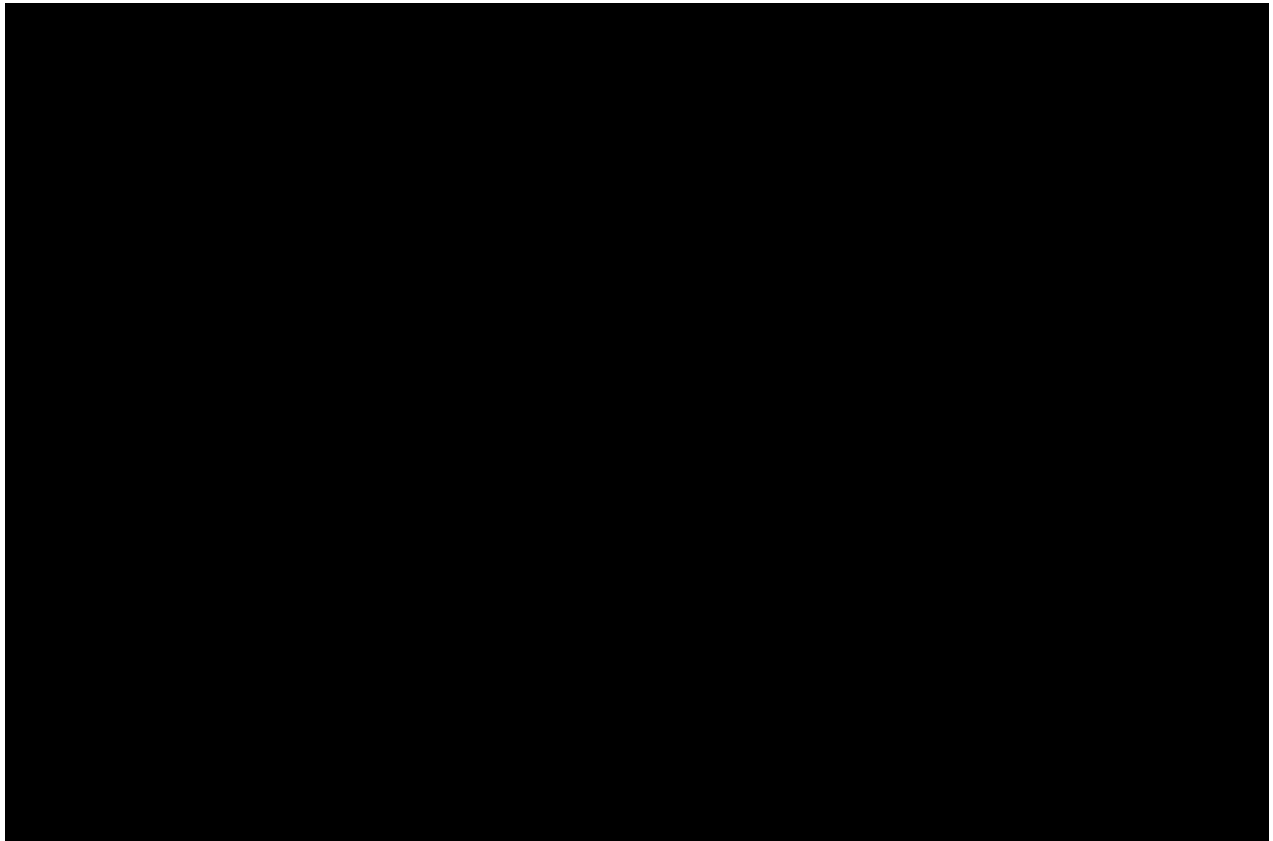
Team CNSI's evoBrix X CPMS solution includes a configurable workflow process that provides the flexibility to define State-specific business processes. The integrated workflow management solution provides improved automation, reduced manual intervention, configurable work routing, and task management. 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 3.10.1.10 Workflow, Page 315 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.



Team CNSI's ISR framework is illustrated in Figure 3.10.1-64.



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 Team CNSI Integration Gateway is built to support exchange of X12, NIEM and NCPDP D.0 transactions. X12 and EDI transactions plays a major role in core claims processing and for the same reason the system is architected with interoperable integration gateway which allows to seamlessly integrate with the agencies systems to receive/send the EDI files.

Team CNSI's evoBrix X CPMS solution is HIPAA/HITECH and ASC X12 5010 compliant that has previously been certified by CMS in Michigan and Washington where it has been serving the Medicaid population for over a decade.

Figure 3.1.10-65 provides some statistics of transaction volumes this framework is supporting in Michigan.

Transaction Name	Processing Mode	Transaction/Day
270/271	RealTime	480,000
270/271	Batch	100,000
837	EDI	200,000
NCPDP Post Adjudicated claims	EDI	150,000

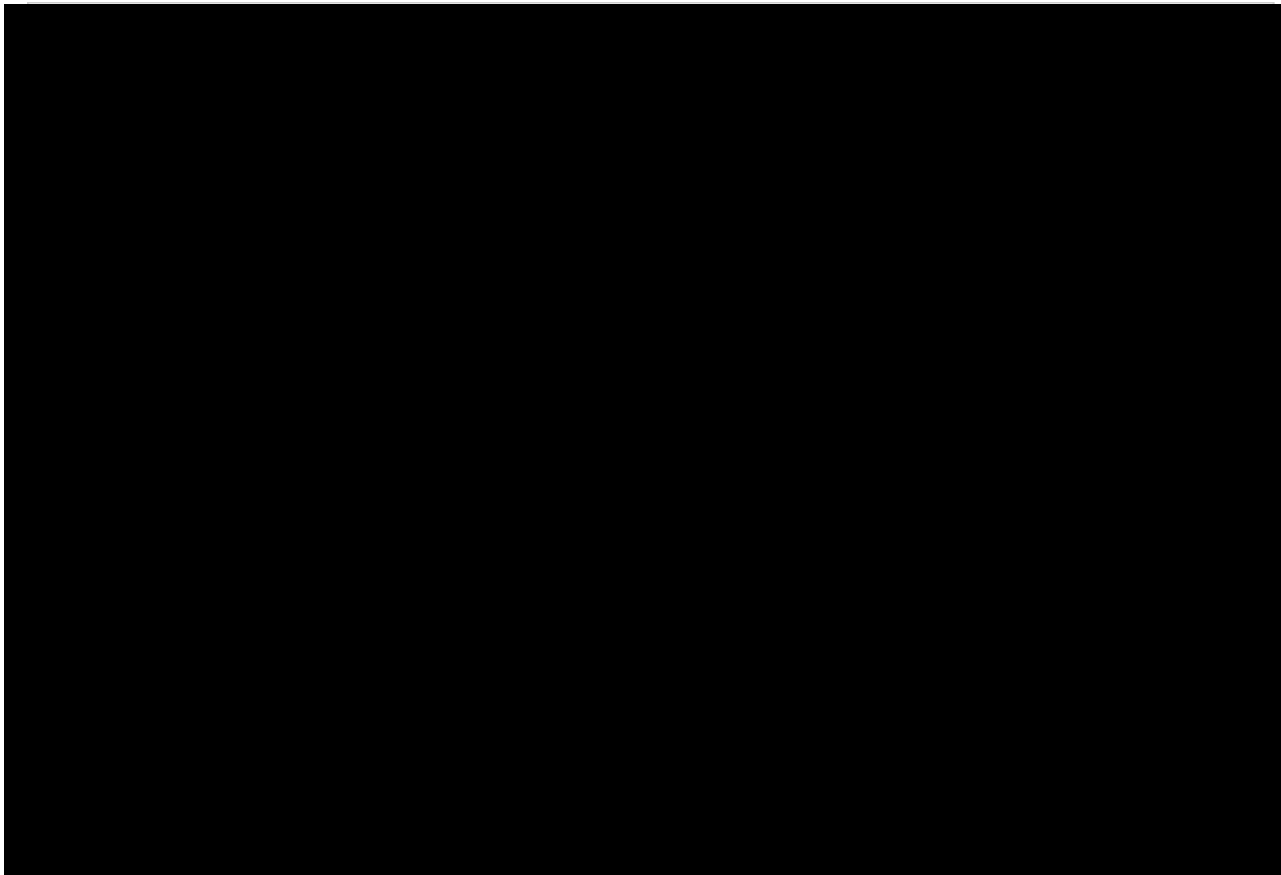
Figure 3.1.10-65. Transaction Statistics. Team CNSI evoBrix X CPMS X 12 transaction framework has been successfully processing EDI transactions in both Michigan and Washington for over a decade.

Team CNSI has extensive experience 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.

- 270 – Eligibility, Coverage, or Benefit Inquiry
- 271 – Eligibility, Coverage, or Benefit Information
- 276 – Electronic Claim Submission System Request
- 277 – Electronic Claim Submission System Response
- 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
- 834 – Benefit enrollment and maintenance
- 820 – Premium Payments
- 997 - Functional Acknowledgment
- 824 - Application Reporting
- 277U- Health Care Claim Status Notification - Health Care Payer Unsolicited Claim Status



evoBrix X CPMS has a modular EDI framework that has the capability to process EDI transactions through various modes of submission in both real time and batch. Team CNSI has experience integrating this EDI framework with state-specific gateways as well as implementing the EDI gateway and will leverage this experience to implement an EDI Gateway for providers in DPHHS. Figure 3.10.1-67 shows evoBrix X CPMS EDI conceptual architecture and how Trading Partners can interact with the system.



The solution accepts HIPAA transactions using EDI Gateway, Council for Affordable Quality Healthcare (CAQH) CORE Phase III compliant API Gateway and using the EDI File Upload feature from evoBrix X CPMS screens from established trading partners. The evoBrix X CPMS EDI Services has a proven track record of processing NCPDP transactions for over decade in the States of Michigan and Washington. Figure 3.10.1-68 depicts the flow of both NCPDP transactions through various stages.

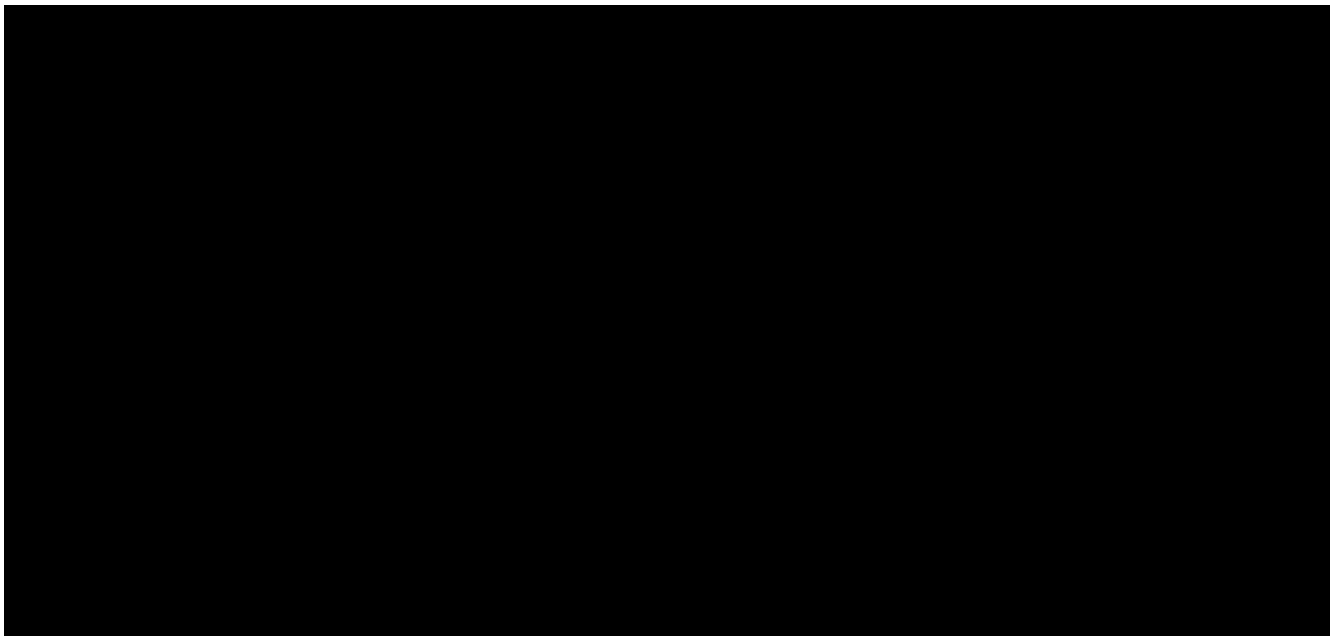


Figure 3.10.1-68. evoBrix X CPMS NCPDP Conceptual Architecture. evoBrix X CPMS uses distributed system architecture, which enables evoBrix to seamlessly integrate with external systems

NCPDP D.0 format files received through EDI Gateway and validated against NCPDP guidelines during validation and a report will be generated with appropriate acknowledgments. The acknowledgement for bad pharmacy claims will detail the reason for failure for these pharmacy claims to help the submitter resubmit pharmacy claims. Good NCPDP D.0 pharmacy claims proceed to the next step and send to Pharmacy Benefit Manager to adjudicate the files and send back NCPDP 4.2 Post adjudication format files through EDI Gateway for validation. The system validates NCPDP 4.2 Post adjudication format files and a report will be generated with appropriate acknowledgments. The acknowledgement for bad pharmacy claims will detail the reason for failure for these pharmacy claims to help the Pharmacy Benefit Manager resubmit pharmacy claims. Good NCPDP 4.2 Post adjudication claims proceed to the next loading process. After validation NCPDP files send to Filenet for archival. Validation is accomplished by an industry accepted COTS product-Edifecs XEngine.

Loading Process: The loading process reads the NCPDP 4.2 Post adjudication format files and loads them into evoBrix X database. While loading these files, the data is subjected to industry wide loading business rules tailored as needed to meet DPHHS requirements.

Claims Adjudication: The system applies NCPDP post adjudication pharmacy claim information for cost sharing during claims adjudication processing.

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 will work closely with DPHHS and the Systems Integrator to define and implement the most effective way to report system availability of the Claims Processing solution automatically to the SI availability solution. Team CNSI uses our Business Monitoring Solution – HealthBeat® -- to provide DPHHS with configurable, automated, and real-time visibility into business operations, SLA compliance, and system monitoring. As part of the DDI phase, we will work with the SI to determine the best method, frequency and content of information that can be provided from our solution to the SI availability tool. HealthBeat will also be used to allow DPHHS, System Integrator or other stakeholders or vendors with approved access to obtain a detailed view into the performance of the Claims Processing module's performance. The following reporting capabilities are available to automatically report system availability to the SI's availability solution.

- Reports
- Dashboards
- Charts
- Kiosk
- Notification Alerts and Emails

The following are key components of healthy operations that our operations staff monitor to ensure continuous operations and prevent disruption:

- 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)

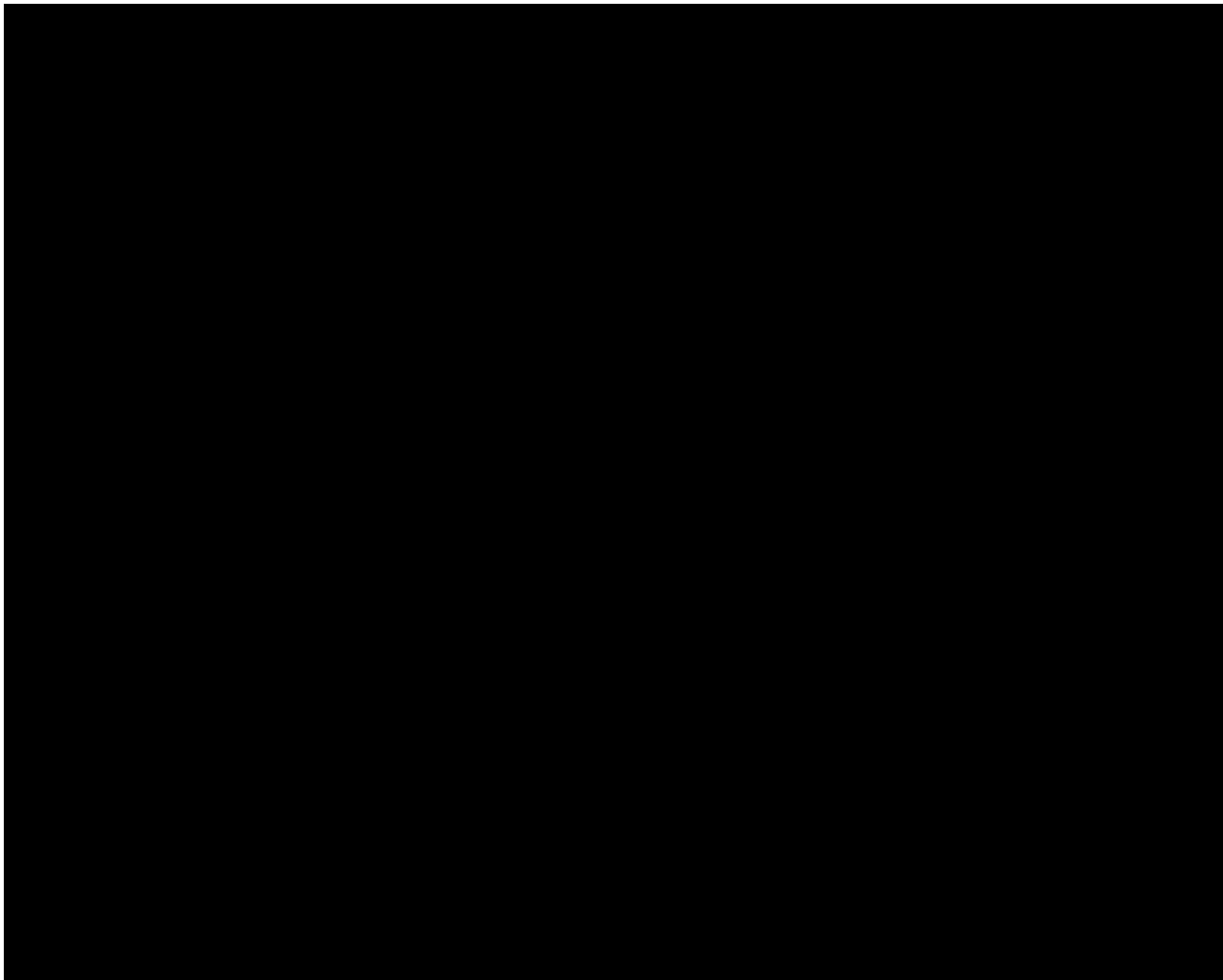
Monitoring and Reporting System Availability

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.

SLA Automation Tool and Operational Performance Standards

Team CNSI’s SLA automation solution provides DPHHS with several configurable SLA management capabilities through a number of different tools. All SLAs will be managed and tracked in Jira Service Desk. These tools allow Team CNSI and DPHHS to track and ensure that SLAs are being met. Figure 3.10.1-70 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, DPHHS and other stakeholders as identified by DPHHS to have visibility of daily system and business functions and their corresponding SLAs performance. The tool is also equipped with tracking, reporting, and management capabilities using the HealthBeat application. For example, the tool allows Team CNSI to measure SLAs on Interfaces processing. This visibility enables Team CNSI to maintain 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

Team CNSI's business monitoring solution, 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 State 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 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 HealthBeat. Figure 3.10.1-71 shows how HealthBeat monitors system resources of real application clustered (RAC) databases.

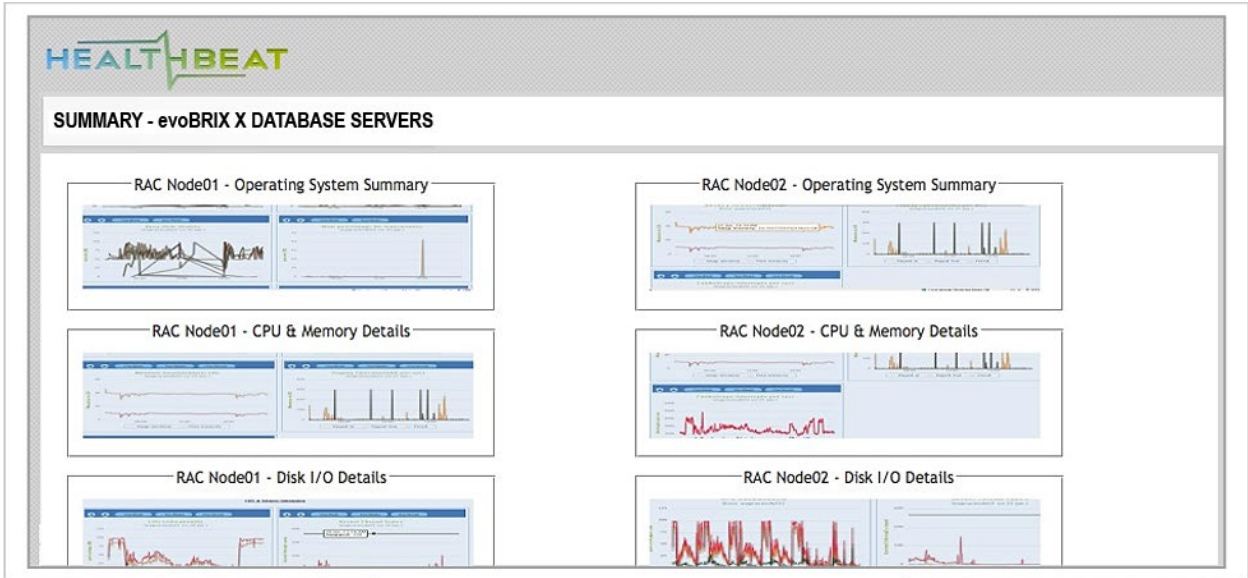
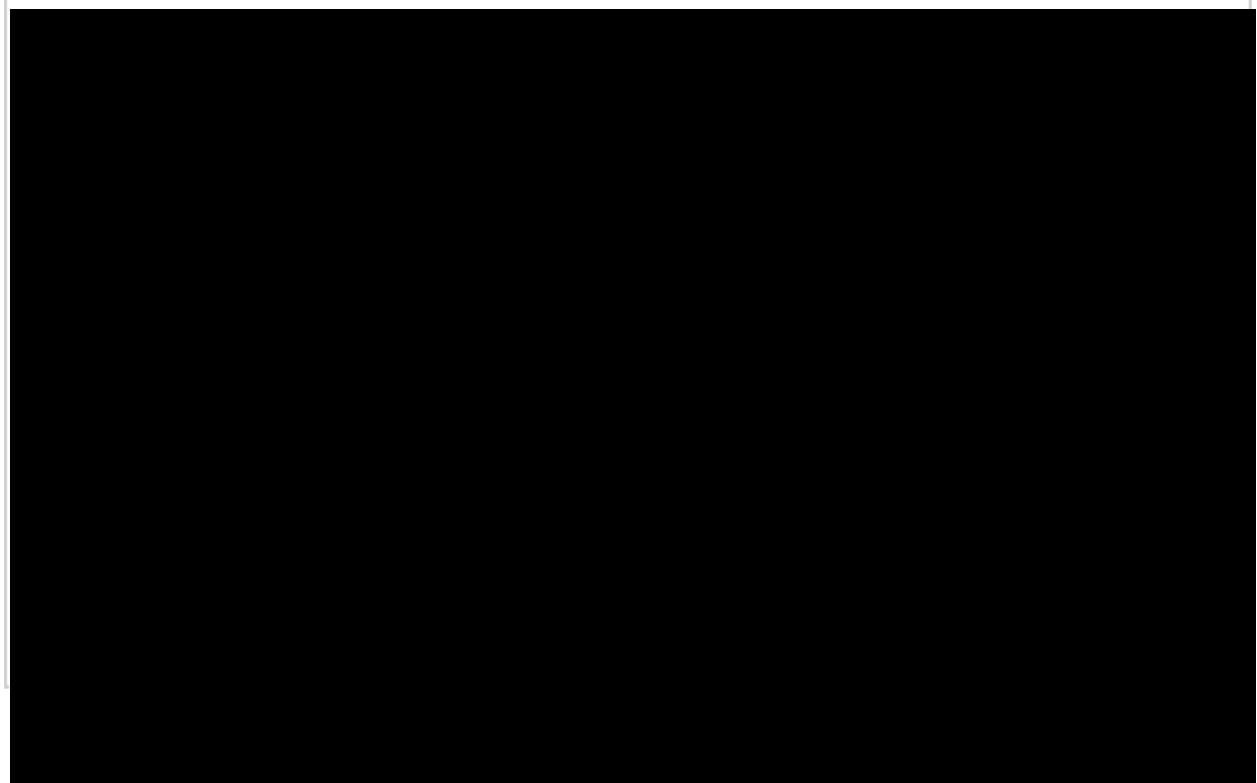


Figure 3.10.1-71. HealthBeat Screen Views of System Monitoring. Our solution offers monitoring of clustered databases.

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.





INT70

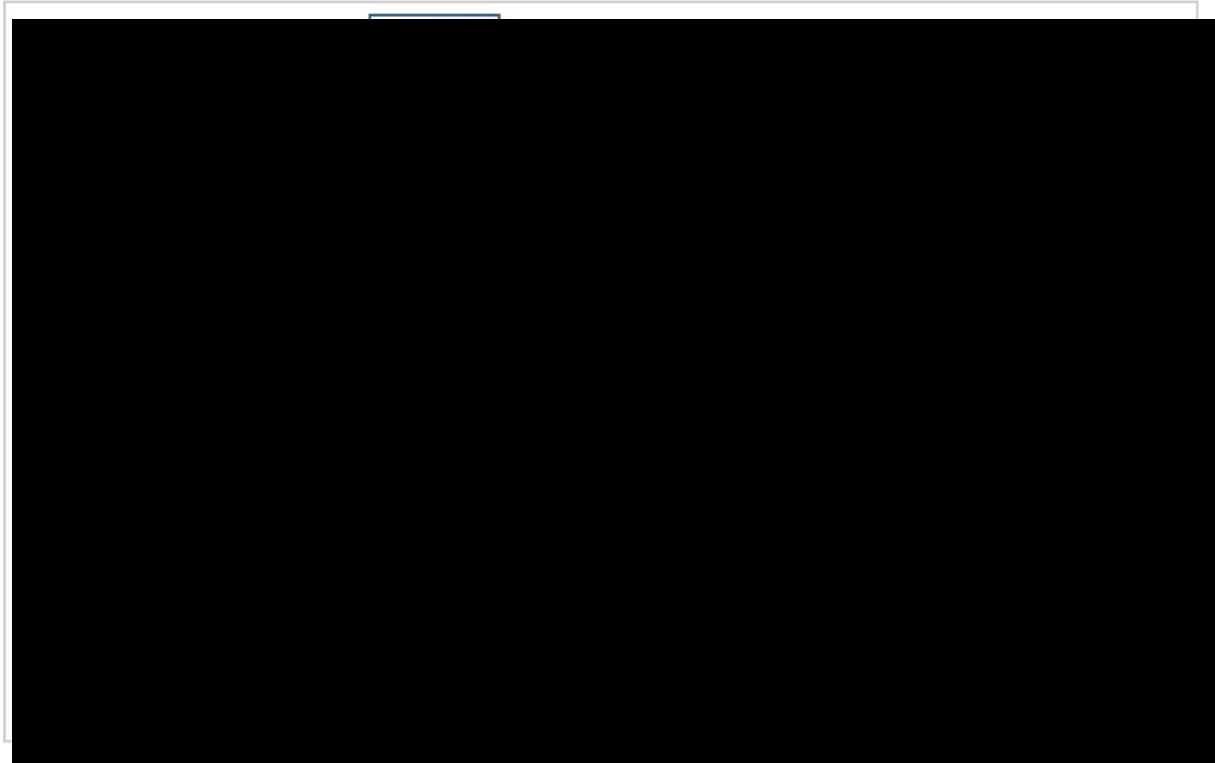
The Contractor shall identify and describe the licenses necessary for the scope of work to support the infrastructure that will provide sufficient bandwidth and redundancy to ensure accessibility, reliability/fault tolerance and acceptable performance.

Team CNSI's evoBrix X CPMS 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.



[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Infrastructure Type	Feature	Solution	License Type



INT73

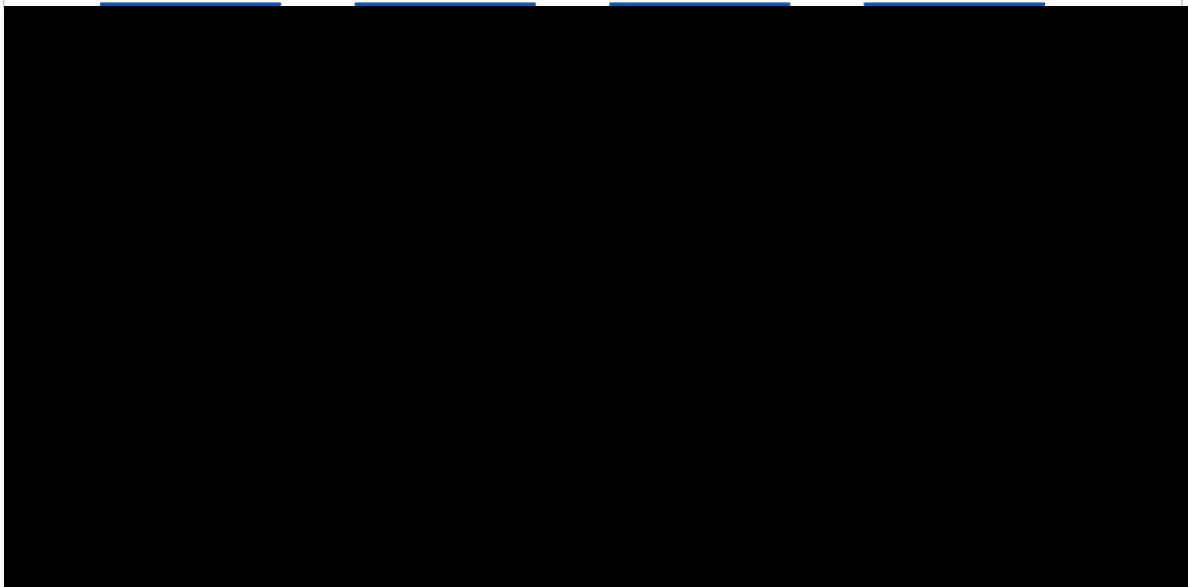
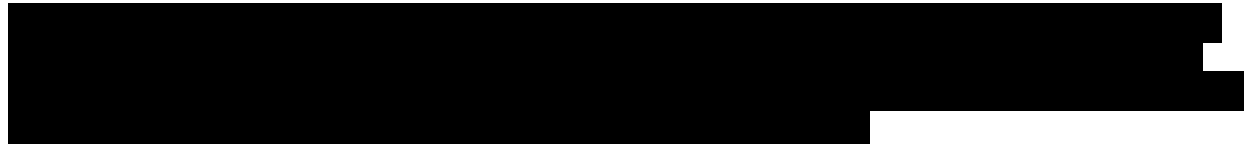
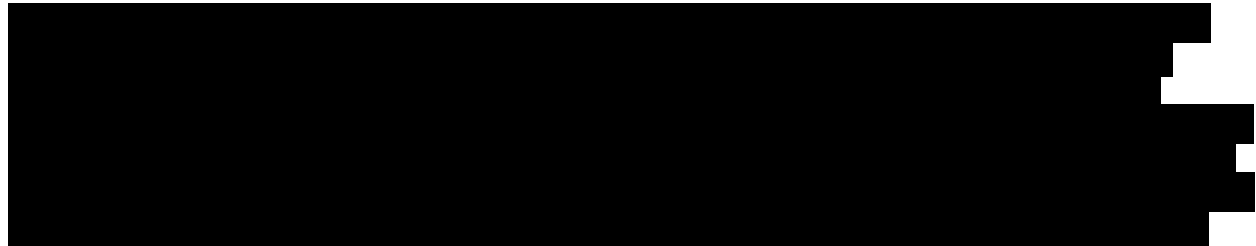
The Contractor shall be responsible for understanding the business processes to automate and orchestrate appropriate workflows, business rules, data flow and metadata within the solution and work collaboratively with the SI.

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 the 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.

INT77

The Contractor's solution shall provide a highly automated systematic processing of healthcare claims and eligibility transactions.

Team CNSI's evoBrix X CPMS solution provides an effective member-centric repository containing comprehensive information about members, including their demographic, financial, socio-economic, and health status information. This repository includes eligibility, enrollment spans, eligible benefit plans/services, member payment, cost sharing, spend-down, and third-party insurance information. The evoBrix X Core Claims module member services also provide flexible administration of benefit plan assignment rules to allow members to enroll in multiple benefit plans based on their eligibility. Team CNSI's solution ensures consistent, accurate, efficient, and faster access to data in real-time, batch mode, and manual processes for addition/update of demographics, eligibility, and enrollment information.



MTCPM-1.2.4-614



INT78

The Contractor shall provide an environment where components can be added or replaced quickly.

Team CNSI's public cloud will be hosted in the AWS, 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 public 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 public cloud can be subscribed to or cancelled, on an ad hoc basis, using the "Pay as you go" subscription model. [REDACTED]

[illegible]

For example, if DPHHS has a requirement to install and configure a security or compliance tool for a short period of time:

- [illegible]

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 X CPMS solution provides State staff and providers with a web-based data entry screens for submitting the paper claims and associating the supporting documents while submitting the claims.

Team CNSI’s evoBrix X Integration Gateway will support automated data exchanges with various Medicaid business process areas and interface partners and includes the below components to provide the ability to share and federate data with other data sharing partners

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

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.

[REDACTED]

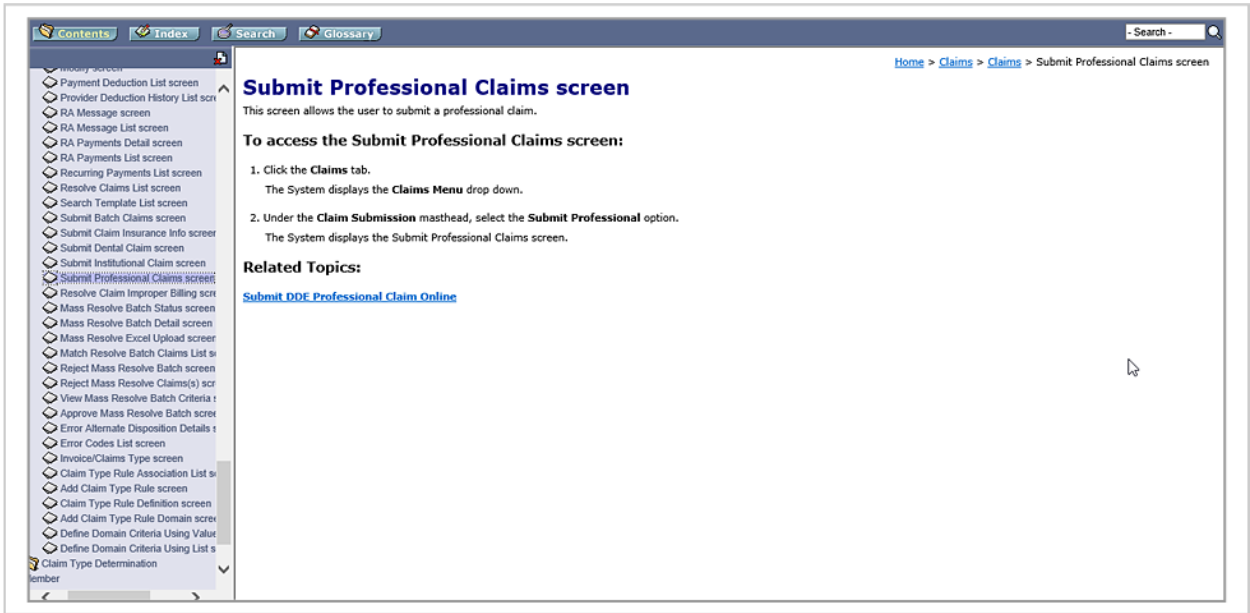
This solution provides an integration backbone that connects core applications and services without directly accessing the underlying systems. The solution is

capable of handling common industry standard service requests such as SOAP and REST. Also, evoBrix X 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.

INT87

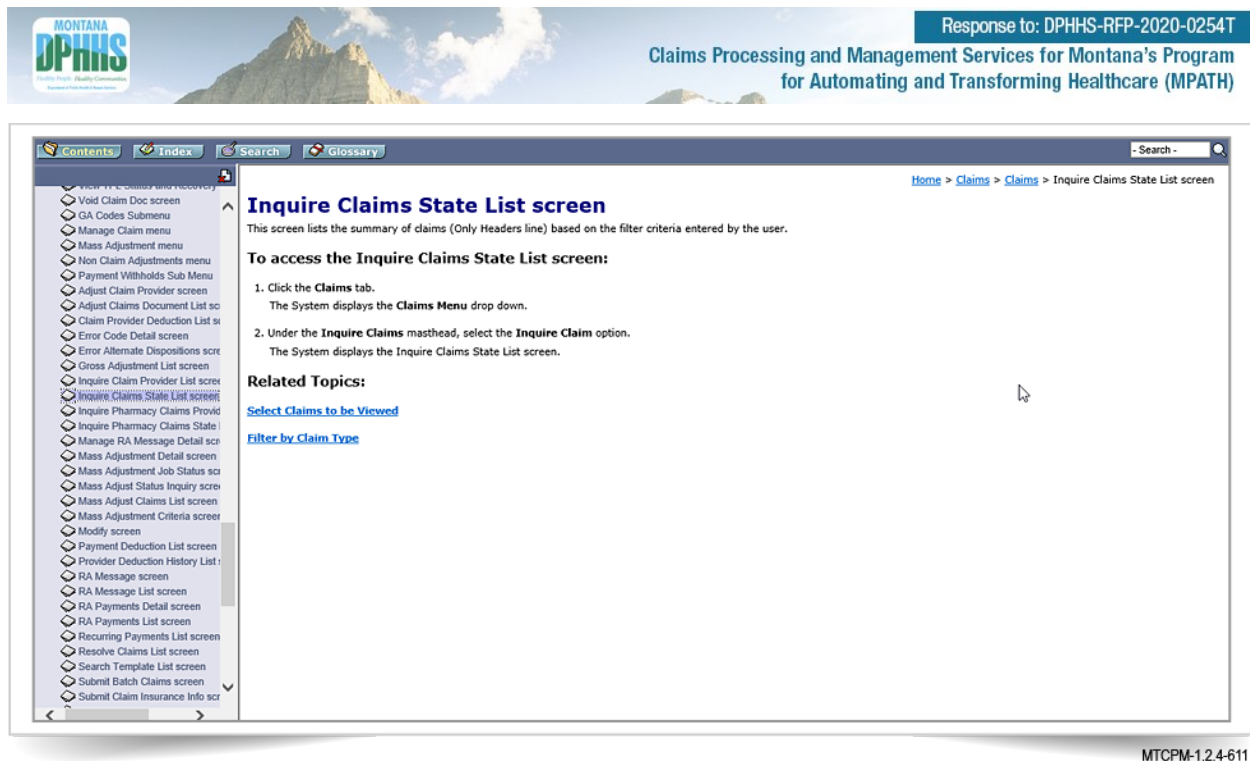
The Contractor’s solution shall provide context sensitive help (situational clarification and support associated with process specific steps), to support user activities (e.g., provider enrollment and maintenance activities).

The evoBrix X CPMS 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 3.10.1-77, and Figure 3.10.1-78 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.



MTCPM-12.4-615

Figure 3.10.1-77. Submit Professional Claims Help Context. User-friendly help is offered through a Claims Submission Screen.



MTCPM-1.2.4-611

Figure 3.10.1-78. Submit Professional Claims Help Context. User-friendly help is offered through a Claims Submission Screen.

INT88

The Contractor shall implement a solution where module components are loosely coupled and can be added or replaced quickly.

One of evoBrix X'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 of our solution enables 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 X'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 X CPMS 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

Team CNSI’s evoBrix X CPMS solution 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 X solution for MT CPMS is supported by standardized data models for meeting the day-to-day technical and business operational needs. We will collaborate with all other modular vendors, including the MPATH System Integrator (Deloitte), to reconcile data elements and integrate our solution with the MPATH Integration Platform to optimize data exchange across the enterprise.

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 X solution for MT CPMS 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 CPMS 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 X platform and collaborate with the MPATH System Integrator and other module vendors to reconcile the State’s ODS data elements with the equivalent elements coming from the MT CPMS solution’s database, which is the system of record.

INT107

The Contractor's solution shall provide an architecture designed to support vertical and/or horizontal infrastructure and application scaling to meet increases in demand.

Team CNSI's evoBrix X CPMS solution will be hosted in the AWS public 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.

Horizontal Scaling – 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.

[Redacted]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Vertical Scaling – 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).

INT108

The Contractor's solution shall use standard messaging formats (e.g. XML, JSON, EDI, etc.) to ensure interoperability.

Team CNSI’s evoBrix X CPMS solution is built upon open standards and uses standard messaging formats to enable interoperability with different platforms, solutions, and modular components

The key interoperability capabilities of evoBrix X CPMS 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 and Correspondence 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.

INT109

All service endpoints/APIs shall be exposed to the State's Integration Platform and are able to receive and submit messages through the State's Integration Platform.

Team CNSI’s evoBrix X CPMS 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 X relies on open standards and standard APIs, such as the Java Business Integration (JBI) standard, for pluggability of third-party communities.

INT110

The Contractor's solution shall have the ability to identify errors in transactions and immediately notify the State's Integration Platform and the source system of the specific errors including whether the errors have precluded loading and/or using the data.

Team CNSI's evoBrix X CPMS solution provides the ability to intake or ingest externally sourced data relevant to the functioning of MT CPMS business operations via evoBrix X ISR solution as illustrated in Figure 3.10.1-75. The ISR solution integrates with external systems via MT Claims 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 webservice where we log complete requests and responses, giving complete visibility within the system and capturing services errors in error log tables. The evoBrix X CPMS 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 CPMS monitoring requirement, and error information will be sent in the reports.

INT111

The Contractor's solution shall be integrated in loosely coupled design patterns with the rest of the enterprise by encapsulating its core functions and interacting with the rest of the enterprise via interfaces to and from the State's Integration Platform which leverage interoperability data standards.

One of evoBrix X'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 have 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 X'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

Our evoBrix X CPMS solution 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.

INT112

The Contractor's solution shall support standard web services and specifications (e.g., REST, WSDL, WS-*, SOAP, JSON, XML, EDI).

Team CNSI's evoBrix X CPMS solution is built upon open standards and uses standard messaging formats to enable interoperability with different platforms, solutions, and modular components

- 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.
- 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

INT113

The Contractor's solution must be capable of receiving, translating, and processing data to and from the variety of secure protocols (e.g., HTTPS, FTPs, SFTP, AS2, AS3). The Contractor shall include in their response a list of protocols supported.

-
-
-

- Messaging Services include: AS1, AS2, ebMS, RNIF

INT114

The Contractor shall participate in the Data Governance process, as defined and administered by the Agency. The Data Governance process will define processes and adjudicate concerns for items including but not limited to:

- Enterprise data lifecycle management processes (including master data management)
- Data synchronization processes
- Data formats for data exchanged by/between systems in Agency's Enterprise
- Management of reference data (i.e. code list versions)
- Dispute resolution for data management issues

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 operationalizing 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, stewards and 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.

INT115

The Contractor's solution shall support full and incremental data synchronization between the solution and the State's Integration Platform for data entities as defined by the Agency.

Team CNSI's evoBrix X platform provides the ability to intake or ingest externally sourced data relevant to the functioning of MT CPMS business operations via evoBrix X ISR solution. The ISR solution integrates with external systems via MT CPMS. 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.

With an industrial level solution in place, evoBrix X CPMS should be able synchronize any externally sourced data, custom needs will have to be handled on a case to case basis.

INT116

The Contractor's solution shall ensure that module operational data is available and is supplied to the State's Integration Platform in a format and frequency as defined by the Agency. The State's Integration Platform may require periodic data refreshes at agreed upon intervals.

Any and all operational data available in any module or sub-module of evoBrix X data design can be made available on the State Integration Platform. With minimal configuration or coding, our evoBrix X CPMS solution can ensure that the State-defined format and frequency is met.

INT117

The Contractor shall work with the Agency and the Systems Integrator if data quality issues arise and shall assist in remediating those issues.

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). Team CNSI will be able to assist and remediate data quality issues, as needed.

INT118

The Contractor shall participate in the API Governance process, as defined and administered by the Agency. The API Governance process will define processes and adjudicate concerns for items including but not limited to:

- Design and definition of solution endpoint API specifications
- Revisions to solution endpoint APIs (minor & major)
- Deprecation of solution APIs
- Definition of data formats and code lists utilized by an API
- Dispute resolution for API designs and behavior
- Publication of solution API specifications to the Agency's API Registry

Team CNSI's evoBrix X CPMS solution is based on industrial strength API solutions:

- 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 and Correspondence 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.
- Secure information exchange using API keys, web service security 1.0 standards, and other security protocols for ensuring data during transit.

Having this experience designing evoBrix X provides MT with an experienced partner that can and will participate in state API's governance process.

INT119

The Contractor shall implement interfaces with the State's Integration Platform in accordance with technical specifications approved by the Agency.

Our evoBrix X CPMS solution aligns 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 conforming to CMMI product engineering standards

The evoBrix X solution offers 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.

Any additional State-specific technical specification will have to be investigated on a case to case basis. Team CNSI evoBrix X's modular design and adherence to industrial strength solution ensures that these standards can be met with minimal or no changes to the core.

INT120

The Contractor's solution shall support query-based service calls (e.g. request & response) for data entities and associated query parameters as required by the Agency.

Team CNSI's evoBrix X solution has well-defined, open interfaces with service definitions conforming to WSDL, Swagger RESTful API. These inherently have the capability to support query-based service calls.

INT121

The Contractor's solution shall support real-time notifications as required by the Agency including but not limited to changes to solution's data, transaction events, etc.

Team CNSI's evoBrix X CPMS solution supports real-time data trading of interfaces based on the business/operations need between state approved trading partners. Team CNSI's evoBrix X solution supports Data trading in near real-time via evoBrix X OSB web services. The evoBrix X 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 X Integrator's configurable ISR solution can handle MT CPMS 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 X 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 X 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.

INT122

The Contractor's solution shall transmit all dates in a format specified by the Agency (ISO8601).

Team CNSI's evoBrix X solution supports multiple ISO standards including ISO8601 for transmittal of data and time fields. The system comes with configurable parameters to ensure this requirement is met

INT123

The Agency reserves the right to make use of and share with stakeholders at the Agency's discretion, the technical specifications supplied by the Contractor for the solution endpoints exposed to the State's Integration Platform.

Team CNSI follows a 'design first' approach when developing 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 (for REST) and WSDL (for SOAP) to publish the API specification. 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, and agency can make use of and share with stakeholders at the agency's discretion for all the evoBrix X API endpoints exposed to the System Integrator platform.

INT124

The Contractor shall ensure that all data, transactions and service calls between the Contractor's solution and other modules (including legacy systems) are routed through the State's Integration Platform as required by the Agency.

One of the inherent strengths of our evoBrix X CPMS solution 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 have 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 X's modular capability includes:

- 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
- 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

This modular extensibility in the design enables us to configure and ensure that service calls between MT CPMS and other modules are routed through the State's Integration Platform.

INT125

The Contractor shall route data, transactions and service calls between the Contractor's solution and third-party systems and federal systems (e.g., CMS, IRS, SSA) through the State's Integration Platform as required by the Agency.

One of the inherent strengths of our evoBrix X CPMS solution 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 have 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 X's modular capability includes:

- 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
- 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

This modular extensibility in the design enables us to configure and ensure that service calls between MT CPMS, other third-party systems including federal are routed through the State's Integration Platform.

INT126

The Contractor's solution shall utilize supporting services, data sources, or data feeds (master indices, reference data, etc.) provided by the State's Integration Platform as required by the Agency.

Team CNSI's evoBrix X CPMS solution provides the ability to intake or ingest externally sourced data relevant to the functioning of MT CPMS business operations via evoBrix X ISR solution. The ISR solution integrates with external systems via MT CPMS 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.

INT127

The Contractor shall generate and supply solution test data (including synthetic or de-identified data). Test data shall approximate production data with sufficient fidelity to ensure reliability and accuracy of test results.

Team CNSI leverages a custom data de-identification solution – dataSecureD - to de-identify both the PHI and PII information in our solutions' transactional data store to generate and supply solution test data. The dataSecureD solution employs a metadata discovery service to screen and identify potential PHI and PII data elements and organize them into clusters based on the type of data. For example, the data elements related to various types of identifiers (such as Social Security Number, Employer Identification Number, Patient Account Number, Service Authorization Number, and Tax Identification Number) are grouped under an IDENTIFIER master group. The solution uses a multi-factor de-identification scheme and techniques, such as substitution, shuffling, number and data variance, and nulling to remove and replace the sensitive PHI/PII data with de-sensitized but realistic values, while maintaining full transactional fidelity, integrity, and accuracy.

INT128

The Contractor shall coordinate security configurations and data sensitivity for multiple environments (e.g. integration testing, pre-production) with the State's Integration Platform as required by the Agency.

The Team CNSI evoBrix X CPMS solution 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. Data which is stored and transmitted in

different tiers are encrypted and secured. Data present in Development and System Test environments are de-identified. evoBrix X CPMS solution is hosted in the AWS public cloud, which includes security and privacy controls that are compliant with FedRAMP, HIPAA, HITECH, FISMA, and NIST standards.

If DPHHS requires additional security practices and configurations, 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.

INT129

The Contractor's solution shall capture, log, maintain and supply upon request to the Agency metadata for transactions and service calls between the solution and the State's Integration Platform. Metadata shall include but is not limited to, enterprise-supplied transaction IDs, transaction success/failure status, and other information as defined by the Agency.

Data Sharing and exchange is the primary function of the evoBrix X Integration Gateway component. Team CNSI's evoBrix X Integration Gateway will support automated data exchanges with various Medicaid business process areas and interface partners and includes the below components to provide the ability to share and federate data with other data sharing partners

evoBrix X Integration Gateway components

- File/EDI Gateway
- API Gateway

Technical components

- Interface Service Repository (ISR)
- EDI Translator and Validator.
- Technical Services - Web Service Framework

Our evoBrix X ISR implements a comprehensive escalation feature to alert multiple levels of event subscribers. For an instance, if an inbound interface file related to claims arrives late, the system will alert the CNSI 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 approved agencies and confirm successful file transfers and uploads. The solution also provides configurable screens to administer the various aspects of the interface operations and provides a dashboard for reporting the status of all the scheduled interfaces. After processing the claim data, email notifications will be sent to the configured personnel on the status of the interfaces, including audit details of the interface.

For example: When an interface completes successfully, the System produces an email to notify the interface monitoring team of the event. Figure 3.10.1-80 provides a sample of the content of the success email. The identifying content of the email will vary based on the specific interface.

```

Subject: Inbound Interface Completion Acknowledgement (<<Interface Name>> [<<File Name>>])

*** DO NOT RESPOND TO THIS E-MAIL ***

<<Interface Name>> [<<Interface ID>>,<<File Name>>] was successfully completed.
Interface Run Details:
Interface Run SID : << Interface Run SID >>
Interface ID : << Interface ID >>
Interface Name : << Interface Name >>
File Name : << File Name >>
Start Time : << Start Time >>
End Time : << End Time >>
Archive Location : << Archive Location >>
Source Records : << Source Records >>
Success Records : << Success Records >>
Error Records : << Error Records >>

Dependents List :

<<Interface Name>>[ <<Interface SID >> ]

Triggered List :

<<Interface Name>>[ << Interface SID >>,<< Interface run SID >> ]

All Errors logged in INTERFACE_RUN_ERROR table.

Error Specifics

(up to 50 errors will be shown here):

*** DO NOT RESPOND TO THIS E-MAIL ***

*** DO NOT RESPOND TO THIS E-MAIL ***

```

MTCPM-1.2.4-478

Figure 3.10.1-80. Sample notification for Interface processed successfully

When an interface is unsuccessful, the solution produces an email to notify the interface monitoring team of the failure. Figure 3.10.1-81 provides a sample of the content of the failure email. Based on Data Validation result, the content of the failure message will vary for the specific type of error encountered.

```

Subject: Inbound Interface File Not Found(<<Interface Name>> [<<File Name>>])

*** DO NOT RESPOND TO THIS E-MAIL ***

The scheduled processing window for Interface <<Interface Name>> [<<Interface ID>>,<<File Name>>] is over but the expected
file was not found.

Interface Run Details:

Interface ID : << Interface ID >>
Interface Run SID : << Interface Run SID >>
Interface Name : << Interface Name >>
File Name : << File Name >>
Prerequisite Interfaces : N/A
Dependent Interfaces : N/A

Dependents List :

<<Interface Name>>[ <<Interface SID>> ]

Triggered List :
None

Interface Run Specifics Follow:

<<Scheduled Time +05mins>>----File not Found
<<Scheduled Time +10mins>>----File not Found
<<Scheduled Time +15mins>>----File not Found
...
<<Scheduled Time +Escalation Time>>----File not Found
Finish time reached, File not found, Notifications Sent
*** DO NOT RESPOND TO THIS E-MAIL ***

*** DO NOT RESPOND TO THIS E-MAIL ***

```

MTCPM-1.2.4-480

Figure 3.10.1-81. Sample notification for Interface Processed with Errors. When an interface is unsuccessful, the solution produces an email to notify the interface monitoring team of the failure.

INT130

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 thorough 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.

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 in detail their approach to meet each of the Data Management requirements in Attachment F – Requirements Response Matrix. The Offeror simply repeating the RFP requirements does not qualify as a good response as defined in Section 6.1.1 of this RFP.

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. Our evoBrix X modular platform is designed with a sound data management strategy that is key for managing the current and future data needs of the evoBrix X Core Claims module 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 leverages our data management strategy to manage the changes typically associated with health care regulations and reforms. Our data management strategy establishes the basic governance processes to handle the complex set of systems and applications, interfacing, and interoperating within the evoBrix X Core Claims module and with the partner/vendor systems that comprise the broader DPHHS Medicaid enterprise.

Team CNSI offers more than 18 years of experience developing and operating Medicaid Management Information System (MMIS) solutions. Our solutions and the highly sensitive data they process and store, meet or exceed State and Federal privacy and security standards. Our team brings this wealth of experience and our extensive set of mature practices to the implementation of the evoBrix X Core Claims module 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 operational data management policies related to the security of state Medicaid systems, and the most recent standards (as they exist on the RFP release date) outlined by HIPAA, HITECH, American Recovery and Reinvestment Act (ARRA), and the Affordable Care Act (ACA).

Our security architecture design is configurable to meet future State and federal requirements and 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, Illinois, Utah, Arizona, and Hawaii. Due to our experience and the maturity of our security practice, Team CNSI is accustomed to 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. Our approach to developing security controls and procedures for the evoBrix X Core Claims module is to tightly integrate the strategies and best practices we have developed with the existing DPHHS security framework and extend or strengthen it wherever necessary.

Timely, secure, and relevant accessibility to enterprise data is key for the evoBrix X Core Claims module. Factoring in the specific data accessibility requirements for MPATH, both for implementing a well-defined operational system as well as giving due consideration to the future needs in the expansion of

The Team CNSI Advantage

Team CNSI brings a proven evoBrix X platform to support the Core Claims 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 X Core Claims

MTCPM-1.2.4-127

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, our overall approach for data accessibility and management for the system of record includes the information shown in Figure 3.10.1-82.

[illegible]

DM02

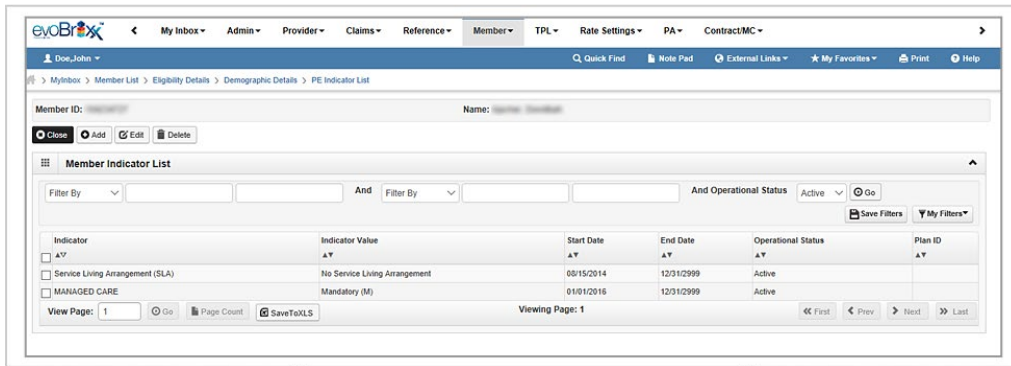
The Contractor's solution shall provide an indicator to suppress generation of documents containing Member identification for confidential services.

Team CNSI’s evoBrix X Core Claims module allows authorized users to add/manage member level indicators through online screens as well as batch and real time interfaces. The data model manages indicator details and uses the member indicator and other attributes to generate correspondence; however, customization/configuration is needed to add new indicators and suppress the generation of documents containing member identification for confidential services.

Team CNSI built the security infrastructure in the evoBrix X Core Claims module to protect Electronic Protected Health Information (ePHI) and to comply with federal standards, such as HIPAA for Member data. HIPAA and FISMA standards define baseline security control implementation requirements, and our security framework provides a secure environment for information management.

Our security framework includes protection against unwanted loss or disclosure of data using authenticated, role-based access control (RBAC) and extensive user audit logging for the audit trail to meet HIPAA Security and Privacy requirements from the application and database levels.

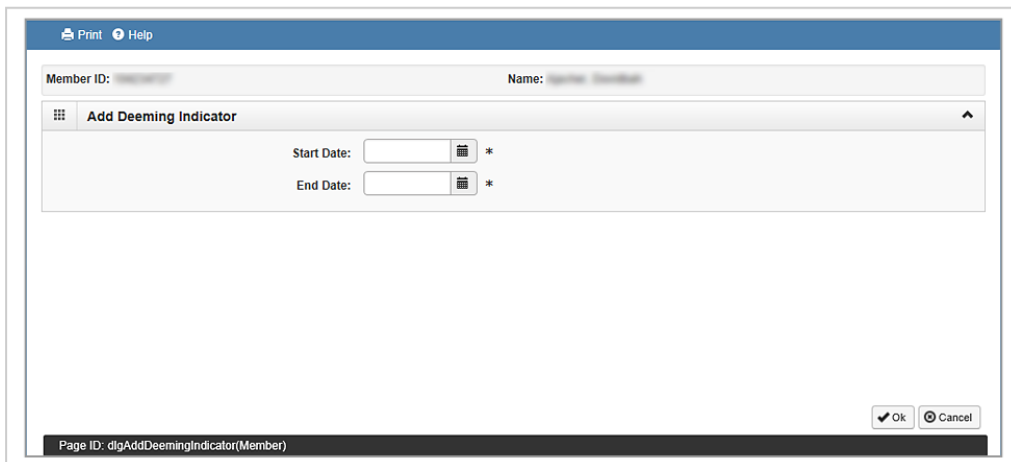
Figure 3.10.1-83 and Figure 3.10.1-84 illustrates how Team CNSI’s evoBrix X Core Claims module add/manage member level indicators through online screens.



Indicator	Indicator Value	Start Date	End Date	Operational Status	Plan ID
☐ Service Living Arrangement (SLA)	No Service Living Arrangement	05/15/2014	12/31/999	Active	
☐ MANAGED CARE	Mandatory (M)	01/01/2016	12/31/999	Active	

MTCPM-1.2.4-671

Figure 3.10.1-83. Manage Member level Indicators. Team CNSI’s evoBrix X Core Claims Module allows users to add/manage member level indicators through screen.



MTCPM-1.2.4-672

Figure 3.10.1-84. Add Member level Indicators. Team CNSI’s evoBrix X Core Claims Module allows users to add member level indicators through screen.

DM03

The Contractor's solution shall maintain a record/audit trail of a Member's requests for copies of personal records (including time/date, source, type, and status of request).

Team CNSI's myHealthPortal solution (Member Portal) allows members to request copies of their personal records. These requests are routed to the evoBrix X Core Claims module using real-time web services. Additionally, Team CNSI's CRM/IVR solution, offered as part of Option B, also facilitates intake of member requests for copies of personal records. Irrespective of the mode of request, we capture and maintain audit trails that includes time/date, source, type, and status of request in the system.

Team CNSI's evoBrix X solution can receive member requests for copies of the following documents for their personal records:

- Medicaid Card (For card product requests, the solution integrates with a room vendor for print and mail services.)
- Correspondences
- 1095B (Health Insurance Coverage)
- Third Party Liability (TPL) Details
- Explanation of Benefits (EOBs)
- Prior Authorizations (PAs)
- Managed Care Enrollment Eligibility Information
- Primary Care Physician (PCP)

Team CNSI's myHealthPortal (Member Portal) solution provides a user-friendly portal that allows Medicaid members to securely access their health information. Figure 3.10.1-85 provides the activities supported by Member Portal solution.

Member Document	Allowed Activities in myHealthPortal (Member Portal)
Medicaid Card	Allows Medicaid Members to securely access their health information, including their Medicaid Member ID card.
Correspondences	Allows Medicaid Members to securely access Correspondence Notifications like MSA & 1095-B Health Coverage
1095B (Health Insurance Coverage)	Allows Medicaid Members to securely access Correspondence Notification 1095-B Health Coverage
Explanation of Benefits (EOBs)	Enables members to perform the following: (a) Check eligibility related to covered benefit plans, and specific services for which the member is eligible. (b) Request coverage information under benefit plans.
Prior Authorizations (Pas)	Allows Medicaid members to view their Prior Authorization and display the list of corresponding Providers in Authorization Details screen.
Managed Care Enrollment Eligibility Information	Enables members to Check eligibility related to covered benefit plans, and specific services for which the member is eligible.
Primary Care Physician (PCP)	Allows Medicaid Members to perform the following: (a) Find doctors in your current geographic location (b) Perform a customized search for doctors

Figure 3.10.1-85. Team CNSI's myHealthPortal (Member Portal) solution features in terms of Member's Document Requests.

Team CNSI's CRM solution which is offered as part of Option B provides a screen to display the demographics of Providers/Members/Facility information. It provides key details such as Member

Name/DOB/SSN and for Provider/Facility, and displays the Provider Name, Facility Name, NPI etc. respectively. The demographics data is loaded in CRM through backend jobs which runs daily. Team CNSI’s CRM solution which is offered as part of Option B provides an organized and streamlined Service Request Management process and life cycle. The Service Requests can be created by various means such as Manual, real-time interface or through backend jobs. Once the Service Request is created, it is assigned to the respective Owner based on the defined Assignment skills. The Customer Service Representative (CSR) can capture the caller information and verify the details using the Provider, Facility and Members screen. The creator of the Service request can assign to other departments as per the business needs, or the CSR can withhold the ownership with themselves and can create Activities for the Service Request and assign to the relevant Owner. When all the activities are completed, the Service Request can be closed with appropriate solution and description. State models are implemented to control the lifecycle of the Service Request status. Critical fields of the service request can be audited for tracking changes using Audit Trail.

DM04

The Contractor’s solution shall maintain record/audit trail of errors during update processes, accounting for originating source and user.

We maintain record/audit trail of errors during update processes, which account for the originating source and user. The evoBrix X Core Claims module includes a comprehensive data model that supports record level history/versioning and audits. Our system captures every change, maintains the history, and provides the information for a specific period. It also captures audit information, such as what changes have been made, who made the changes, and when those changes were made.

Based on our extensive experience implementing and supporting operations for multiple states, we provide an audit trail of all pertinent events, applying 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 (e.g., 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 Agency’s System Integrator (SI) 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 evoBrix X Core Claims module receives the corrected data in the next interface run.

Figure 3.10.1-86, Figure 3.10.1-87, Figure 3.10.1-88, and Figure 3.10.1-89 illustrate the evoBrix X Core Claims module’s transactional record and error maintenance with the tracking of the originating source, audit trail summary and details, and user information applicable during update processes.

Member ID: Name:

Close Add Edit Delete

All Active Go

Save Filters My Filters

Eligibility Source	Scope	Coverage	Program	TOA	MA Case Number	MICChild Case Number	Citizen	HSW	Residential	MVA	MAGI Category	FPL Percent	Presumptive Eligibility	MOMS SDA Status	GPL	Due Date	Application Date	Created Date	Transaction Date	Start Date	End Date
☐ AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT	AT
☐ MA	1	F	N		631317560		B	00			C - Parents/Caretakers	37.77	N					09/19/2017	09/19/2017	09/01/2014	12/31/2999
☐ MA	1	F	N		631317560		B	00				41.00	N					06/18/2016	05/24/2017	08/01/2014	08/31/2014
☐ MA	1	F	N		631317560		B	00			C - Parents/Caretakers	41.00	N					06/18/2016	05/24/2017	03/01/2014	07/31/2014
☐ MA	1	F	N		631317560		B	00				0.00						06/18/2016	06/18/2016	06/01/2013	02/28/2014
☐ MA	1	E	N		631317560		B	00				0.00						06/01/2013	06/01/2013	04/01/2010	05/31/2013
☐ MOM														MA-ESO	6705931	06/12/2011		02/07/2011	06/22/2012	10/01/2010	08/31/2011

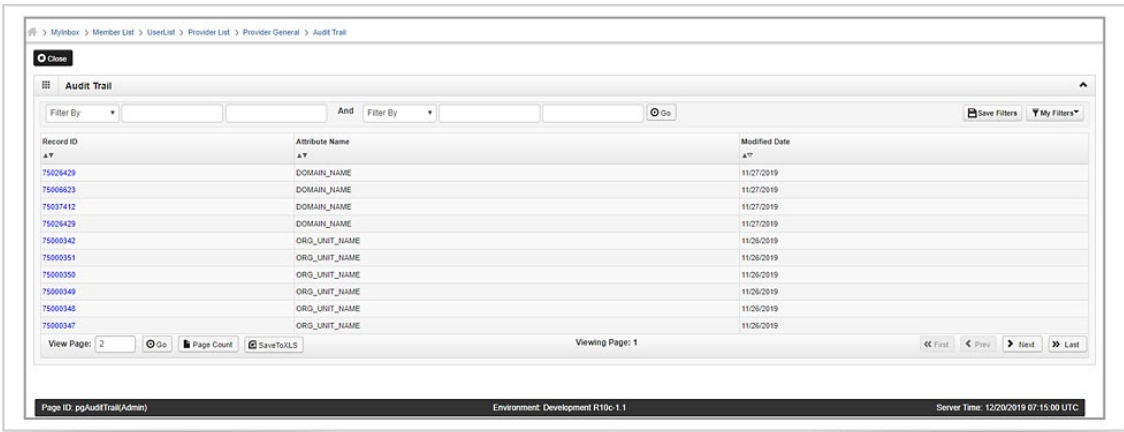
View Page: 1 Go Page Count SaveToXLS

Viewing Page: 1

First Prev Next Last

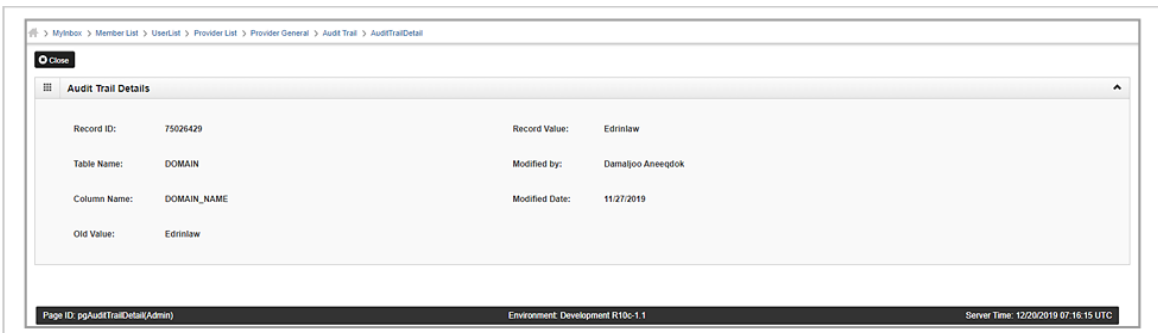
MTCPM-12.4-527

Figure 3.10.1-86. Record maintenance with originating source details during update processes. Team CNSI's evoBrix X solution ensures to store the originating source of the data.



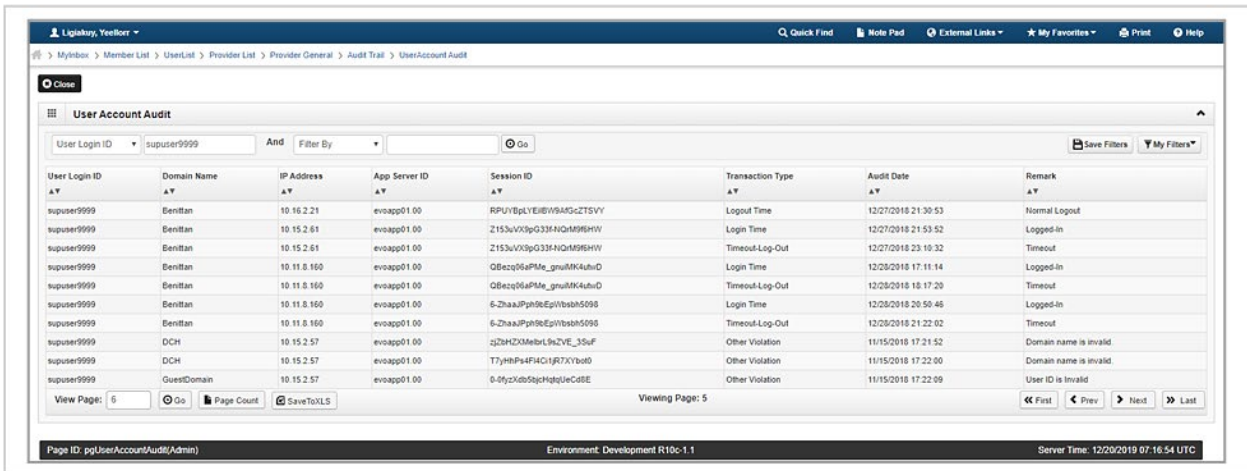
MTCPM-1.2.4-517

Figure 3.10.1-87. Audit trail summary information during update processes. Team CNSI's evoBrix X solution ensures to store the complete audit trial information for each data update.



MTCPM-1.2.4-518

Figure 3.10.1-88. Audit trail details during update processes. Team CNSI's evoBrix X solution ensures to store the complete audit trial detail information for each data update.



MTCPM-1.2.4-519

Figure 3.10.1-89. User account audit details during update processes. Team CNSI's evoBrix X solution ensures to store the user account audit information for each transaction.

DM56

The Contractor's solution shall receive and process member eligibility information from external sources (such as through the State's Eligibility Systems) on a real-time or near real-time basis, including:

- a. Producing total and detailed information that supports error correction and synchronization.
- b. Applying reconciliation changes.

Team CNSI's evoBrix X Core Claims module receives and processes member eligibility information from external sources (e.g., through the State's Eligibility Systems) on a real-time or near real-time basis, including: producing total and detailed information that supports error correction and synchronization; and applying reconciliation changes. Our solution offers a robust and comprehensive framework, which includes ISR and Oracle SOA, to manage the member eligibility data received from external sources. For our existing implementations for the states of Michigan and Washington, the Core Claims module processes 98% of the incremental or daily update member files with up to 300,000 member records within two hours. These records contain multiple eligibility, authorization, and demographic information segments.

The evoBrix X Core Claims module member repository can perform bulk loading, which is implemented using configurable multi-threaded processing. The Core Claims module identifies data conflicts via a member match algorithm, which detects invalid, duplicate, or overlapping records. Member or eligibility data issues, such as duplicate records or invalid data, are captured and reported on the scheduled member level error reports. The business rules for data validation are configured in evoBrix X and the error reports are generated on a daily basis. Data may be received from external sources in batch files or via real-time web services. The evoBrix X Core Claims module tracks transactions, providing a complete history that includes all the manual actions, which supports auditing and future traceability.

DM05

The Contractor's solution shall be able to store existing relationships created in other systems (e.g., a filing unit, parent/legal guardian/caretaker to a child/dependent, and any other member relationship(s) required to administer the State's healthcare programs).

Team CNSI's evoBrix X Core Claims module includes functionality to store existing relationships created in other systems (e.g., a filing unit, parent/legal guardian/caretaker to a child/dependent, and any other member relationship(s) required to administer the State's healthcare programs). The solution receives and maintains relationship data from multiple eligibility sources to administer and support the State's healthcare programs. The relationship data is used for benefit plan assignments, program enrollments, and correspondence generation for members.

Team CNSI's evoBrix X CPMS solution can receive and process relationship data from multiple sources. The solution uses the member identifier, relationship type, and member attributes from the inbound feed and validates that information against the case number and other member attributes to derive a head of household identifier. This identifier is a key element in determining the member association with multiple household groups and calculating the cost share details. Figure 3.10.1-90 shows how the evoBrix X CPMS solution maintains member relationship data.

Response to: DPHHS-RFP-2020-0254T

Claims Processing and Management Services for Montana's Program for Automating and Transforming Healthcare (MPATH)

Member ID: [REDACTED] Name: [REDACTED]

Begin Date: 10/01/2019 End Date: 12/31/2019 Group Income: 20,532.00

Medicaid Household Cost Share Met: Medicaid Household Cost Incurred: 5% Cap Amount: 256.65

PE Flag: Cost Sharing Limit Letter: N Date Cost Share Letter Sent:

Members In Group

Name	Member ID	Relationship with Primary	Cost Incurred(\$)	Member Cost Share Met	Date Member Cost Share Met
[REDACTED]	[REDACTED]	SO - Son	0.00	Y	10/01/2019
[REDACTED]	[REDACTED]	SE - Self	0.00	Y	10/01/2019

View Page: 1 [Go] [Page Count] [SaveToXLS] Viewing Page: 1 [First] [Prev] [Next] [Last]

Other Groups

Medicaid Household ID	Name	Relationship with Primary	Group Income(\$)	5% Cap(\$)	Member Cost Share Met
[REDACTED]	[REDACTED]	MO - Mother	0.00	0.00	Y

View Page: 1 [Go] [Page Count] [SaveToXLS] Viewing Page: 1 [First] [Prev] [Next] [Last]

MITCPM-1.2.4-551

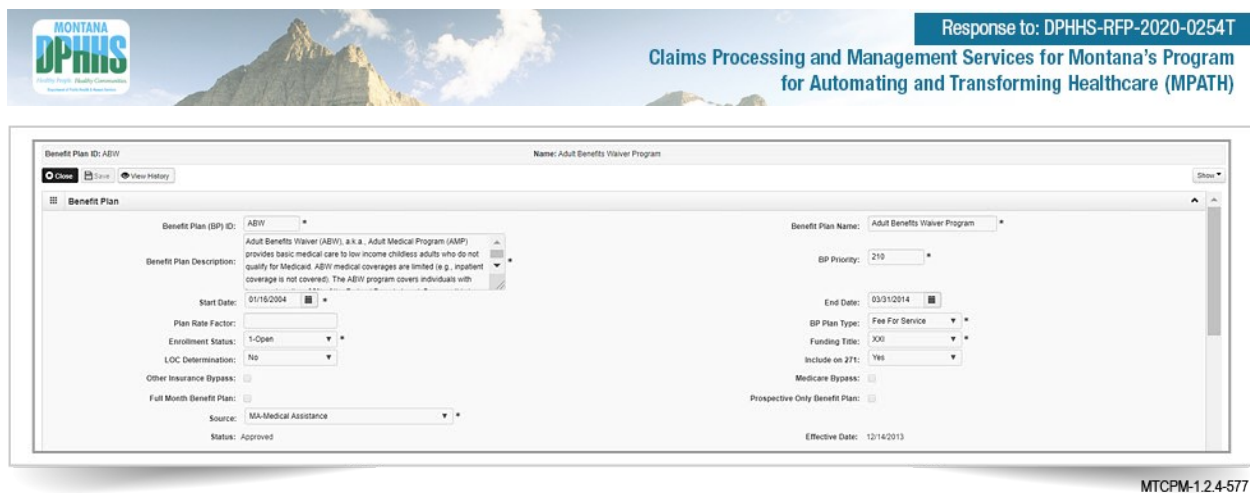
Figure 3.10.1-90. Member relationship maintenance screen in Team CNSI's evoBrix X Core Claims. Team CNSI's evoBrix X solution receive, store and maintain the relationship information of a member to administer State's health programs.

DM06

The Contractor's solution shall maintain a current and historical record of benefit plan assignment(s) for members, including periods of dual-eligibility.

Team CNSI's evoBrix X Core Claims module maintains current and historical record of benefit plan assignment(s) for members, including periods of dual eligibility spans. The solution includes a Benefit Plan component that supports benefit plan assignments based on a member's eligibility code. The Benefit Plan screen allows users to define and customize benefit plans necessary to meet the DPHHS requirements. Users can also configure benefit plans using member eligibility attributes (e.g., scope, coverage, program code, MAGI category, recipient aid category, and demographic information). The system assigns eligible Medicaid members who match the configured characteristics to the benefit plan. Every member is assigned to receive services under at least one benefit plan. In addition, members are assigned to one or more benefit plans based on the receipt of eligibility. This assignment process derives benefit plans based on member attributes and stores information at the member level, along with a start and end date.

Team CNSI's evoBrix X CPMS solution provides a Benefits Administration framework that enables DPHHS to structure benefits for efficient care delivery and faster realization of program and benefit plan changes and eliminate most of the hard-coding needed in backend software programs. The solution offers a user-controlled, business rule-driven mechanism that provides DPHHS with a flexible, out-of-the-box solution to meet business requirements. Team CNSI has worked extensively with Medicaid stakeholders on our CMS-certified implementations in the States of Michigan and Washington to help define and mature benefit plans to support delivery models such as FFS, Managed Care, and Waiver programs. Figure 3.10.1-91 provides a screenshot of the benefit plans screen.



MTCPM-1.2.4-577

Figure 3.10.1-91. Benefit Plan Screen in Team CNSI's evoBrix X Core Claims. Team CNSI's evoBrix X solution add, store and maintain the benefit plan assignment for members.

The evoBrix X CPMS solution provides the functionality to establish, view, and maintain benefit plans. It offers online screen functionality to define the category of service through procedure codes, diagnosis codes, benefit limitations, provider exclusions, eligibility criteria, effective dates, and member cost sharing. Authorized users can make timely changes to plan information through online screens and reduce or add services, define monetary limitations, or impose premium and co-pay restrictions. The system assigns eligible Medicaid members who match the configured characteristics to the benefit plan. Every assigned member then receives services under at least one benefit plan. In addition, members are assigned to one or more benefit plans (dual eligibility) based on the receipt of eligibility using the co-existence benefit plan functionality. This assignment process derives benefit plans based on member attributes and stores information at the member level, along with a start and end date. Any change in benefit plan attributes automatically re-derives the benefit plan along with audit fields (e.g., from date, to date, and effective date), which enables the solution to maintain historical archives. The system maintains the complete benefit plan history, which is used during claims adjudication to derive benefits based on date of service.

Team CNSI's evoBrix X Claim Adjudication engine checks eligibility and benefit plans for a member at the time of adjudication and pays or denies a claim appropriately. The system can also receive and process retroactive eligibility changes from DPHHS. Claims can be re-processed once the system makes eligibility and final benefit plan assignments.

Benefit Plan ID	Benefit Plan Name	Type	Priority	Status	Start Date	End Date	Effective Date
ABIV	Adult Benefits Waiver Program	F Fee For Service	210	Approved	01/15/2004	03/31/2014	12/14/2013
ABIV/ESO	Adult Benefits Waiver (Emergency Services)	F Fee For Service	630	Approved	01/15/2004	12/31/2009	06/10/2009
ABIV/ESD	Adult Benefits Waiver (Emergency Services)	F Fee For Service	630	Approved	01/15/2004	03/31/2014	12/14/2013
ABIV/MC	Adult Benefits Waiver Program (Managed Care)	M Managed Care	190	Approved	01/15/2004	12/31/2009	06/10/2009
ABIV/MC	Adult Benefits Waiver Program (Managed Care)	M Managed Care	190	Approved	01/15/2004	03/31/2014	12/14/2013
ALME	Additional Low Income Medicare Beneficiary	N No Benefits	830	Approved	06/01/2001	12/31/2009	06/10/2009
APS	Amplified Provider Services	F Fee For Service	89	Approved	07/01/2014	12/31/2099	06/10/2014
AUT	Adult-Retired Services	M Managed Care	113	Approved	01/01/2016	12/31/2099	01/01/2016
AUT	Adult-Retired Services	M Managed Care	113	Approved	04/01/2013	12/31/2015	01/05/2013
BCCCP	Breast and Cervical Cancer Control Program	N No Benefits	870	Approved	01/01/2014	12/31/2099	03/25/2014

MTCPM-1.2.4-578

Figure 3.10.1-92. Benefit Plans List Screen in Team CNSI's evoBrix X Core Claims. Team CNSI's evoBrix X solution provides future of viewing and reporting all the available benefit plans.

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.

The evoBrix X system provides an audit trail to allow information on all transactions to be traced from receipt through completion. The audit trails capture, at a minimum, date/timestamp, data source, worker ID, and action taken. In addition, the system logs any errors encountered, which authorized users can then use for reporting purposes.

Different sources can initiate data updates to our solution data mart, including: application screens updating transactional data; our evoBrix X Interface Service Repository (ISR) solution updating reference and transactional data; and inbound Electronic Data Interchange (EDI) file transactions. Each source is 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 are not limited to, the originating user/application identity responsible for the data modification and the modified time. In addition, audit fields (e.g., from date, to date, and effective date) are applicable to functionalities like enrollment, which is active only for a certain time period. Our Core Claims module maintains history of such transactions as part of audit requirements and traceability. The Figure 3.10.1-93 depicts the audit details of a transaction traced from receipt through completion.

Member ID: XXXXXXXXXX

Name: XXXXXXXXXX

Close

Add

Edit

Delete

AllActiveGo

Save FiltersMy Filters

Eligibility Source	Scope	Coverage	Program	TOA	MA Case Number	MIChild Case Number	Citizen	Ol	HSW	Residential	MVA	MAGI	Category	FPL Percent	Presumptive Eligibility	MOMS MA SDA Status	GPL	Due Date	Application Date	Created Date	Transaction Date	Start Date	End Date
AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY	AY
MA	1	F	N		631317560		B	00					C - Parents/Caretakers	37.77	N					09/19/2017	09/19/2017	09/01/2014	12/31/2999
MA	1	F	N		631317560		B	00					C - Parents/Caretakers	41.00	N					06/18/2016	05/24/2017	08/01/2014	08/31/2014
MA	1	F	N		631317560		B	00					C - Parents/Caretakers	41.00	N					06/18/2016	05/24/2017	03/01/2014	07/31/2014
MA	1	F	N		631317560		B	00						0.00						06/18/2016	06/18/2016	06/01/2013	02/28/2014
MA	1	E	N		631317560		B	00						0.00						06/01/2013	06/01/2013	04/01/2010	05/31/2013
MOM																MA-ESO	6705931	06/12/2011		02/07/2011	06/22/2012	10/01/2010	08/31/2011

View Page: 1GoPage CountSaveToXLS

Viewing Page: 1

FirstPrevNextLast

Figure 3.10.1-93. Audit details of transaction. Team CNSI's evoBrix X solution stores all the transactions to trace from receipt of the transaction through the completion of the transaction.

We capture any exceptions and log them into error/exception tables in the evoBrix X error data mart while processing transactions through the evoBrix X CPMS solution screens or EDI file processing. 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. We use the evoBrix X Reporting Solution to summarize and report error transactions for critical modules for necessary action.

While the application and EDI updates occur as part of the evoBrix X Core Claims module, the evoBrix X ISR solution handles all interface files. Through its various interface methods (i.e., fully automated workflow, user-intervened workflow, or screen uploads), the evoBrix X ISR solution receives data from various internal and external sources and incorporates the information into the reference and transactional data mart. As a part of the MPATH operations process, any error information is logged into the ISR data mart. The error information includes, 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.

Figure 3.10.1-94 shows the email notification of an inbound interface to log any errors encountered for reporting.



Figure 3.10.1-94. Sample Email Notification of Inbound Interface facilitated by evoBrix XISR Solution. This notification provided Team CNSI Business Operations with the status of the Interface processing and to log any errors encountered for reporting.

Users can report errors through email notifications, the evoBrix X Reporting solution, HealthBeat, or error report extracts, depending on the interface method. We also note any escalations on source data correction or processing for respective actions.

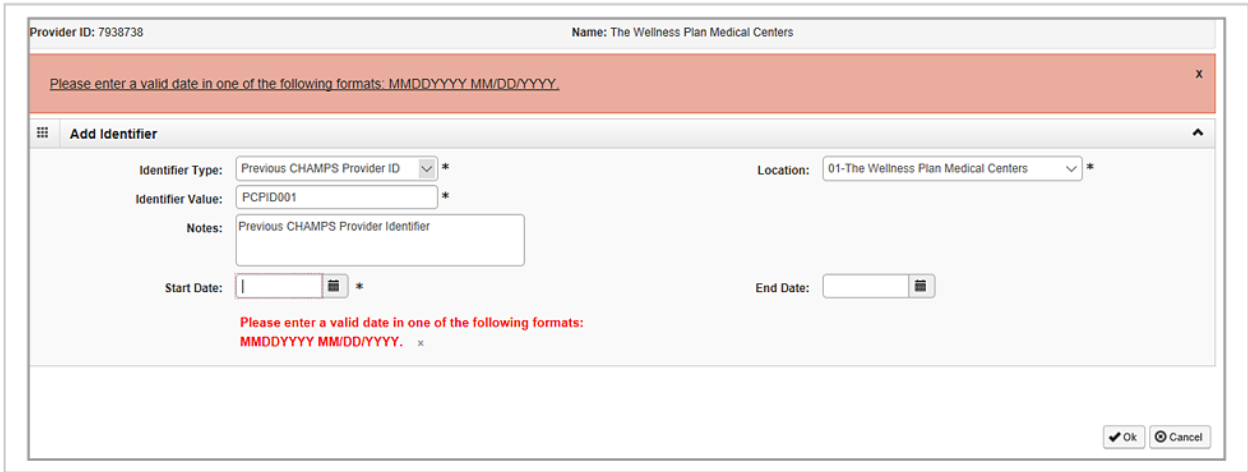
DM71

The Contractor's solution shall verify that all dates are valid and reasonable.

Team CNSI's evoBrix X Core Claims module provides an application portal to enable business operations users to manage day-to-day operations and verify that all dates are valid and reasonable. The application screens are powered by a robust framework that ensures that all entered date values 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 users so they can 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 is 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 validates 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 3.10.1-95 shows the evoBrix X Core Claims module application screen that enforces comprehensive validation of date formats/values.



The screenshot displays the 'Add Identifier' form in the evoBrix X Core Claims module. At the top, it shows 'Provider ID: 7938738' and 'Name: The Wellness Plan Medical Centers'. A red error banner at the top states: 'Please enter a valid date in one of the following formats: MMDDYYYY MM/DD/YYYY.' Below this, the form fields include:

- Identifier Type:** A dropdown menu set to 'Previous CHAMPS Provider ID' with an asterisk indicating it is required.
- Identifier Value:** A text input field containing 'PCPID001' with an asterisk.
- Notes:** A text area containing 'Previous CHAMPS Provider Identifier'.
- Location:** A dropdown menu set to '01-The Wellness Plan Medical Centers' with an asterisk.
- Start Date:** A date picker field with an asterisk.
- End Date:** A date picker field with an asterisk.

Below the date fields, a red error message states: 'Please enter a valid date in one of the following formats: MMDDYYYY MM/DD/YYYY.' At the bottom right, there are 'Ok' and 'Cancel' buttons.

MTCPM-1.2.4-147

Figure 3.10.1-95. Validations for Date Format/Value. Team CNSI’s evoBrix X Core Claims module supports comprehensive validation for date formats and values prompting users to take corrective action on the application screens.

DM10

The Contractor shall ensure that all narrative descriptions of codes and abbreviations are available for reporting.

Team CNSI’s evoBrix X Core Claims module manages reference data through online screens or through batch file uploads. Procedure codes (e.g., HCPCS, ICD) and all other metadata are maintained through reference data management. Each code includes fields for narrative description and effective start and end dates. Authorized users can extract these narrative descriptions as well as applicable abbreviations into reports, screens, or outbound interfaces.

Team CNSI’s evoBrix X CPMS solution maintains up-to-date versions of all provider-related reference data such as enrollment types, provider types, specialty, and sub-specialty. All codes include corresponding short and long descriptions as part of the reference data. These narrative descriptions could be extracted into reports using SQL query extracts, using the Excel download feature from the applicable screens, or using the ad-hoc reporting capabilities available through HealthBeat. Figure 3.10.1-96 is a screenshot of the solution’s diagnosis and code description screen.



Response to: DPHHS-RFP-2020-0254T

Claims Processing and Management Services for Montana's Program
for Automating and Transforming Healthcare (MPATH)

DiagnosisCode ID: 01500

Description: TB of joint NEC-unspec

Diagnosis Code Category: ICD-9-CM

Diagnosis Details

Diagnosis Code: 01500

Short Description: TB of joint NEC-unspec

Long Description: Tuberculosis of other specified joint, unspecified

Gender: B-Both

Start Date: 01/01/1979

End Date: 09/30/2015

National Begin Date: 01/01/1979

National End Date: 09/30/2015

Effective Date: 10/02/2015

Status: Approved

MTCPM-1.2.4-579

Figure 3.10.1-96. Diagnosis Code and Description. Team CNSI's evoBrix X solution stores and maintain all the Diagnosis Code and Description for reporting.

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.

The evoBrix X CPMS solution is designed on an integrated data model, which is managed through 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 X data model, and its supporting data dictionaries, help maintain the compatibility and integrity of data by enforcing business rules. Leveraging the erwin Data Modeler 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. It also ensures the timely availability of the relevant models for the transactional and operational systems for day-to-day business use.

We create standardized documentation for sharing the data design details of the evoBrix X Core Claims module for facilitating MPATH program operations. The Core Claims module follows industry standards for data element definition. The system documents the data dictionary by cataloging the different aspects of attributes, including size and other constraints. We publish a standard business data dictionary that details the definition, semantics, and element usage across different systems, and uses the concept of creating crosswalks between the different definitions of industry standards. Team CNSI assumes that valid values will be provided in the form of spreadsheets and not as column comments in the data dictionary. The alignment and adoption of industry standards-based approach ensures easier reporting and allows the evoBrix X platform to leverage industry benchmarks to improve overall program delivery.

We define and maintain a DPHHS-approved data dictionary as part of the evoBrix X physical data model using the 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 3.10.1-97 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 X 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 X table:

 CNSI

©2020 CNSI | Section 3.10
Page 222

Data Dictionary Component	Details
	(a) Field name in human readable format (b) Field description (c) Database field name (d) Database table (e) Field type and length (f) Database constraints (Referential integrity, Check/Not Null constraint, etc.) for the field, as applicable (g) Valid values and corresponding descriptions
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 X tables

Figure 3.10.1-97. Data Dictionary Component. Team CNSI's standard business data dictionary.

As required, the data dictionary contains the following information for each field, at a minimum: field name in human readable format, field description, database field name, database table, field type and length, valid values and their corresponding descriptions. The Figure 3.10.1-98, Figure 3.10.1-99, and Figure 3.10.1-100 shows sample of table structure, fields and valid values of them with descriptions.

Column(s) of Table "CLM_TYPE"					
Column Name	Comment	Data Type	Null	Is PK	Is FK
CLM_TYPE_CID	Unique system identifier for the claim type.	NUMBER(3)	Not Null	true	false
CLM_TYPE_NAME	Name (short description) for the Claim Type Code.	VARCHAR2(100)	Not Null	false	false
CLM_TYPE_DESC	Long description for the Claim Type Code.	VARCHAR2(200)	Not Null	false	false
INVOICE_TYPE_LKPCD	General Categories of the type of invoice: Professional Institutional Dental	VARCHAR2(1)	Not Null	false	false
CLM_TYPE_CODE	The code identifier for a claim type.	VARCHAR2(2)	Null	false	false
FROM_DATE	Date from which the claim error group relation is applicable.	DATE	Not Null	false	false
TO_DATE	Date unto which the claim error group relation is applicable.	DATE	Not Null	false	false
OPRTNL_FLAG	The flag indicating the status of the record.	VARCHAR2(1)	Not Null	false	false
CREATED_BY	Id of the user who created the record. This will always be a system user id	NUMBER(15)	Not Null	false	false
CREATED_DATE	Creation Date and time of the record. This shall be used on insert only.	DATE	Not Null	false	false
MODIFIED_BY	Person who modified this record.	NUMBER(15)	Not Null	false	false
MODIFIED_DATE	Date on which the record was modified.	DATE	Not Null	false	false

MTCPM-1.2.4-674

Figure 3.10.1-98. Table Structure Component of Data Dictionary. Team CNSI's standard Table Structure in business data dictionary.

CLM_TYPE_CID	CLM_TYPE_NAME	CLM_TYPE_DESC
0	All	All
1	Professional	Professional
2	Inpatient	Inpatient
3	Outpatient OPBS	Outpatient OPBS
4	Dental	Dental
5	PNMI/CRBH Claim	PNMI/CRBH Claim
6	Crossover A Claim	Crossover A Claim
7	Home Health/Hospice Claim	Home Health/Hospice Claim
8	Optical Claim	Optical Claim

CLM_TYPE_CID	CLM_TYPE_NAME	CLM_TYPE_DESC
9	Drug Claim	Drug Claim
10	Crossover B Claim	Crossover B Claim

Figure 3.10.1-99. The valid values of the data base table fields and their corresponding descriptions. Team CNSI's standard Table fields with valid values and their corresponding descriptions.

INVOICE_TYPE_LKPCD	Description
P	Professional
D	Dental
I	Institutional

Figure 3.10.1-100. The valid values of Lookup Code and their corresponding descriptions. Team CNSI's standard Lookup Code field with valid values and their corresponding descriptions.

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 evoBrix X Core Claims module supports backup and archiving requirements consistent with DPHHS SLAs and CMS, State, and industry standards. In addition, we adhere to data retention requirements cited in 45 CFR 164.316 and the State's Administrative Rules. Our approach is reliable and robust and is based on adherence with the following principles:

- Data is stored in native format
- Data de-duplication and replication
- Usable copies of production data for various use cases
- Fully managed and fully monitored solution by dedicated operations team

Backup retention is decided based on DPHHS data retention requirements cited in 45 CFR 164.316, the State's Administrative Rules, and industry standards. In addition, 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:





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 X Core Claims module maintains an audit trail of all data changes, including changes made in error that are subsequently backed out of or suspended. The 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 Core Claims 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 the Core Claims module. 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.

Figure 3.10.1-104, Figure 3.10.1-105, and Figure 3.10.1-106 depict the audit trail summary information, audit trail detailed information tracking the old and new values, and user account audit information of changes to transactional data.

Response to: DPHHS-RFP-2020-0254T

Claims Processing and Management Services for Montana's Program for Automating and Transforming Healthcare (MPATH)

MyInbox

Member List

UserList

Provider List

Provider General

Audit Trail

Audit Trail

Filter By

And

Filter By

Go

Save Filters

My Filters

Record ID	Attribute Name	Modified Date
AT	AT	AT
75026429	DOMAIN_NAME	11/27/2019
75006623	DOMAIN_NAME	11/27/2019
75037412	DOMAIN_NAME	11/27/2019
75026429	DOMAIN_NAME	11/27/2019
75000342	ORG_UNIT_NAME	11/26/2019
75000351	ORG_UNIT_NAME	11/26/2019
75000350	ORG_UNIT_NAME	11/26/2019
75000349	ORG_UNIT_NAME	11/26/2019
75000345	ORG_UNIT_NAME	11/26/2019
75000347	ORG_UNIT_NAME	11/26/2019

View Page: 2

Go

Page Count

SaveToXLS

Viewing Page: 1

First

Prev

Next

Last

Page ID: pgAuditTrail/Admin

Environment: Development R10c-1.1

Server Time: 12/20/2019 07:15:00 UTC

MTCPM-1.2.4-517

Figure 3.10.1-104. Audit trail information of all data changes. Team CNSI's evoBrix X solution ensures to store and maintain the complete audit trial information for each data change.

MyInbox

Member List

UserList

Provider List

Provider General

Audit Trail

AuditTrailDetail

Audit Trail Details

Record ID:

75026429

Record Value:

Edrinlaw

Table Name:

DOMAIN

Modified by:

Damaljo Aneegdok

Column Name:

DOMAIN_NAME

Modified Date:

11/27/2019

Old Value:

Edrinlaw

Page ID: pgAuditTrailDetail/Admin

Environment: Development R10c-1.1

Server Time: 12/20/2019 07:16:15 UTC

MTCPM-1.2.4-518

Figure 3.10.1-105. Audit trail detail information of data changes. Team CNSI's evoBrix X solution ensures to store and maintain the complete audit trial detail information for each data change.

Logging, Yeeleer

Quick Find

Note Pad

External Links

My Favorites

Print

Help

MyInbox

Member List

UserList

Provider List

Provider General

Audit Trail

UserAccount Audit

User Account Audit

User Login ID

And

Filter By

Go

Save Filters

My Filters

User Login ID	Domain Name	IP Address	App Server ID	Session ID	Transaction Type	Audit Date	Remark
AT	AT	AT	AT	AT	AT	AT	AT
supuser9999	Benitan	10.16.2.21	evosapp01.00	RPuV8pLYEIBWMSzZTSVY	Logout Time	12/27/2018 21:30:53	Normal Logout
supuser9999	Benitan	10.15.2.61	evosapp01.00	Z153uV03pG33FNGM9HWH	Login Time	12/27/2018 21:53:52	Logged-in
supuser9999	Benitan	10.15.2.61	evosapp01.00	Z153uV03pG33FNGM9HWH	Timeout-Log-Out	12/27/2018 23:10:32	Timeout
supuser9999	Benitan	10.11.8.160	evosapp01.00	QBecq06APMe_gnuMK4u0D	Login Time	12/28/2018 17:11:14	Logged-in
supuser9999	Benitan	10.11.8.160	evosapp01.00	QBecq06APMe_gnuMK4u0D	Timeout-Log-Out	12/28/2018 18:17:20	Timeout
supuser9999	Benitan	10.11.8.160	evosapp01.00	6-2haaIPph8EpiVbsh5098	Login Time	12/28/2018 20:50:46	Logged-in
supuser9999	Benitan	10.11.8.160	evosapp01.00	6-2haaIPph8EpiVbsh5098	Timeout-Log-Out	12/28/2018 21:22:02	Timeout
supuser9999	DCH	10.15.2.57	evosapp01.00	q2hKZMebL9nZVE_35uF	Other Violation	11/15/2018 17:21:52	Domain name is invalid
supuser9999	DCH	10.15.2.57	evosapp01.00	T7y8P4F4G1R7XVb0d	Other Violation	11/15/2018 17:22:00	Domain name is invalid
supuser9999	GuestDomain	10.15.2.57	evosapp01.00	0-0yZx0b5QchqgUeCd8E	Other Violation	11/15/2018 17:22:09	User ID is invalid

View Page: 6

Go

Page Count

SaveToXLS

Viewing Page: 5

First

Prev

Next

Last

Page ID: pgUserAccountAudit/Admin

Environment: Development R10c-1.1

Server Time: 12/20/2019 07:16:54 UTC

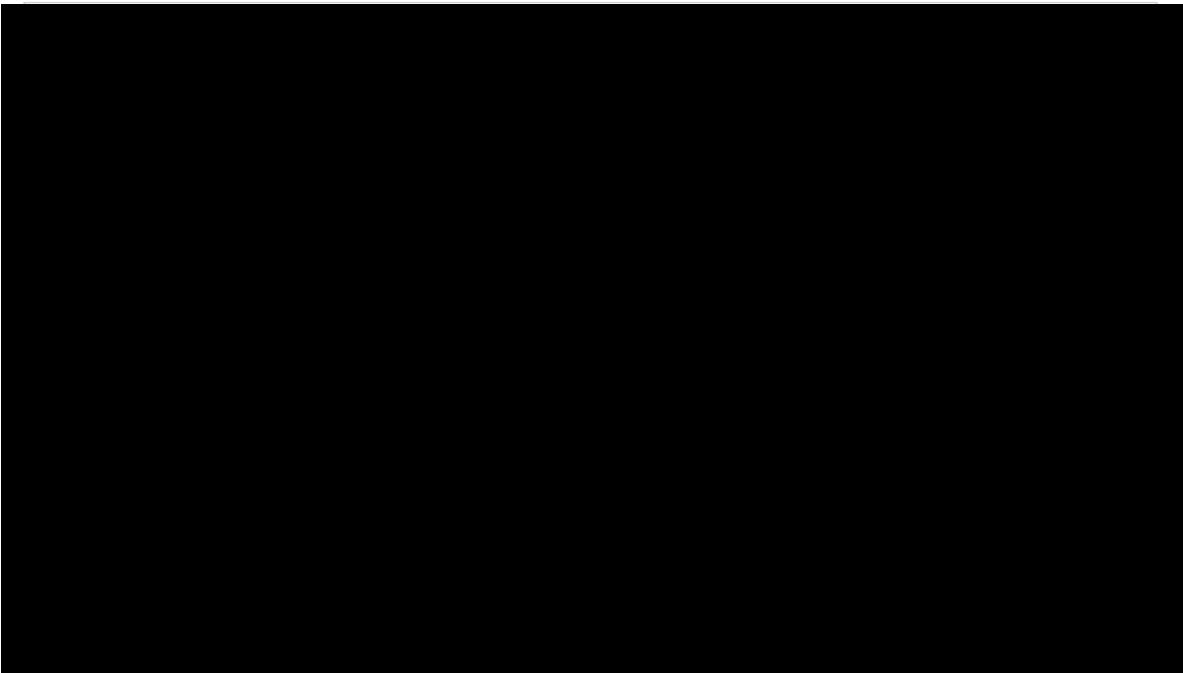
MTCPM-1.2.4-519

Figure 3.10.1-106. User Account Audit Information. Team CNSI's evoBrix X solution ensures to store and maintain the User Account audit information for each data change.

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's evoBrix X Core Claims module stores and applies updates to all applicable codes upon release at an appropriate for the data or when requested by DPHHS. 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 X Core Claims module 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.

**Batch Interfaces via Interface Service Repository (ISR)**

Scheduled interfaces load support data files automatically into Team CNSI's evoBrix X Core Claims module staging through the ISR solution. The data is then validated and processed per business requirements before it is loaded into the target data mart. As a part of our proposed Core Claims Operations process, error information is logged in the ISR data mart and reported through 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 X Core Claims module 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 X Core Claims module 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 DPHHS, can also be updated via the evoBrix X Core Claims application 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 X data repository.

DM18

The Contractor's solution shall perform batch control including logging and reporting.

Team CNSI's evoBrix X ISR solution provides a configurable design that features management of scheduling, loading, auditing, testing, error logging, reporting, and escalation. Batch interfaces are the preferred way to load data that is updated on a frequent basis during evoBrix X operations. The ISR solution receives batch files on a scheduled basis or through screen uploads. Received files go through file level validation, record level validation, and business level validation to ensure only correct data is loaded into the evoBrix X data mart. The error records during the validation process are logged into evoBrix X error tables. Audit information, including start and end time of the transaction, total number of records in the file, total error records, total successful records, and originating source are stored in evoBrix X audit tables.

Batch statuses, transactional errors, escalation, and audit information are reported through email notifications, our Reporting solution, or our HealthBeat solution. The ISR solution also reports unsuccessful file transfers and uploads to approved MPATH agencies and confirms successful file transfers and uploads. The solution also provides configurable screens to administer the various aspects of evoBrix X interface operations and provides a dashboard for reporting the status of all scheduled interfaces. In addition to reporting solutions, evoBrix X generates database reports to communicate the granular outcome of the individual batch process.

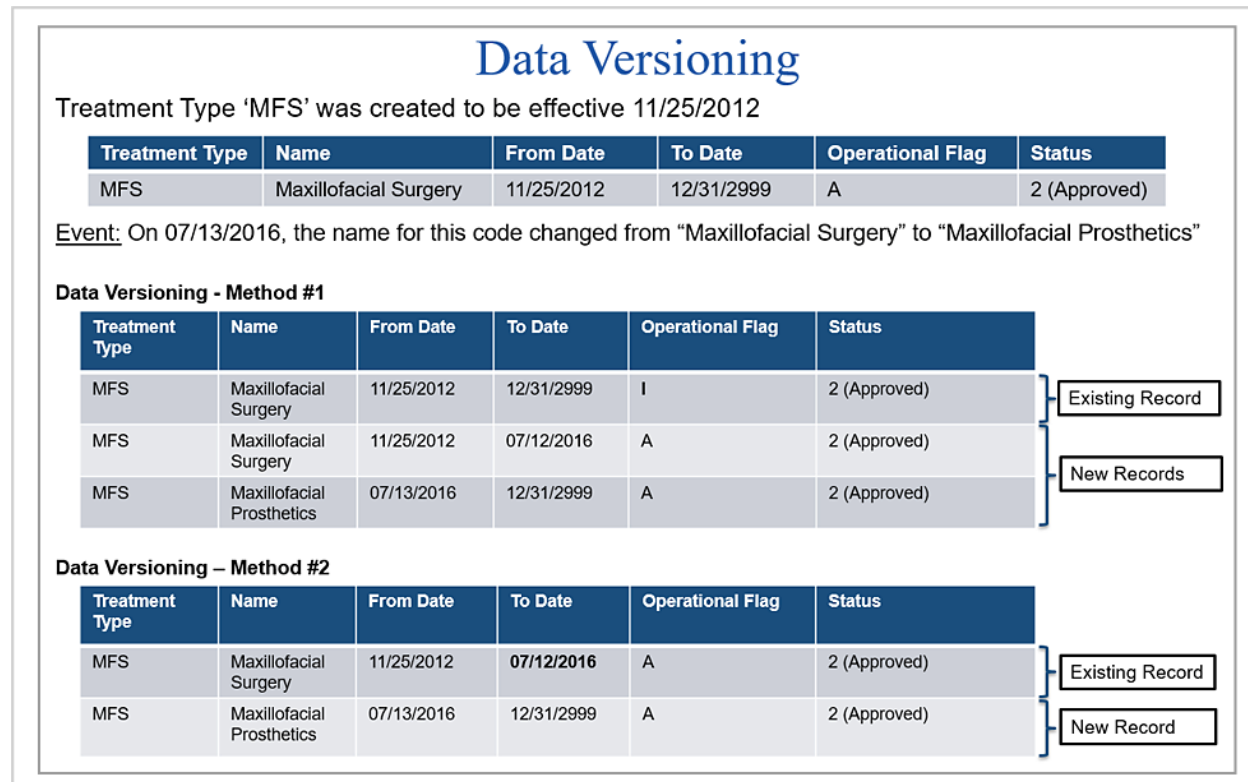
evoBrix X ISR implements a comprehensive escalation feature to alert multiple levels of event subscribers. For instance, if an inbound interface file related to claims arrives late, the system alerts Team CNSI operations staff and, if the file never arrives, the system subsequently notifies applicable business users. The system also reports unsuccessful file transfers and uploads to approved agencies to confirm successful file transfers. The solution also provides configurable screens to administer the various aspects of the interface operations and provides a dashboard for reporting the status of all scheduled interfaces. After processing claim data, the system sends email notifications regarding interface status, including audit details, to the configured personnel. For example, when an interface is successfully completed, the system produces an email to notify the interface monitoring team.

DM19

The Contractor's solution shall archive all versions of reference information and update transactions.

Team CNSI's evoBrix X Core Claims module adopts a data modeling paradigm that ensures no aspect of the reference information or changes/updates to 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 record to support a temporal report of events. Data segmentation helps visualize the data changes as "time slices" for varying time horizons. Figure 3.10.1-108 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).



MTCPM-1.2.4-135

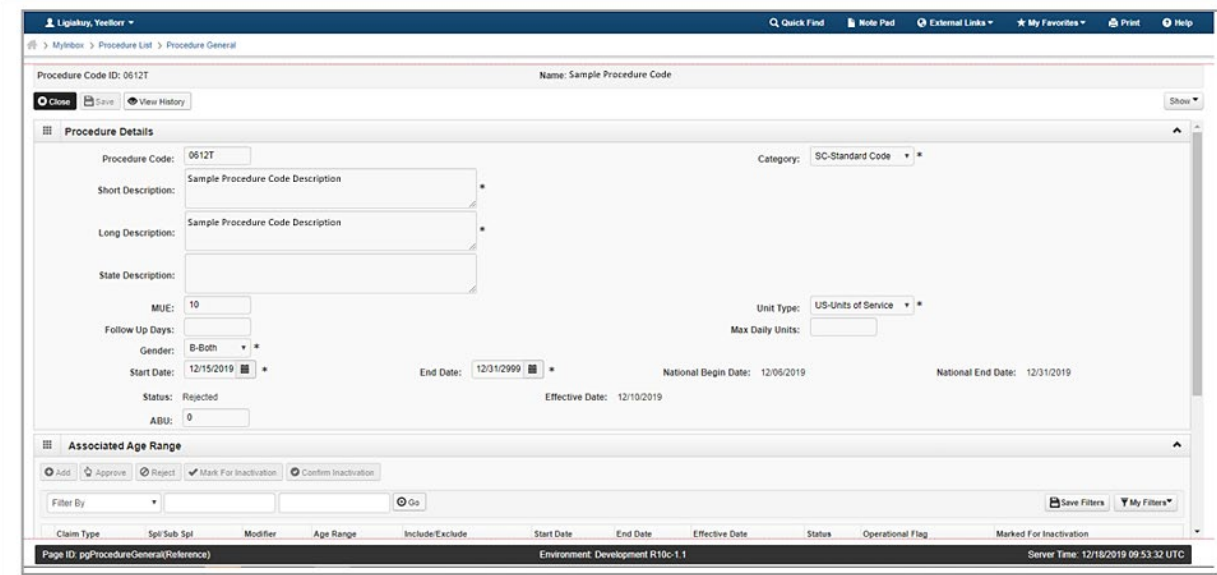
Figure 3.10.1-108. Data Versioning. Team CNSI's evoBrix X solution supports a comprehensive versioning mechanism to archive historical data changes.

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 X Core Claims module can void or reverse recent changes by rolling back to prior configurations. The module 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 to ensure that any change in pre-configured reference data do not impact existing transactions. Editable reference details are stored with appropriate statuses and effective date ranges in a detail table. Figure 3.10.1-109. depicts the configuration of reference data (Procedure Code) through a front-end screen.

When there is a need for a rollback of already configured reference data, the system can inactivate/end date the existing records and create new records with the latest details. Transactions 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.



MTCPM-1.2.4-481

Figure 3.10.1-109. Configuration of reference data (Procedure Code) through front-end screen. Team CNSI's evoBrix X solution allows configuration of reference data with from and to dates to of the validity with capable of void/reverse the changes done recently.

The application and database is architected to prevent the creation of duplicate or orphan records. In addition, Team CNSI has designed the system 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 includes built-in exception handling features to rollback 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 rollback a transaction that has violated the applicable business rules. Figure 3.10.1-110 shows the configuration of reference data history that was reversed or inactivated transactions.

Remark	Created Date	Created By	Modified Date	Modified By	Effective Date	From Date	To Date	Operational Flag	Status Name	History
	12-06-2019 14:14:43	Ligakuy,Yeellor	12-10-2019 10:57:16	Ligakuy,Yeellor	12-10-2019 10:55:59	12/06/2019	12/31/2999	Inactive	Approved	
	12-10-2019 10:56:05	Ligakuy,Yeellor	12-10-2019 10:57:44	Ligakuy,Yeellor	12-10-2019 10:57:16	12/06/2019	12/31/2019	Inactive	Approved	
	12-10-2019 10:57:39	Ligakuy,Yeellor	12-10-2019 10:57:44	Ligakuy,Yeellor	12-10-2019 10:57:44	12/15/2019	12/31/2019	Active	Approved	
	12-10-2019 10:57:44	Ligakuy,Yeellor	12-10-2019 10:57:44	Ligakuy,Yeellor	12-10-2019 10:57:16	12/06/2019	12/14/2019	Active	Approved	
	12-10-2019 10:58:50	Ligakuy,Yeellor	12-10-2019 11:01:31	Ligakuy,Yeellor	12-10-2019 11:01:31	12/15/2019	12/31/2999	Active	Rejected	

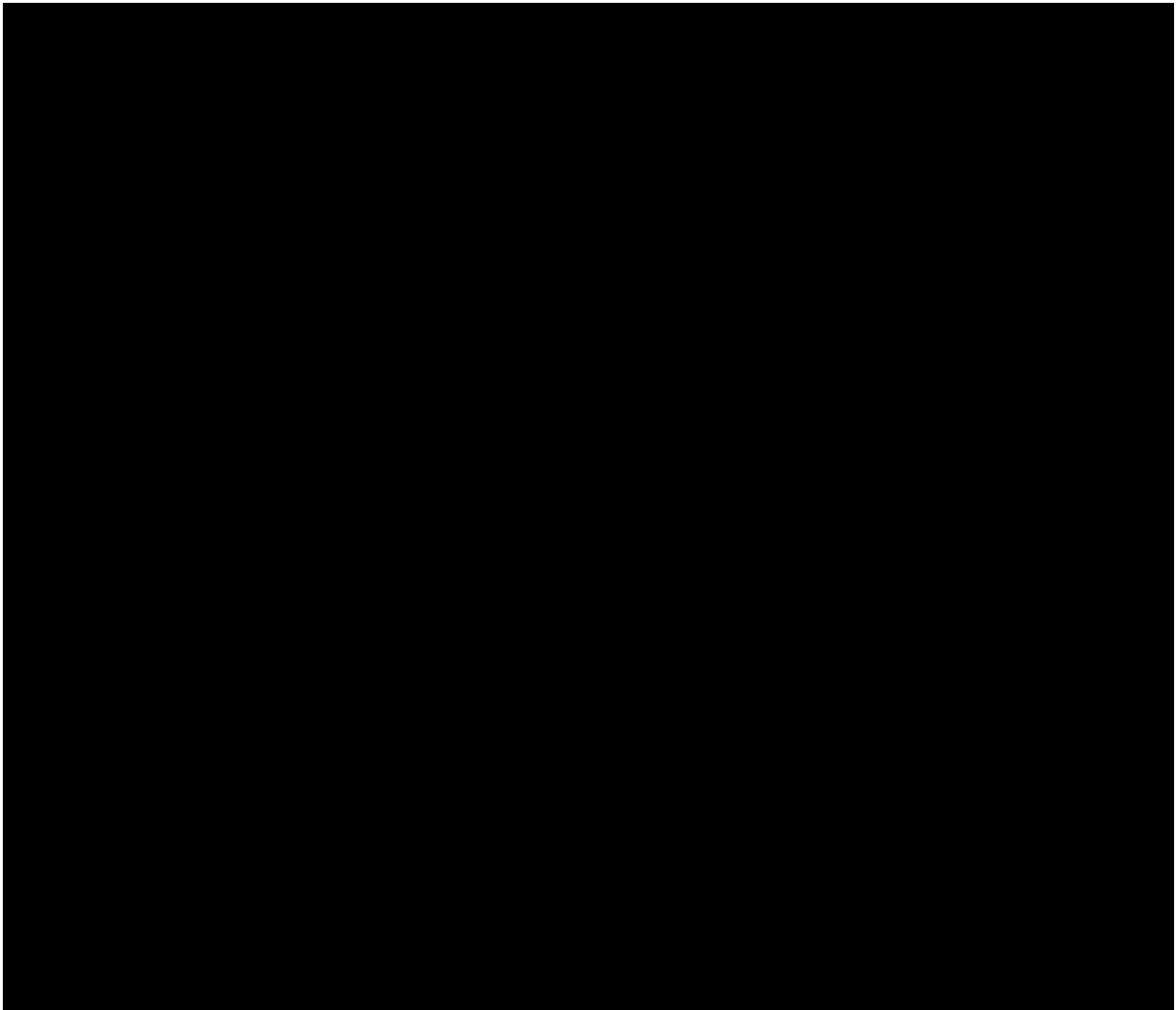
MTCPM-1.2.4-482

Figure 3.10.1-110. Configuration of reference data history. Team CNSI's evoBrix X solution stores the complete history of rolled back or inactivated transactions.

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).

Our data management strategy includes the following concepts: data integrity, data availability, data authenticity, data security, and non-repudiation of data. As such, the evoBrix X Core Claims module fully meets or exceeds all MARS-E specifications for security. The evoBrix X security standard is written to comply with CMS, NIST, FISMA, and HIPAA standards applicable to the system. The evoBrix X CPMS solution is designed with layered security zones, as shown in Figure 3.10.1-111. This layered design places 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 X system interfaces with the supporting vendor modules within the larger DPHHS enterprise system. All users accessing the evoBrix X system initially authenticate to the DPHHS system using the DPHHS-federated single sign-on (SSO) authentication system. That identity information is then passed onto the evoBrix X security system for authorization to data within the evoBrix X system using RBAC. The RBAC model ensures that users can only alter or modify data that they are authorized to access and change.

All data access is tracked within the system.



Using this tool, Team CNSI can:

- 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

We designed the evoBrix X system 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 includes full power redundancy, as well as fire and environmental protections. All hardware and network equipment in the primary site is duplicated and redundant; a 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 X system also has a fully equipped secondary site geographically separated from the primary to prevent failure due to facility disruption from natural disasters. The secondary site is built with the exact security and facilities standards as the primary site. All data is replicated in real time to the secondary site so that it fully assumes all tasks and workload in the event the primary site is not available. Based upon our annual testing, the secondary site becomes fully operational within four hours.

Data Security

Team CNSI's evoBrix X Core Claims module 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 X Core Claims module 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 X system use SSL technology for a fully encrypted connection. All file transfer connections use secure file transfer protocols for encrypted transfer. Where a flat file transfer is required, Team CNSI evoBrix X uses Oracle SOA MFT to ensure encryption of a file in transit and a 256bit AES encryption to encrypt the files. Administration and operational staff use encrypted VPN connectivity to access the servers. All data transferred on the network uses the Oracle network encryption technology to protect the data while in flight. Thus, all data in flight is encrypted as well. This avoids the risk of data loss on the network.

Team CNSI's evoBrix X Core Claims module 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 so users need to log into the system to access updates.

All data transfers between the Team CNSI evoBrix X Core Claims module and other parts of the DPHHS system occur through encrypted file transfers. Oracle SOA MFT is used for any transfers of files between trusted systems. All transfers of data are governed by the rules in the RBAC system, which restricts access to only that data a 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 X Core Claims module 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 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.

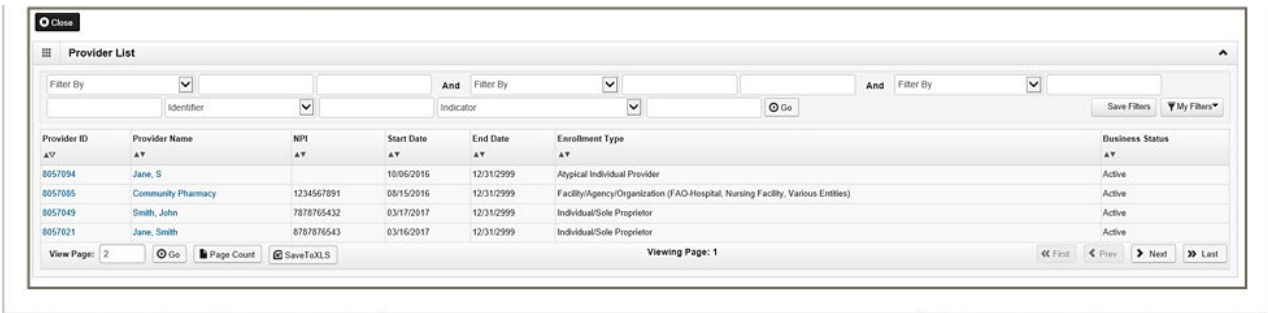
The use of the RBAC model in the evoBrix X system ensures full confidentiality of PHI and PII information. Users of the system can only access a limited set of data based on authorization in the system. The evoBrix X system facilitates easy removal of people from the list of authorized people to view information. The connector between the evoBrix X system and the larger DPHHS system is also governed by RBAC to prevent data leakage to other subsystems within the 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 X Core Claims module application screens allow authorized users to search for providers (entities) on the “Provider List” option. This page allows the user to search using multiple provider attributes to locate a specific enrolled provider (e.g., Provider Name, SSN, NPI, phone number) or a group of providers sharing a common set of attributes (e.g., EIN/TIN, ZIP code, and specialty).

The Provider List page includes three primary filters and two secondary filters, which can be configured by each user according to their preference. The user can then save their favorite search criteria using the “Save Filters” option. These criteria can then be retrieved later under the “My Filters” dropdown whenever the user wishes to re-use them. The retrieved results may be exported and saved to an Excel workbook for additional analysis using “Save to XLS” option. Figure 3.10.1-112 shows a sample provider list page from the Team CNSI evoBrix X CPMS Solution with the various filter options to facilitate an enhanced search for business users.



MTCPM-1.2.4-140

Figure 3.10.1-112. 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.

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.

Team CNSI’s evoBrix X Core Claims module ensures complete transparency of all data fields in reports generated including providing DPHHS 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, the source code or SQL for the underlying database objects needed to provide data for reports can be accessed and viewed through Team CNSI’s evoBrix X 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 X Core Claims module maintains a set of DPHHS/Team CNSI-defined online operational reports that are available for use from day one of implementation. In addition, users can build self-service reports with pre-defined parameters (e.g., provider number, procedure code, date of service) to monitor daily system operations and Fiscal Agent operations using the IBM Cognos BI tools in our Reporting Solution.

The evoBrix X Core Claims module’s reporting capabilities includes extensive features that offer a comprehensive view into day-to-day business operations as well as system activity. The module turns data into useful, actionable information. Team CNSI has built the evoBrix X reporting framework on a scalable data architecture and business process management layer to ensure data integrity and accurate, consistent reporting. The evoBrix X reporting and analytics architecture supports the business needs for successful MPATH operations.

Figure 3.10.1-113 shows the salient features and benefits of our reporting and analytics solution.

Features	Benefits
Granular data access	Medicaid-specific, detailed data that are not available in typical off-the-shelf solutions, which Team CNSI uses for ad-hoc reporting and analysis purposes.
Self-service BI reporting	We deliver user satisfaction and productivity gains reports to end users over the Internet with the ability to print/save as needed.
Ad-hoc reporting	DHPPS users can access aggregated data with different dimensions and underlying detailed data to support critical activities (e.g., reconciliation and policy making).
Pre-built reports/templates	Increased productivity with pre-built operational reports and templates.
Single sign-on	Reduced risk of account compromise with single sign on with the application and IBM Cognos BI, without replicating user credentials across multiple directory stores.
Operational reporting	Powerful payment cycle information, business SLA compliance alerts, worker productivity, and business operations summary to provide comprehensive operational reporting.

Figure 3.10.1-113. The State’s Various Reporting Requirements.

Based on DPHHS requirements, pre-defined reports and ad-hoc reports can be parameter driven. For ad-hoc reporting, users can design their reports as well as select from a pre-defined set of parameters to obtain the desired results.

Pre-defined reports contain both On-Demand and Scheduled reports. Both reports can be designed to be parameter driven as well. Figure 3.10.1-114-shows the End-to-end FFS Claims Tracking Report prompt page, where users can input the values according to business requirements.



MONTANA
DPHHS
Healthy People. Healthy Communities.
Transforming Health Care

Response to: DPHHS-RFP-2020-0254T

Claims Processing and Management Services for Montana's Program
for Automating and Transforming Healthcare (MPATH)

End to End Tracking of FFS Claims Report
🔍 ⚙️ ⋮ 🔔 👤 ?

Find

Report

PAGES

Report pages

Page1

Prompt pages

Prompt Page1

Classes

End to End Tracking Of FFS Claims Report

Either Pay Cycle Number OR Invoice Number OR Provider Number OR NPI OR Payment Number OR TCN OR Main Check Date is Mandatory!

Fiscal Year:	+	
Pay Cycle Number:	+	
Invoice Number:	+	
Provider Number:	+	
NPI:	+	
Payment Number:	+	
TCN:	+	

MTCPM-1.2.4-523

Figure 3.10.1-114. End-to-end FFS Claims Tracking Report prompt page. Team CNSI's evoBrix X reporting solution allows the users to input the values according to business requirements.

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 DPHHS data resides in data centers located in the continental United States. This data is only 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 is 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

Data in all development environments for the evoBrix X Core Claims module 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 PHI and PII information. The dataSecureD solution is fast, reliable, and secure and includes pre-configured components and templates purpose-built for Team CNSI’s evoBrix X 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 restorability.

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 X Core Claims module uses Pitney Bowes Spectrum Universal Addressing Module to validate and standardize postal addresses according to United States Postal Service (USPS) verification, validation, and standardization rules. Team CNSI periodically updates the Spectrum Universal Addressing Module database to keep up with the changes in the USPS addresses. The evoBrix X solution uses address validation functions to ensure efficient handling of USPS addresses, reduce costs associated with returned mail handling, and to ensure compliance with regulatory requirements. The following Figure 3.10.1-115 and Figure 3-10-1-116 depict examples of USPS Address Validation Failure and Success.

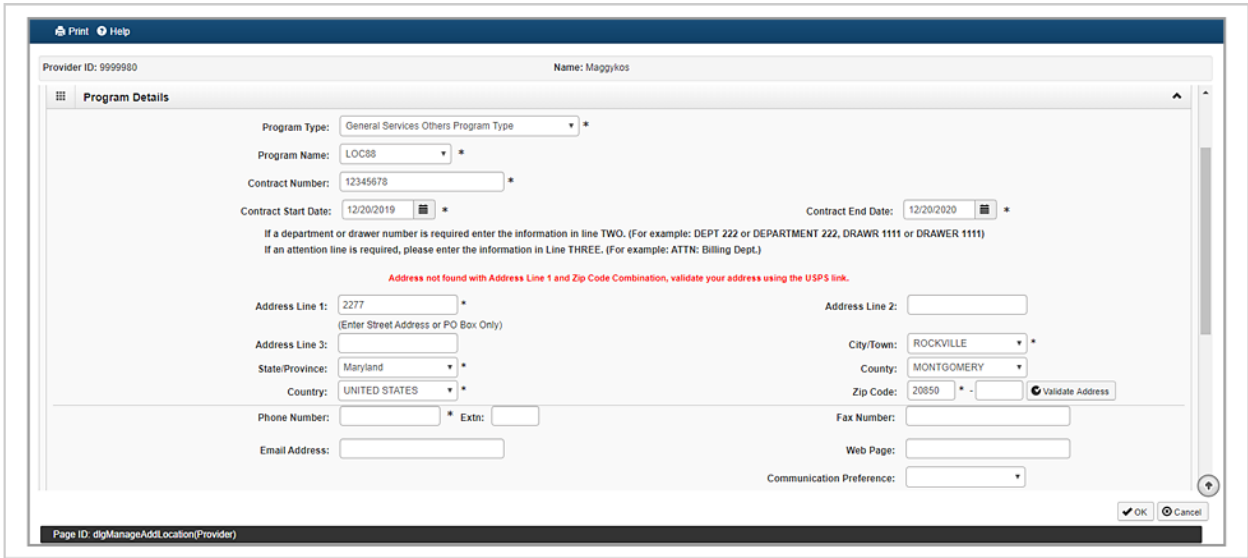


Figure 3.10.1-115. USPS Address Validation – Failure. Team CNSI’s evoBrix X solution capable of validating the address against the standardized USPS addresses.



MONTANA DPHHS
Healthy People. Healthy Communities.
Transforming Health Services.

Response to: DPHHS-RFP-2020-0254T

Claims Processing and Management Services for Montana's Program for Automating and Transforming Healthcare (MPATH)

Provider ID: 9999900
Name: Maggykos

Program Details

Program Type: General Services Others Program Type *

Program Name: LOC88 *

Contract Number: 12345678 *

Contract Start Date: 12/20/2019 *

Contract End Date: 12/20/2020 *

If a department or drawer number is required enter the information in line TWO. (For example: DEPT 222 or DEPARTMENT 222, DRAWN 1111 or DRAWER 1111)
If an attention line is required, please enter the information in Line THREE. (For example: ATTN: Billing Dept.)

Address validation successful

Address Line 1: 2277 Research Blvd *

(Enter Street Address or PO Box Only)

Address Line 3: *

State/Province: MARYLAND *

Country: UNITED STATES *

Phone Number: * Extn: *

Email Address: *

Address Line 2: *

City/Town: Rockville *

County: Montgomery *

Zip Code: 20850 * - 3224 *

Fax Number: *

Web Page: *

Communication Preference: *

Page ID: digManageAddLocation(Provider)

MTCPM-1.2.4-521

Figure 3-10-1-116. USPS Address Validation – Successful. Team CNSI’s evoBrix X solution capable of validating the address against the standardized USPS addresses.

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 X Core Claims module facilitates real-time data processing including data cleansing, data loading, data brokerage, integration, validation, reconciliation, and synchronization with the State’s enterprise. The module can intake or ingest externally sourced data relevant to the functioning of MPATH operations via evoBrix X ISR. The ISR solution integrates with external systems via evoBrix X 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 files in near real time or in batches on a scheduled basis. Any error and audit information are logged into the ISR solution’s error and audit data marts respectively.

Team CNSI’s evoBrix X Core Claims module is built on a relational database modelling paradigm with normalized data structures. This model ensures 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 X ISR solution can send the required extracts with the defined data sets to the DPHHS data warehouse on a schedule or request basis to ensure the data from the evoBrix X system of record is synchronized with the larger State’s enterprise.

DM38

The Contractor’s solution shall optimize and consolidate data management storage.

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.

[REDACTED]

[REDACTED]

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 offers a configurable data retention framework to meet the varying data retention needs for different business areas of the evoBrix X solution. The framework can address the data retention needs for audit, history, core partitioned, and non-partitioned entities managing the current and historical transactional/operational data. We consider any data that falls outside the defined data retention period as operationally non-relevant historical data and the framework physically deletes the applicable data record in the evoBrix X Core Claims module. We retain data from all supporting inbound and outbound interfaces for a period as defined by DPHHS. The HIPAA Code Sets (e.g., HCPCS and NDC defined by the HIPAA Administrative Simplification Rule) are maintained indefinitely, while the transactional 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) support storage for seven years.

Although the data retention framework is designed to be implemented at varying frequencies (e.g., daily, monthly, annual, or ad hoc), Team CNSI ensures that day-to-day business operations are not impacted due to the implementation of the data retention policies. The physical deletion of data is managed through 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 through direct physical daily deletes for low-volume transactional entities, thus balancing the needs of the data retention requirements and optimal system performance.

DM40

The Contractor's solution shall maintain a normalized RDBMS with referential integrity and is optimized to meet performance requirements.

Team CNSI maintains a normalized Relational Database Management System (RDBMS) with referential integrity, which is optimized to meet performance requirements. The evoBrix X physical data model addresses data needs of enterprise-wide Medicaid operations and includes the physical data model for all business areas of the Core Claims module (e.g., Provider, Member, Reference and Rates, Service authorization, Claims and Encounters), 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 implementations across the United States.

The evoBrix X physical data model balances the normalization needs of a data model with the performance needs of a large volume transaction processing system. Figure 3.10.1-117 shows evoBrix X's average operations processing volumes broken down by the functional modules applicable for various tenants. 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.

Tenant	Functional Module(s)							
	Provider	Member	Prior Authorization	FFS Claims	Encounters	Pharmacy Claims	Pharmacy Encounters	Managed Care Capitations Payments
Michigan	An average of 98 providers are approved daily (Since 2017).	85K	400	68K	254K	N/A	N/A	Over 6 Million monthly / 200,000 daily
Washington	7,500 Providers Screened	8,500 Eligibility Updates daily	300	35K	230K	12K	70K	80K
CMS EDPS	2.5 Million refreshes monthly/83,333 refreshes daily	500K – 1 Million updates / new members daily	N/A	N/A	3.5 - 4.5 Million received daily	N/A	N/A	N/A
VA-FSC	N/A	N/A	20K	35K	N/A	N/A	N/A	N/A

Figure 3.10.1-117. Team CNSI's evoBrix X average operations processing volumes applicable for various tenants. Team CNSI's evoBrix X Solution operations metrics show the optimized capability of meeting the performance requirements.

We applied both the entity-relationship approach and the normalization approach, as appropriate, to develop the evoBrix X 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, which enables easier maintainability. Normalization levels are lower on tables that are used to inquire and report on data to allow for faster query response. A subset of tables that is used heavily in both modification and inquiry required architectural design scrutiny. We used performance and volume testing and, more importantly, implementation experience, to reduce impacts to both functions. Team CNSI has conducted specific performance benchmark 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 re-work on the user interface and avoids additional background processes when changes are initiated, while still allowing for backward compatibility.

Physical Data Model Components

We built the evoBrix X platform using the Oracle RDBMS. The evoBrix X Physical Data Model includes the components shown in Figure 3.10.1-118.

Database Schema Component	Details
Subject Area	Logical grouping of tables to make business sense

Database Schema Component	Details
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
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 3.10.1-118. Database Schema Component. Details of components of the evoBrix X Core Claims 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 X Core Claims module includes multiple channels to access, query, and report against the transactional/archived data that resides in the evoBrix X solution database, including archived data external to the Operational Data Store (ODS). Team CNSI provides authorized users with access to archived data, within established data retention timeframes, so that they can query information and generate reports. All archival data is stored in a dedicated evoBrix X ODS database. Named users are created for approved State and business operations users in the evoBrix X ODS database and users have read only permission to that data. State users can also create intermediate derivative data in their own named user schemas.

As State users will maintain direct connectivity to the evoBrix X ODS database, they can query/report ODS data against any other external data source. The user's PC must have the Oracle database client in order to access data from evoBrix X ODS; connectivity between the PC and the ODS is encrypted using the AS-256 algorithm.

DM43

The Contractor shall demonstrate through data analysis that the implementation outcomes have been validated and are accurate.

We plan and perform data analysis and validation across various phases of the project starting from Development, SIT, UAT, and production implementation to ensure we validate outcomes as accurate. For data (files and file types) moved from the legacy system to Team CNSI's evoBrix X Core Claims module, we perform the following test process validations to ensure we track and measure implementation outcomes:

- Verify that all source data required to be moved into evoBrix X tables have been populated and are accounted for. This includes data loaded manually as well as data loaded through Extract-Transform-Load (ETL) data conversion jobs.

Verify that any data transformations, translations, and edits are 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 X has not been adversely impacted.

- Verify that the loaded data is accessible through evoBrix X. This testing may be done using the evoBrix X online application or, alternatively, through SQL queries of the evoBrix X 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 X. Note that not all data loaded into evoBrix X may be accessible through the graphic user interface (GUI). In such cases, queries are 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 X screens and validate that target data is correctly displayed.

DM44

The System shall maintain a snapshot of member eligibility and plan enrollment information (i.e., full audit history or equivalent capabilities) that existed at the time of claims/encounters/capitation adjudication or payment. All transactions, including the execution of database scripts, need to be recorded in the full audit history.

Team CNSI's evoBrix X Member Module maintains a snapshot of member eligibility and plan enrollment information (i.e., full audit history or equivalent capabilities) that existed at the time of claims/encounters/capitation adjudication or payments. The module stores applicable details received from multiple eligibility sources in the inbound batch files or through real-time web services.

Our solution tracks all transactions, including the execution of database scripts, needed to create a complete audit history. As such, we develop a complete history, which includes all manual actions, necessary to support auditing and future traceability purposes. Our solution also allows users to store and update complete member-related information, as shown in Figure 3.10.1-119.

Member level support data attribute category	High-level listing of the comprehensive set of attributes that support the management of MPATH Member data
Member Demographics	■ Name ■ Race ■ Date of Birth ■ SSN ■ Ethnicity ■ Gender ■ Spoken/Written Languages ■ Citizenship ■ Phone Number ■ Individual Income ■ Pregnancy Information ■ Death Information ■ Address information
Eligibility Information	■ Eligibility Source ■ Eligibility Attributes ■ Scope ■ Coverage ■ Program code ■ Recipient Aid Categories ■ MAGI Category ■ FPL percentage
Third Party Insurance information	Policy Details for both Medicare and Commercial: ■ Payer Name ■ Payer ID ■ Coverage Type ■ Group Number ■ Policy Number ■ Policy Holder ID

Member level support data attribute category	High-level listing of the comprehensive set of attributes that support the management of MPATH Member data
	■ Begin Date ■ End Date
Provider Assignments	■ Primary Care Provider Details ■ Restricted Provider Details
Benefit Plans	■ Current Benefit Plans ■ History of Benefit Plans
Managed Care Plans	■ Enrollment Indicator ■ Enrollment Type ■ Mandatory ■ Voluntary ■ Assigned Plan Identifier
Patient Pay Amounts	Patient Pay Amounts for: ■ Long Term Care Services ■ Inpatient Services

Figure 3.10.1-119. Member Level Data Attributes. evoBrix X manages member data across a broad range of data attributes.

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 standardizes 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 X 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 X 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 and Correspondence 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 X Core Claims module's accessor provides user communication through web-based and mobile-enabled portals (e.g., consumer portal and worker portal). The solution is modular by nature and rapid adoption to change is accommodated by versioning through the mediation layer.

DM47

The Contractor shall participate in ongoing data governance meetings as required by the Department.

Team CNSI applies established data management strategies as part of 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 operationalization of additional data elements and re-use of existing elements for different purposes is a typical aspect of shifting business models. Leveraging expertise from our successful approach for data governance in previous implementations, Team CNSI will also play an active part in ongoing data governance meetings as required by DPHHS to:

- Define Data Asset Owners: The initial step in the implementation of a data governance program involves defining the owners, stewards or custodians of the data assets in the enterprise. Team CNSI applies our existing best practices to establish clear guidelines regarding who is accountable for each aspect of the data, including accuracy, accessibility, consistency, completeness, and updates.
- Define Data Access Processes: The second step in the approach is to define the data management processes. Team CNSI documents processes concerning how data is stored, archived, backed up, and protected from mishaps, theft, or attacks.
- Define 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.

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 X Core Claims module's adaptability and extensibility capabilities enable DPHHS to add new and incremental data items from module components required by the ongoing component, product, or service integration. In addition, the module can 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 X 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 X solution is also scalable to accommodate any additional data elements introduced due to changes in existing processes, new functionalities, and new interfaces. The Core Claims 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 X Core Claims module team defines what those flex fields should store based on DPHHS CPM 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 re-use 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 3.10.1-120 shows a sample transactional entity, MBR_COST_SHARE, with a “numeric” flex-field (FLEX_FIELD_NMRC1) and the configuration of this flex field for storing a claim-utilized amount for one tenant and the re-use of that same flex-field for storing a pharmacy encounter used amount for another tenant or potentially store additional data elements for future expansion within the MPATH Medicaid enterprise.

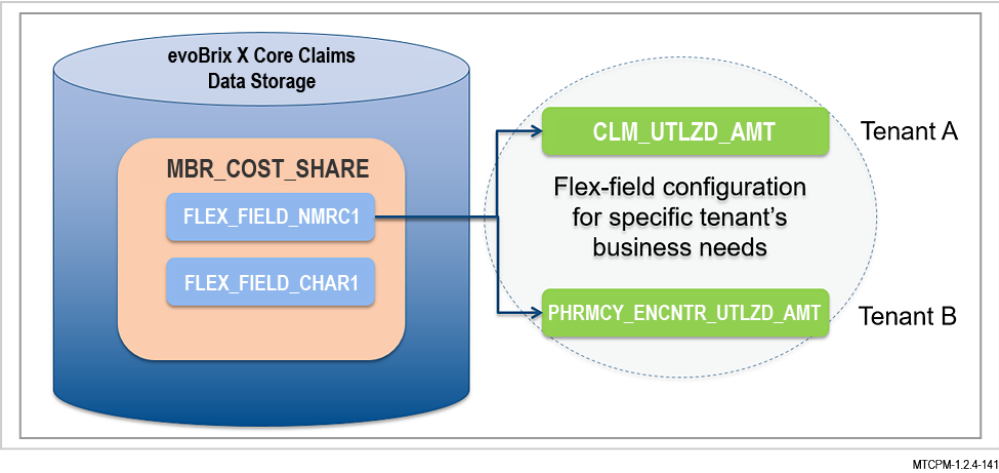


Figure 3.10.1-120. Support for Flex-fields. Team CNSI’s evoBrix X Core Claims module supports the use of flexible (flex) data fields to accept new and incremental data items from DPHHS module components without adversely affecting the operational system.

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 X Integrator Services offers batch and near real-time data trading of interfaces between the evoBrix X Core Claims module and the DPHHS-approved trading partners 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). The solution transfers Medicaid data required by State-approved trading partners for the successful implementation of the business needs based on defined roles. The solution supports inbound and outbound interfaces, service mediation, and pass-through (DB2DB) data exchange within evoBrix X 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 allows for current/future interfaces. The transactional data is sourced and made available to the evoBrix X Core Claims module data mart on a near real-time basis through evoBrix X Integrator Services. To reduce the management, technical stress, and the load on the evoBrix X data repository, data trading can be performed 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 3.10.1-121, Figure 3.10.1-122, Figure 3.10.1-123 and Figure 3.10.1-124 show sample evoBrix X Interface configuration screens, which detail the basic interface information, the interface transport details for exchanging the interface data to external systems, and interface run details.

Close

Transport Details

Schedule

Notifications

Dependencies

Interface ID:

1039.04b

Interface Name:

sendQHPOI89B

Description:

send QHP OI89 Disenroll Labels To MaximusB

Interface Type:

BATCH

Data Format:

Cobol Copy book

Modified By:

IntProcess

Modified On:

06/07/2017 16:32:19

Operational Flag:

Inactive

FTP Flag:

No Batch

Update

View History

Interface Run Info

Interface ID	Interface SID	Interface Run SID	Interface Name	Interface Status	FTP Status	Scheduled Start Time	Actual End Time	Total Records	Processed Records	Error Records
1039.04b	341	200020802	sendQHPOI89B	99		02/08/2017 14:35:00				0

Figure 3.10.1-121. Basic Interface Information Screen. Team CNSI’s evoBrix X ISR solution provides configurable screens to view the basic details of an interface.

MyInbox

Interface Options

Interface List

Interface Details

Interface Schedule

View History

Close

Schedule Information:

Frequency Name:

Monthly

Monthly Occurrence:

No

Yes

Monthly Day Number:

1

Schedule Date:

12/04/2009

Hour:

12

Min:

00

AM

PM

End Date:

12/31/1999

Error Count Percentage:

Modified By:

IntProcess

Modified Date:

11/30/2016 12:26:55

Parent Interface:

1027.01|Incarceration file

Update

Schedule An Interface Run:

Run Date:

Hour:

---SELECT---

Minute:

---SELECT---

AM

PM

Schedule

Figure 3.10.1-122. Interface Schedule Information Screen. Team CNSI’s evoBrix X ISR solution provides configurable screen to schedule the interface.

Response to: DPHHS-RFP-2020-0254T

Claims Processing and Management Services for Montana's Program for Automating and Transforming Healthcare (MPATH)

MyInbox > Interface Options > Interface List > Interface Details > Interface Transport Details

Close View History Update

Transport Detail:

FTP Directory:

FTP File Name: MV961@DCH0010

FTP Host Address: migrate.state.mt.us

FTP Port: 21

FTP User: JUNK

FTP Password:

Update

Local Directory: /1039-04b/output

Local File Name: Test.dat

Archive Directory: /1039-04b/archive

Archive File Name: 1039_04b.txt

Modified By: 116

Compression Type: NONE

Header Trailer Validation: F

Header Trailer Validation Type: 00

Header Length: 0

Trailer Length: 0

Header EDI Type:

Trailer EDI Type:

File Number Validation: 0

File Number: 0

EDI App:

EDI User:

Modified Date: 09/19/2017 10:01:20

Multiple Files: N

MTCPM-1.24-143

Figure 3.10.1-123. Interface Transport Details Screen. Team CNSI's evoBrix X ISR solution provides configurable screens to view the transport details of an interface to support the exchange of data with external systems within DPHHS.

MyInbox > Interface Options > Interface Run List

Close

Interface Run Info

Filter By

Go

Save Filters

My Filters

Interface ID	Interface SID	Interface Run SID	Interface Name	Interface Status	FTP Status	Scheduled Start Time	Actual End Time	Total Records	Processed Records	Error Records
2025	2025	200000013	CSHCS - Generate SYS_Financial Review	140		01/31/2012 18:00:00				0
2026	2026	200000014	CSHCS - Generate SYS_Medical Review	140		01/31/2012 04:00:00				0
2027	2027	200000015	CSHCS - Generate SYS_Financial/Medical Review	140		01/31/2012 18:30:00				0
2028	2028	200000016	CSHCS - SeeBeyond_NPI Mass Update	140		01/31/2012 00:00:00				0
2029	2029	200000017	CSHCS - Automated MHP Update	140		01/31/2012 20:00:00				0
1076.02	2006	200000106	Send New Medical Eligibility Determinations to Health Plans	99		10/24/2016 18:00:00				0
1076.03	2005	200000107	Send CSHCS Enrollees to Health Plans	140		10/24/2016 15:00:00	10/24/2016 16:06:24	3		3
1077.01	2001	200000109	Receive CSHCS Oracle Upload	99		10/24/2016 17:00:00	10/24/2016 18:04:28	0		1
2015	2015	200000111	CSHCS - Generate Balance_Due_Letter_2	140		10/24/2016 18:00:00	10/24/2016 18:09:59	0		0
2027	2027	200000601	CSHCS - Generate SYS_Financial/Medical Review	140		10/28/2016 15:53:00	10/28/2016 16:02:27	614		0

View Page: 2

Go

Page Count

SaveToXLS

Viewing Page: 1

First

Prev

Next

Last

MTCPM-1.24-144

Figure 3.10.1-124. Interface Run Details Screen. Team CNSI's evoBrix X 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.

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 uses the latest possible version of the Oracle database and associated tools to maintain responsibility for the backup and retention of data. 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.

The Oracle RMAN backup strategy is incremental in nature, thereby saving storage costs without compromising on recovery or recovery timelines. Team CNSI employs the following processes to perform 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 maintain the backup/restore performance and realize storage savings without compromising on 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 of BASIC, LOW, MEDIUM, and HIGH.

Team CNSI maintains the following SLAs, shown in Figure 3.10.1-125, 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 3.10.1-125. Backup and Retention Schedule. Team CNSI’s compliance to the State-mandated backup and retention schedule for the evoBrix X Core Claims module.

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 the archiving of pre-built and scheduled report outputs into IBM Cognos BI Content Store. Team CNSI’s evoBrix X Core Claims module maintains 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 the evoBrix X Core Claims module, can be configured per pre-defined retention policies.

DM60

The Contractor shall be responsible for data management including ensuring the architecture addresses data semantics, data harmonization, and shared-data ownership.

Team CNSI maintains responsibility for data management including ensuring the architecture addresses data semantics, data harmonization, and shared-data ownership. We designed the evoBrix X Core Claims module with a sound data design and provisioning strategy, as it is not only a key aspect for managing the current and future needs of DPHHS, but also one of the vital elements of an extensible, interoperable infrastructure. DPHHS’s MMIS system depends on varying datasets such as Provider, Eligibility,

Reference/Lookup, Claims, Payments, and TPL to manage the technical and operational needs of the existing system. In response, Team CNSI’s evoBrix X Core Claims module can 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 DPHHS’s existing Claims system to the new solution.

Team CNSI’s evoBrix X 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 includes 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 X Core Claims module 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 DPHHS’s vision of shared-data ownership.

DM61

The Contractor's solution shall collect and maintain the relevant data necessary to support the budget neutrality reporting requirements specified in the State's 1115 Waiver (including the ability to identify those Members who would be ineligible for Medicaid in the absence of the State's 1115 Waiver).

Team CNSI collects and maintains the relevant data necessary to support the budget neutrality reporting requirements specified in the State's 1115 Waiver (including the ability to identify those Members who would be ineligible for Medicaid in the absence of the State's 1115 Waiver). Team CNSI’s evoBrix X solution contains eligibility, benefits, and payment data for all State-defined programs which can be utilized/customized for the reporting requirements as per State agency needs.

The Benefits Administration Module is facilitated through a hierarchical structure and provides DPHHS with online configurable functionality to define service coverage information, cost share, service limit, and funding details for all types of benefit plans including waiver programs. Service coverage definitions can be specified at the elementary level, such as procedure code, or at a higher level, such as diagnosis code, taxonomy code, or a combination of code sets. The allowed code set categories include ICD diagnoses and procedures, HCPCS, procedure modifiers, revenue codes, bill types, places of service, provider taxonomy or specialty, claim type, revenue code, and provider type. The solution can also create a no-benefits benefit plan, which allows users to track members who would be ineligible for Medicaid in the absence of the State's 1115 Waiver using member eligibility attributes.

Team CNSI’s evoBrix X Core Claims module includes the functionality to configure and manage the account coding segments. Team CNSI can configure each segment to include multiple segment values and rules to derive the right segment value based on various claim attributes and derived elements. This allows users to define a more granular chart of accounts that enhances the audit fields for CMS-required reporting purposes. The solution captures and consolidates financial data for all demonstration projects to streamline reporting projections based on without waiver (WOW) and waiver enrollment data according to CMS budget neutrality requirements.

For example, the below screen shot (Figure 3.10.1-126) shows the Member Level Error Report with Habilitation Supports Waiver (HSW) Program Benefit Plan assignment processing errors with Medicaid Assistance (MA) is not available.

Report Date: 12/27/2019 8:00:02 AM		Member Level Error Report					
Transaction Source	DHS County	DHS District	RID/CIN	Fatal Error(s)	Warning Error(s)	Duplicate Matched ID	Error Records
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0001461595 20191101 20191130 170528
/ 1015 05				MA Not Active for member - HHO Cannot be Processed - Transaction Rejected			204092826 0027 0002382070 20191101 20191130 281356
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0002471518 20200101 20200131 281356
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0004051590 20200101 20200131 281356
/ 1015 05				Transaction contains Invalid Eligibility Dates - Transaction Rejected			204092826 0027 0004139040 20191101 20191130 281356
/ 1015 05				MA Not Active for member - HHO Cannot be Processed - Transaction Rejected			204092826 0027 0004367466 20200101 20200131 281356
/ 1015 05				MA Not Active for member - HHO Cannot be Processed - Transaction Rejected			204092826 0027 0004367466 20191101 20191130 281356
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0027 0004367466 20191101 20191130 281356
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0004558623 20200101 20200131 281356
/ 1015 05				MA Not Active for member - HHO Cannot be Processed - Transaction Rejected			204092826 0027 0004614849 20200101 20200131 281356
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0004652705 20200101 20200131 281356
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0004652705 20191201 20191231 281356
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0005046803 20200101 20200131 170528
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0005046803 20191201 20191231 170528
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0005046803 20191101 20191130 170528
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0005046803 20191001 20191031 170528
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0005119109 20191001 20191031 281356
/ 1015 05				MA Not Active for member - HHO Cannot be Processed - Transaction Rejected			204092826 0027 0005441808 20191101 20191130 281356
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0006117477 20191201 20191231 281356
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0006117477 20191101 20191130 281356
/ 1015 05				MA Not Active for member - HSWMC Cannot be Processed - Transaction Rejected			204092826 0045 0006117477 20200101 20200131 281356

MTCPM-1.2.4-675

Figure 3.10.1-126. Member Level Error Report. Team CNSI's evoBrix X Core Claims module supports generating Member Level Error Report with Habilitation Supports Waiver (HSW) Program Benefit Plan assignment errors with Medicaid Assistance (MA) is not available.

DM62

The Contractor's solution will ensure current and historical provider IDs are linked back to one universal/common identifier.

Team CNSI's evoBrix X Core Claims module ensures that a provider's historical and current identifiers are linked to a single master record (i.e., universal/common identifier). Even if multiple identifiers are associated with a provider, Team CNSI's evoBrix X Core Claims module retains the information under a single enrollment and a unique Provider Identifier (Provider ID) that is linked to the provider's NPI and TIN. Figure 3.10.1-127 shows the different identifiers tied to a unique provider ID that can be tracked through the evoBrix X Provider Identifier List screen.

Provider Identifier List						
Filter By		And	Filter By		And Operational Status	
					Active	
					Go	
					Save Filters	
					My Filters	
Identifier Type	Identifier Value	Start Date	End Date	Status	Operational Status	Inactivation Date
☐ Legacy Medicaid Provider ID	7938739	10/10/2016	12/31/2999	IN REVIEW	Active	
☐ Legacy Medicaid Provider ID	7938738	09/15/2014	12/31/2999	APPROVED	Active	
☐ Legacy Medicaid Provider Type	98	10/11/2013	12/31/2999	APPROVED	Active	
View Page: 1		Page Count		SaveToXLS		
		Viewing Page: 1		First		Last

MTCPM-1.2.4-145

Figure 3.10.1-127. Support for Multiple Provider IDs. Team CNSI's evoBrix X Core Claims module supports multiple alternative identifiers, both current and historical, to link all the records related to a provider identified via a unique evoBrix X 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 X Core Claims module assigns standardized unique internal identifiers for entities to prevent the creation of duplicate records. The module identifies, tracks, and reports individual providers across multiple application types. When multiple identifiers for the same provider are fed into

the system through various sources, the evoBrix X Core Claims module identifies the duplicates and ensures that there is always a unique set of active identifiers for a provider stored under a unique PI linked with the provider’s NPI and TIN.

Team CNSI’s evoBrix X Core Claims module performs the following validations to ensure data integrity before provider data is 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 NPPES.
- **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.

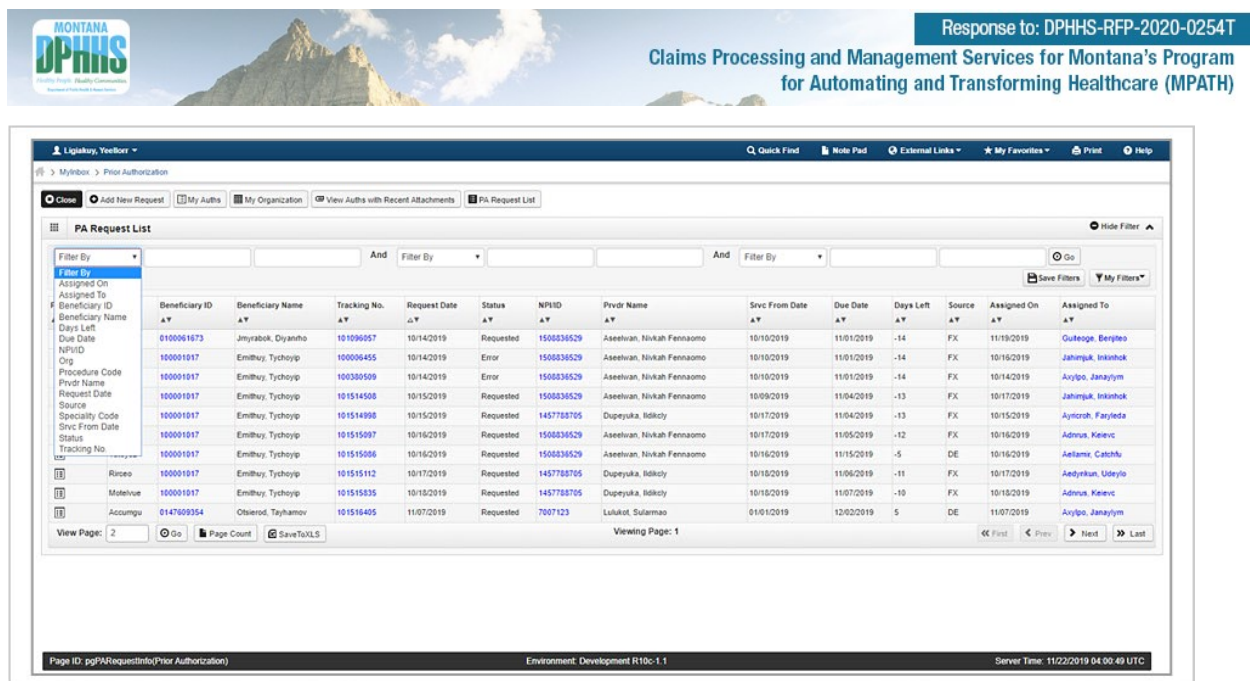
DM65

The Contractor's solution will provide service authorization search based on user defined criteria (e.g., provider name, provider ID, member name, member Medicaid ID number, date of submission range, dates of service requested range, service requested, status of the request).

Team CNSI’s evoBrix X Core Claims module application screens allow authorized users to search for service authorizations based on various user-defined criteria using applicable menu options. The search results are rendered through the “PA Request List” page. This page allows users to search using multiple user-defined criteria (e.g., provider name, provider ID, member name, member Medicaid ID number, service request status) to locate a specific service authorization record, or a group of authorization records sharing a common set of attributes (e.g., date of submission range, dates of service requested range, etc.).

The PA Request List page includes three primary filters, which can be customized by each user according to preference. The user can then save their favorite search criteria using the “Save Filters” option. This information can then be retrieved under the “My Filters” dropdown as needed. The retrieved results may be exported and saved to an Excel workbook for additional analysis using “Save to XLS” option.

Figure 3.10.1-128 shows a sample PA Request list page from Team CNSI’s evoBrix X solution with the various filter options to facilitate an enhanced search for business users.



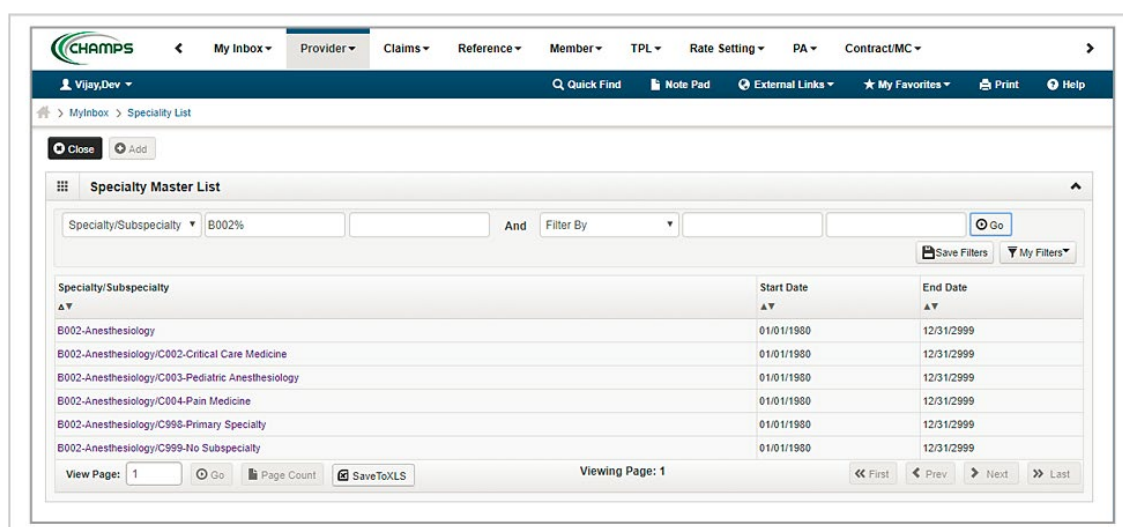
MTCPM-1.2.4-041

Figure 3.10.1-128. Prior Authorization (PA) Request List Page Showing Filter Capability. Team CNSI evoBrix X Core Claims solution screen highlights the three major filters, the Save Filters and My Filter retrievals, and Save to XLS features.

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.

The Team CNSI's evoBrix X Core Claims module maintains online access to all reference tables with an option to search and display by reference data type and code. The module can 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 3.10.1-129 shows the evoBrix X Core Claims module Specialty Master List application screen that provides support for searching specialties by code.



MTCPM-1.2.4-230

Figure 3.10.1-129. Provider Specialty Online Maintenance Screen. Team CNSI's evoBrix X Core Claims module 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 X Core Claims module uses a generic model framework referred to as Message Management Framework (MMF) to maintain and interact with the 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 the Core Claims module. 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 3.10.1-130 shows the nomenclature we use to drive the configuration of messages in the evoBrix X Core Claims module using the Message Management Framework.

Message Component	Description	User-Control option
Tenant Code	This is unique code assigned to each Tenant.	Cannot be configured
Message Type	The Unique code for the message type. The Message Type is built as follows: The messages are categorized as: (a) Application Message (AM) (b) Validation Message (VM) (c) Security Message (SEM) (d) System Message (SYM) These messages are further sub-categorized as: (1) Client Validation Message (CVM). (2) Business Validation Message (BVM). (3) Persistence Validation Message (PVM). (4) Data Validation Message (DVM). Examples for Unique message type code are: AM-CVM (Application Message - Client Validation Message (CVM)), AM-BVM (Application Message - Business Validation Message (BVM)), AM-PVM (Application Message - Persistence Validation Message (PVM)) and AM-DVM (Application Message - Data Validation Message (DVM)).	Configurable
Message Code	The Unique message code assigned to each message.	Configurable
Message Description	This holds the description of message.	Configurable

Figure 3.10.1-130. Message Management Framework (MMF) Components. This table shows various components of MMF with description and user-control options.

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

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).

Team CNSI's evoBrix X Core Claims module provides 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 of the module enables business users to 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 for users should they need to take corrective actions should it be invalid. For example, as stated, should a user enter a special character into an alphanumeric field, it is rejected by the screen and the user is 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 validates 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 then prompts the user for an action should it fail the data range check.

Figure 3.10.1-131 shows the evoBrix X Core Claims application screen that enforces comprehensive validation for data fields supporting alphanumeric data.

Provider ID: 7938738

Name: The Wellness Plan Medical Centers

Only AlphaNumeric values can be entered for Identifier Value. x

Add Identifier

Identifier Type: Previous CHAMPS Provider ID *

Identifier Value: PCPID001% *

Location: 01-The Wellness Plan Medical Centers *

Only AlphaNumeric values can be entered for Identifier Value. x

Notes:

Start Date: *

End Date:

Ok

Cancel

MTCPM-1.2.4-148

Figure 3.10.1-131. Data Validations for Alphanumeric Data Fields. Team CNSI's evoBrix X Core Claims module 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 X Core Claims module captures and maintains data items needed for State and federal reporting requirements. Our solution includes a pre-defined set of State-specific standard reports as part of the evoBrix X Core Claims module. Additionally, the evoBrix X Core Claims module includes an extensible reporting model comprised of a standard structured set of data elements as a part of Claims and Financial Reporting that is necessary to ensure system operations transparency. DPHHS can leverage the reporting model to configure scheduled or on-demand reports. It provides an enhanced self-service user experience through ad-hoc reports, according to the State or federal reporting requirements.

We can leverage our expertise with Transformed Medicaid Statistical Information System (T-MSIS) extracts and the related implementations in the states of Utah and Washington in support of the MPATH project. We can reduce the risk of meeting T-MSIS requirements as it applies to the data elements for core claims required for T-MSIS data extracts, which are sent to DPHHS for submission to CMS. The majority of the T-MSIS data elements can be directly mapped from the evoBrix X data model and, for any State-specific customizations, through configurable transformation rules that can be leveraged seamlessly while extracting the data.

DM74

The Contractor's solution shall validate calculated data items.

Team CNSI's evoBrix X Core Claims module leverages the generic data validation framework orchestrated through reusable components that applies to the various modes of accessing data (frontend, backend, interfaces, web services), which ensures that a consistent and streamlined outcome is produced to validate calculated data items. The evoBrix X solution employs different test cases to validate the accuracy of calculated fields. Various levels of testing are performed based on test cases to ensure 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 ensure all calculated field values are accurate.

Team CNSI's evoBrix X Core Claims module 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 users 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 is presented with a standardized message to take corrective action before any further calculations can be performed.

Team CNSI's evoBrix X Core Claims module comes with the feature to show how a claim is getting priced in a single page and includes the formula which is used to derive the claim pricing amount along with the breakup amounts used in the formula. This will be useful to validate the claim. The Figure 3.10.2-132 and Figure 3.10.1-133 are sample screens which shows the formula used for the calculations in Team CNSI's evoBrix X Core Claims module.

TCN : 311910710000004000 Claim Type : S - FQHC

Pricing Flow

Toggle All

☒ Computed Billed Amount

	Submitted Charges	130
	Other Payer Paid Amount	60
	Other Payer CARC Adjustment Amount	
Submitted Charges - (Other Payer Paid Amount + Other Payer CARC Adjustment Amount)	Computed Billed Amount	70

MTCPM-1.2.4-676

Figure 3.10.2-132. Claim Pricing – Computed Billed Amount. Team CNSI's evoBrix X Core Claims module screen that shows the formula used to calculate the Computed Billed Amount with breakup components.

TCN : 311910710000004000 Claim Type : S - FQHC

Pricing Flow

Toggle All

☒ Non Medicare Pricing

Line - 1

	Claim Line TCN	311910710000004001
	Payable Amount Before Deduction Of Non Medicare OI Amount	102.9
	Computed Line Billed Amount	110
	Non Medicare OI Paid Amount	50
Payable Amount Before Deduction Of Non Medicare OI Amount - Non Medicare OI Paid Amount	Payable Amount	52.900000000000006
Lesser Of Logic Between(Computed Billed Amount,Payable Amount)	Payable Amount	52.900000000000006

MTCPM-1.2.4-677

Figure 3.10.1-133. Claim Pricing – Non-Medicare Pricing. Team CNSI's evoBrix X Core Claims module screen that shows the formula used to calculate the Payable Amount with breakup components.

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 X Core Claims module validates that all data items that contain self-checking digits (e.g., National Provider Identifier [NPI]) pass a specified check-digit test. The module supports an interactive enrollment application that provides structured, online screens with a Business Process Wizard (BPW) for provider enrollment. The wizard guides the provider 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 3.10.1-134 shows the evoBrix X Core Claims application screen that validates the NPI and prompts the user to correct the value should the keyed-in value be of the wrong format or if it does not comply with the check-digit test.

Basic Information: Enter required fields and click Confirm button.

Please enter valid number in EIN/TIN.

Please enter valid number in NPI.

Basic Information

Legal Entity Name:

(As shown on the Income Tax Return)

Entity Business Name:

Robert Langdon Associates *

(Doing Business As)

EIN/TIN:

TIN001 *

Please enter valid number in EIN/TIN.

Organization/Business Type:

Medicaid *

Vendor ID:

VEN001 *

NPI:

NPI001 *

Please enter valid number in NPI.

Contact Email Address:

Email-1:

email@email.com *

Email-2:

Email-3:

Email-4:

Email-5:

Email-6:

Confirm

View Screening Result

Finish

Cancel

MTCPM-1.2.4-149

Figure 3.10.1-134. Validations for Fields with Check-digit Test. Team CNSI’s evoBrix X Core Claims module supports comprehensive check-digit validation for data fields such as NPI prompting users to take corrective action on the application screens.

The evoBrix X Core Claims module 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.

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 DPHHS business areas. Team CNSI’s integration framework is comprised of the following components to integrate the systems with other information systems leveraging the applicable Extract, Transform, and Load (ETL) processes, as needed:

- Batch Interfaces via ISR
- Web services via evoBrix X integrator

Batch Interfaces via ISR

Team CNSI’s evoBrix X ISR configurable solution supports automated data exchanges with DPHHS and DPHHS-approved agencies. The 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 X 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.

Following are key features of the ISR solution:

- Supports the data exchanges between DPHHS and DPHHS-approved trading partners by adding the required configurations.
- Handles all industry-standard file formats.
- Includes configurable interface schedules, validations, error thresholds, external agency details, and email alerts for DPHHS interfaces.
- Scales for growth in data volumes and transaction volumes seamlessly and takes advantage of the rich features of the underlying hardware and software resources.
- Built on a scalable and high available infrastructure.
- Includes robust error logging and auditing features. When processing DPHHS interfaces, errors are logged, and the details can be sent to approved email IDs for further correction.
- Supports modular approach through the plug and play of generic code. DPHHS-related interfaces can be configured easily.
- Handles large payloads with failover cluster.
- Enables seamless and simplified connectivity with external agencies using SFTP and SSL.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

DM114

The Contractor's solution shall use the most current version of clinical codes (e.g., ICD-10, HCPCS, CPT, ICD Surgical Procedure Codes, NDCs).

The evoBrix X Core Claims module uses the most current version of clinical codes (e.g., ICD-10, HCPCS, CPT, ICD Surgical Procedure Codes, NDCs). As part of the claim's adjudication process, our solution

validates all codes received on a claim. These codes are checked against the national standard code sets that are preloaded into the Benefits and Administration area in our base solution, evoBrix X. evoBrix X custom loads other flexible and variable rates and can support the contractual agreements between DPHHS and its partners. Our Core Claims module maintains NDC/HCPCS crosswalk drug files for J-Code quantity drug rebates, along with effective dates that are used in adjudication of J-code claims. The module accepts feeds from CMS and other approved sources on code sets. Major reference codes include:

- CPT4 procedure codes
- Modifiers
- ICD-10 Diagnosis and procedure codes
- DRG codes
- APC codes
- Revenue Codes
- HCPCS codes
- Revenue code/HCPCS relationships

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 X Core Claims module ensures that we collect, store, and maintain data required for T-MSIS reporting per CMS federal specifications. The evoBrix X system maintains T-MSIS valid values information in the data repository and creates a configurable cross-reference table between CMS and evoBrix X values. Any future modifications on T-MSIS data requirements can be easily handled by Team CNSI's configurable evoBrix X solution.

The majority of the T-MSIS data elements can be directly mapped from the evoBrix X Data Model and State-specific customizations through configurable transformation rules that are leveraged seamlessly while extracting the data. Wherever necessary, Team CNSI works 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 helps DPHHS build the crosswalks efficiently.

Team CNSI evoBrix X data model supports all provider segments (location and contact, licensing information, identifiers, taxonomy classification, Medicaid enrollment, and bed type information). Figure 3.10.1-135 shows the crosswalk for OWNERSHIP-CODE that we 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 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

State Valid Values		CMS T-MSIS Valid Values	
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 3.10.1-135. Sample Ownership Code T-MSIS Mapping. Team CNSI's evoBrix X Core Claims module supports the mapping of provider segments to facilitate CMS T-MSIS reporting.

DM138

The contractor shall participate in governance processes led by the Agency and including the System Integrator and other module vendors as appropriate during design, definition, and any subsequent revisions of data formats to be used for communicating data to and from the module.

Team CNSI will participate in DPHHS-lead governance processes with the MPATH System Integrator (Deloitte) and other module vendors as appropriate during design, definition, and any subsequent revisions of data formats to be used for communicating data to and from the Core Claims module. We apply established data management strategies to handle the complex set of systems and applications needed to interface and interoperate 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 due to the operationalization of additional data elements and re-use 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 DPHHS and assist you in:

- **Defining Data Asset Owners:** The initial step in the implementation of a data governance program involves defining the owners, stewards or custodians of the data assets in the enterprise. Team CNSI uses our 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 documents processes regarding how 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 over the life of the contract.

DM145

The Contractor's solution shall provide, implement, operate, and maintain a data modeling tool to develop and maintain comprehensive structural metadata data models for data processed by, stored in, or delivered for consumption from the solution for the duration of the Contract that includes the documentation and illustration of data elements, structures, and their relationships of the following:

- **Conceptual Data Model** - a graphical depiction of the conceptual data model for the solution that identifies data field names and relationships. Business process flows and data models (e.g., Entity Relationship Diagrams (ERD) and any other descriptive graphic document) of the entire system and all

modules and functions, showing all inputs, processes, programs, interfaces, program interrelationships, and outputs

- Logical Data Model - a graphical depiction of the logical data model for the solution that provides data field names, attributes and relationships, data tables, and primary key fields
- Physical Data Model - a graphical depiction of the physical data model for the solution that identifies data field names, attributes and relationships, data tables, and primary key fields. Unlike the conceptual and logical data models that use descriptive table and field names, the physical data model will reference actual table and field names used for coding.

Team CNSI provides, implements, operates, and maintains a data modeling tool to develop and maintain comprehensive structural metadata data models for data processed by, stored in, or delivered for consumption from the solution for the duration of the Contract that includes the documentation and illustration of data elements, structures, and their relationships of the following:

- Conceptual Data Model
- Logical Data Model
- Physical Data Model

Conceptual Data Model

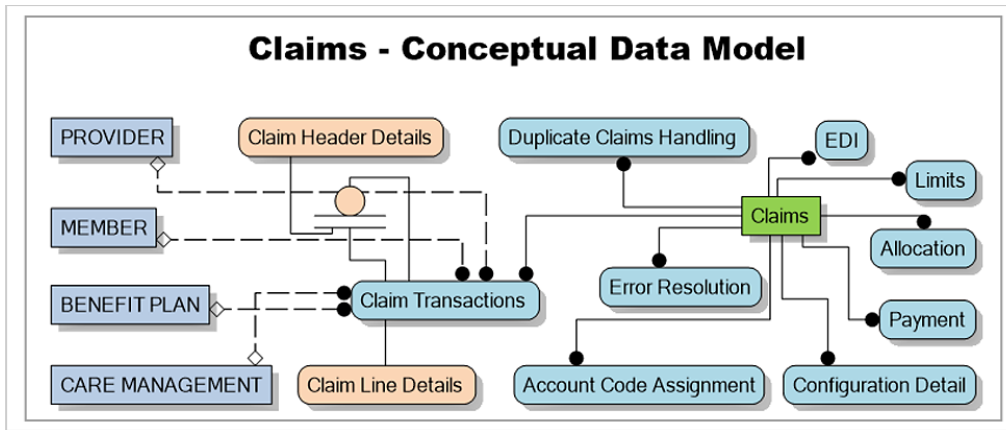
Team CNSI's evoBrix X Solution's Conceptual Data Model (CDM) depicts major business information objects in their relationships to each other, using business terminology. The CDM provides a mechanism to ensure completeness of the business model and enables reengineering of the State's Medicaid business processes. The evoBrix X Solution employs the conceptual data model for all business areas of the State Medicaid System. The CDM helps DPHHS understand the layout of data from different sources within the evoBrix X Solution. Figure 3.10.1-136 shows an example of the CDM.

The conceptual data model forms the base upon which the logical data model is designed. It depicts various business processes of the Medicaid system at a high level. The evoBrix X CDM is classified into different subsystems that form the building blocks of the evoBrix X solution.

Team CNSI's evoBrix X Solution's conceptual data model is designed based upon the Entity-Relationship Diagram (ERD) method of designing CDMs. The model consists of a core process that forms the crux of the subsystem surrounded by the various key supporting processes.

Team CNSI's evoBrix X Solution's Conceptual Data Model includes the following components:

- Subject Area – Logical grouping of business processes based on functional specifications
- Core Business Process – The core business process defines the chief functionality of the subsystem.
- Sub-Process– A sub-process is any key process that supports the core business process.



MTCPM-1.2.4-133

Figure 3.10.1-136. Conceptual Data Model. A sample of Conceptual Data Model from Team CNSI's evoBrix X Solution.

Logical Data Model

Team CNSI's evoBrix X solution's Logical Data Model (LDM) provides the mechanism to ensure the completeness of the business model and serves as a tool that enables the re-engineering of the State's Medicaid business processes. The model logically groups all these business areas into one product. It also evolved over multiple versions and represents universal data needs across multiple states.

The logical data model is a detailed pictorial representation of various functional requirements independent of database management systems. It provides in-depth details of various entities and attributes irrespective of how they are implemented in the backend. The LDM provides the following benefits:

- A focus on the data that comprises the organizational rather than individual business processes.
- Facilitation of business-focused data analysis.
- Aid in understanding enterprise-wide standardized business rule definitions and business data usage as well as help in uncovering existing data defects.
- A basis for performing data integration and harmonization.
- Improved data quality.

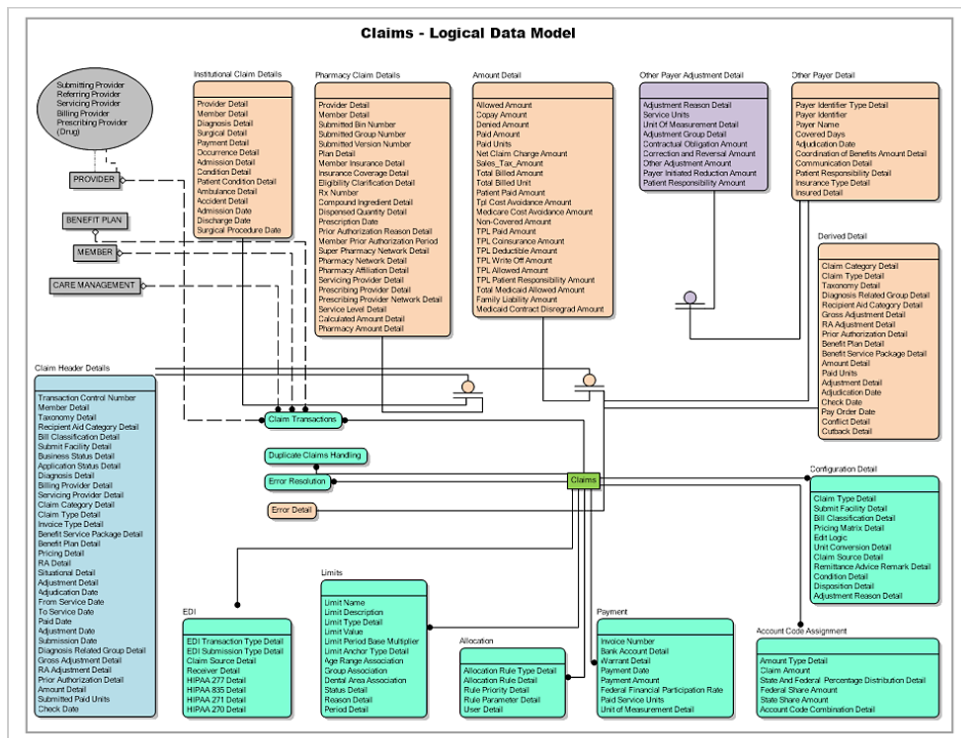
Components of Logical Data Model:

- Class – A class represents a person, place, thing, organization, event, or concept of interest to the Medicaid Enterprise. It is an object (or concept) to store information. In general, a class will have the following characteristics:
 - A stereotype allowing an extension of the UML vocabulary with specific properties, e.g., “Organization” contains the id, name, address, website, email, and Tax ID attributes.
 - One or more attributes that distinguish between individual occurrences of that entity.
 - At least one relationship to another entity.
- Class Properties
- General – General Information includes the name of the class and visibility.
- Attributes – An attribute is an item of data, a fact, or a single piece of information about an entity (e.g., the attribute Member Birth Date provides information about the entity member). An attribute will have the following characteristics:
 - Identified by name containing the visibility, data type, default value, and multiplicity, i.e., many (*), zero or one (0.1), one (1), at least one or more (1*). Multiplicity indicates the number of occurrences and whether the attribute is an optional or required element.

- Defined using clear, precise, and unambiguous language that identifies and distinguishes them from any other actual or possible item.
 - Specific stereotypes, constraints, and relationships.
 - Relationships – Relationships depict the business requirements joining two entities and traces the interaction between the entities in either direction.
 - Documentation – The documentation should contain definitions that are clear, precise, and unambiguous and use examples or exclusions as needed to improve clarity.
- Domains – The human-friendly computer hostnames translated into IP addresses where the system stores a specified entity or attribute.
 - Related Standards – The industry agreed-upon rules applied to the entity or attribute.
 - Entity-Relationship Diagram (ERD) – Entity-relationship diagramming is the method that produces a formal, graphical depiction of the model. It includes classification or super classes, common classes, common data types, common vocabulary, input messages, and output messages.

The objective of the LDM is to have a fully attributed and normalized data model as given in Figure 3.10.1-137 below. Additionally, data organization rules (known as Normalization) also apply to the data model in order to:

- Minimize duplication
- Ensure precise capture of standardized business rule definitions
- Prevent loss of information
- Aid in model management



MTCPM-1.2.4-137

Figure 3.10.1-137. Logical Data Model. A sample of Logical Data Model from Team CNSI's evoBrix X solution.

Physical Data Model

The evoBrix X solution's physical data model (as shown in Figure 3.10.1-138) addresses data needs of enterprise-wide Medicaid operations. Our solution includes the physical data model for all business areas

of a Medicaid System (e.g., Provider Management System, Member Management System, Claims and Encounters Loading/Processing/Adjudication/Pricing, Prior Authorization, etc.). It is a stable and proven data model that evolved over multiple versions and encompasses best practices learned from MMIS implementations across multiple states.

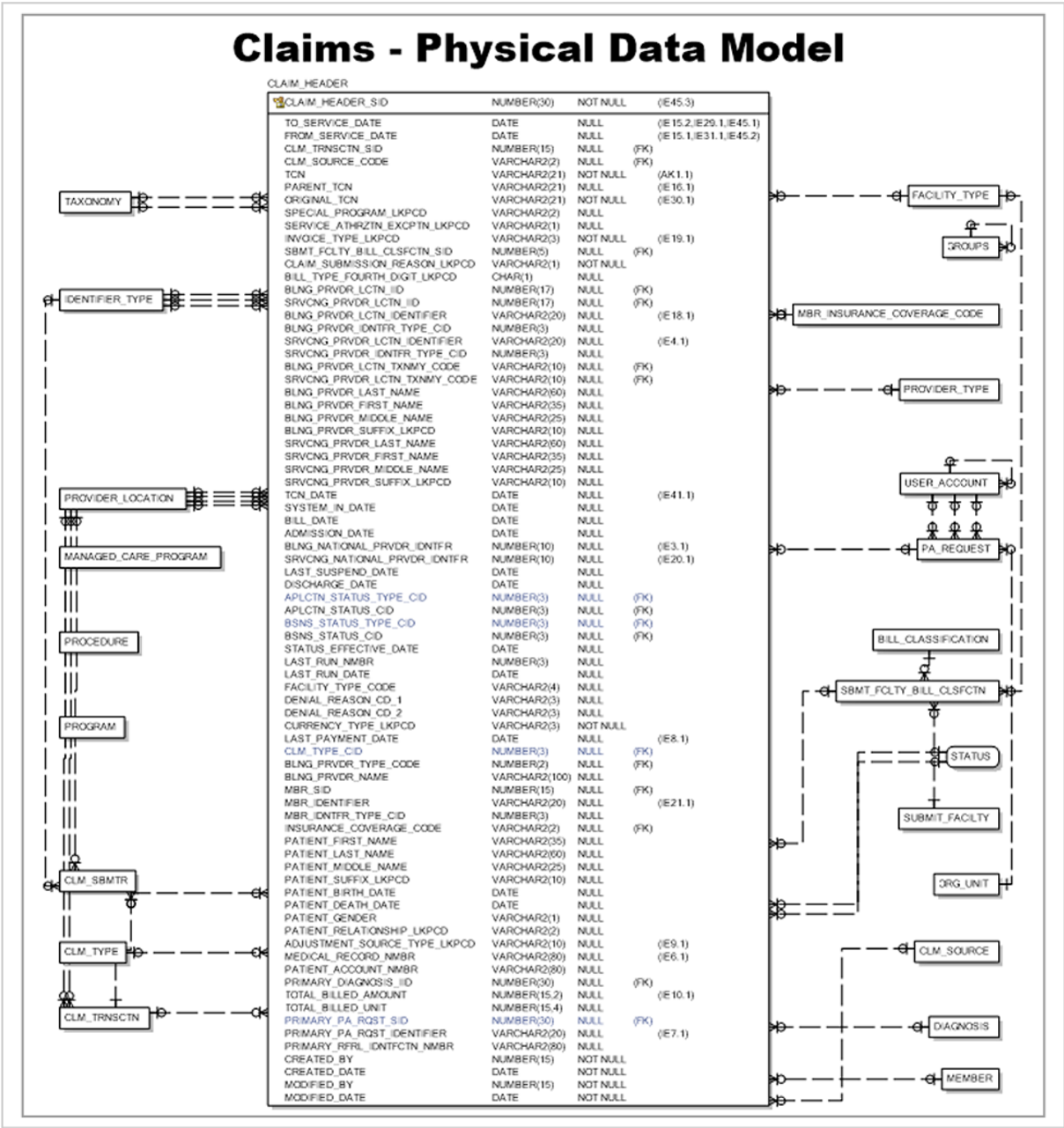


Figure 3.10.1-138. Physical Data Model. A sample of Physical Data Model from Team CNSI's evoBrix X solution.

Our solution’s 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.

We applied both the entity-relationship approach and the normalization approach, as appropriate, to develop the evoBrix X database. For example, we applied entity-relationship modeling in the design of the Reference business area data structures, whereas we applied the normalization technique on transactional data structures in the Claims and Prior Authorization (PA) business areas. The degree of normalization also varies. We use higher normalization in case of tables that are frequently modified by either inserts or updates, which enables 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 benchmark testing to determine the throughput of the system and has fine-tuned the data models for optimal performance based on the results. The proposed data model is currently operational in the states of Washington and Michigan in addition to being re-engineered to be multi-tenant compliant for the upcoming and future tenants onboarding the Cloud.

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 flex fields (flexible 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.

The evoBrix X Physical Data Model includes the following components:

- 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 in the column.
- 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 that data stored in it. NOT NULL constraint, Check Constraint etc. are some examples of column constraints.

DM139

The Contractor shall provide the capability to exchange data in standard and non-standard formats as well as structured and unstructured data with multiple sources.

The proposed evoBrix X Core Claims solution includes functionality to exchange data in standard and non-standard formats as well as structured and unstructured data with multiple sources. The solution uses the following key interoperability capabilities to exchange the data:

- SOA/Standards-based integration approaches using protocols including REST, SOAP, and supporting application APIs. (COTS)
- 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 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.
- 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.

[REDACTED]

- [REDACTED]
 - [REDACTED]
 - [REDACTED]

- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

DM140

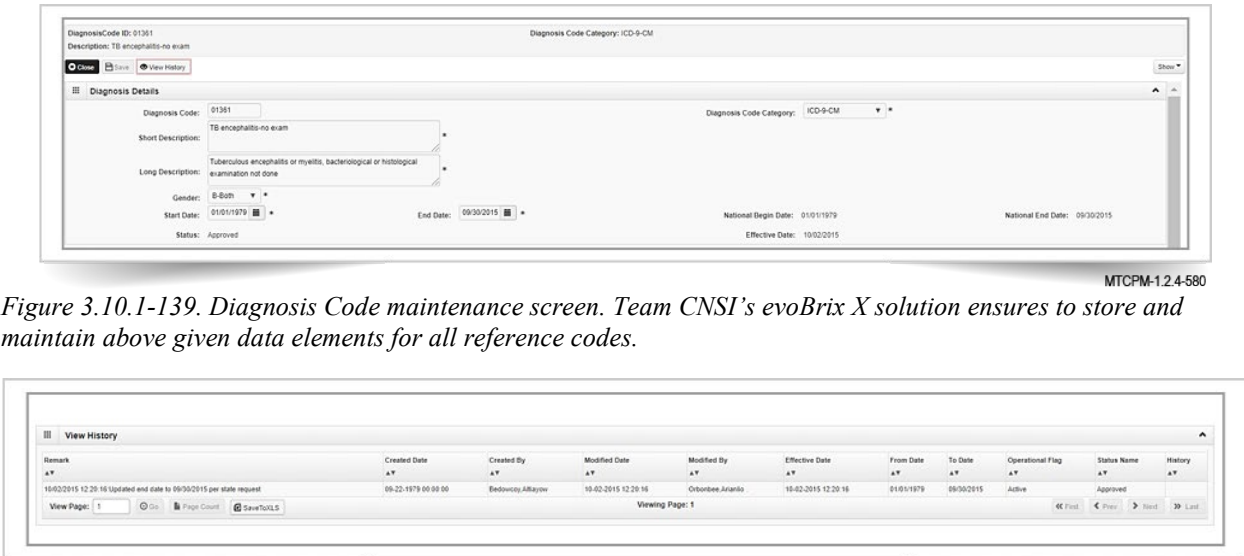
For audit and reporting purposes, the system shall provide and maintain the following data for all reference codes:

- a. Effective date
- b. End date
- c. Date when last changed
- d. Who made last change
- e. Short description
- f. Long description
- g. Create date
- h. Create user

Team CNSI’s evoBrix X Core Claims module maintains a complete audit trail of changes made to any data stored in the system, including 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 X Core Claims module begins 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 a user made the last change to the system
- Modified By: User ID of the person or system acting on the change
- Date Created: The date a user created an entry
- Created By: User ID of the person or system creating an entry
- 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

Figure 3.10.1-139 and Figure 3.10.1-140 show a Sample Audit trail of changes made to the data stored in the system.



DM141

The Contractor shall provide real-time access to transactional data (e.g., detailed data for member, provider, claims, and claims-related functions) for all module components).

Team CNSI’s evoBrix X Core Claims module allows authorized users to access, view, manage, and maintain real-time transactional data (e.g., detailed data for member, provider, claims, and claims-related functions) through online screens in real time. The solution also maintains a complete audit trail of changes made to any transactional data stored in the Core Claims data mart.

DM142

The Contractor's solution shall provide the ability to modify transactions (e.g., updates to reference information, member demographics and eligibility, provider information, service authorization details and amount used, TPL information) in real-time

Team CNSI's evoBrix X Core Claims module allows users to modify transactions (e.g., updates to reference information, member demographics and eligibility, provider information, service authorization details and amount used, TPL information) in real time. The module's 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 with the generation of appropriate audit trails for full traceability and audit compliance. They also allow for configuration of features for a personalized user experience.

Team CNSI's evoBrix X Core Claims module 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 to handle 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 business operations users. End users have easy access to data and a complete view of all their interactions with the system and operations staff on a real-time basis; the solution also allows them to modify transactions in real-time to meet the operational and workflow requirements of the evoBrix X Core Claims module to achieve contractual service levels.

The evoBrix X system, with its SOA-based integration engine, seamlessly integrates data from other systems, external agencies, and business partners in the DPHHS enterprise environment. The Provider Enrollment and the broader Core Claims modules enable DPHHS to manage the business processes for provider enrollment and balance it with real-time data access and support. The evoBrix X 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.

DM143

The Contractor's solution shall capture, maintain, and link relevant information (e.g., member and provider) associated with the claim (for all claims) during the adjudication process for the claim date of service.

Team CNSI's evoBrix X Core Claims module captures, maintains, and links relevant information (e.g., member and provider) associated with a claim (for all claims) during the adjudication process for the claim date of service. The module provides an effective member-centric repository containing comprehensive information about members/providers, including their demographic, financial, socio-economic, and health status information.

The repository includes eligibility, enrollment spans, eligible benefit plans/services, member payments, cost sharing, spend-down, and third-party insurance information. The evoBrix X Core Claims module also provides flexible administration of benefit plan assignment rules to allow members to enroll in multiple benefit plans based on their eligibility. Our solution ensures consistent, accurate, efficient, and faster access to data in real-time, batch mode, and manual processes for additions/updates of demographics, eligibility, and enrollment information. The member and provider data are used during the adjudication process based on the date of service and includes the appropriate edits Figure 3.10.1-141, Figure 3.10.1-142, and Figure 3.10.1-143 show the details as to how the claims information and the associated / linked provider and member details are accessible from the evoBrix X application screens.



MONTANA DPHHS
Healthy People. Healthy Communities.
Transforming Healthcare.

Response to: DPHHS-RFP-2020-0254T

Claims Processing and Management Services for Montana's Program for Automating and Transforming Healthcare (MPATH)

Print Help
Header TCN: 311900110138573000
Beneficiary ID: 1589061467
Name: [REDACTED]
Show

Errors to Resolve

TCN	Error Code	Error Description	Disposition	Forfeible	Suspended Date	Erroneous Date	Assigned to/Denied by	Assigned Date/Closed Date
311900110138573000	1387	DATE/NAME BILLING PROVIDER TYPE FAILED	Ignore	Y				
311900110138573000	8034	HEADER BILLING ZIP CODE IS INVALID	Pay and Report	Y		4/10/2143		
311900110138573000	8111	Primary Care Rate Increase Payment Made	Pay and Report	Y				

View Page: 1
Page Count: 3
Save/URLS

Header Details

TCN: 311900110138573000

Original TCN: [REDACTED]

No of Lines: 1

Related Cases: NO

Beneficiary ID: [REDACTED]

Gender: M-Male

Patient Account Number: 436962V16197

Place of Service: 31-Skilled Nursing Facility

Other Insurance

Billing Provider ID: 1589061467 Type: NPI

Billing Provider Taxonomy: 1043351366 Type: NPI

Referring Provider ID: 267Q0380X Type: [REDACTED]

Supervising Provider ID: [REDACTED] Type: [REDACTED]

Auth R: [REDACTED]

Diagnosis Codes: 1: F32 2: 6789 3: F03.1 4: F01.1

5: [REDACTED] 6: [REDACTED] 7: [REDACTED] 8: [REDACTED]

Delay Reason Code: [REDACTED]

Submitted Charges: \$123.00

Warrent/EFT Number: 201901071K

Claim Type: J-Professional

Adjustment Source: [REDACTED]

Medicare: N

Source: MIRA

Claim Status: Paid

Commercial: N

Last Name: [REDACTED]

DOB: [REDACTED]

Admit Date: [REDACTED]

First Name: [REDACTED]

Age: 61

Pay To Provider ID: 1589061467 Type: NPI

Vendor ID: CV0010774

Referring Provider ID: [REDACTED] Type: [REDACTED]

Primary Care Referring Provider ID: [REDACTED] Type: [REDACTED]

Referral R: [REDACTED]

CLM Number: [REDACTED]

Diagnosis Code Category: ICD-10-CM

Bill Amount: \$123.00

Approved Amount: \$51.70

SA Number: 78631791

Pay Cycle Date: 2019-01-09

Cancel

MTCPM-1.2.4-501

Figure 3.10.1-141. Claims Information. Team CNSI evoBrix X Core Claims capture and maintain Claims information.

Print Help
Member ID: [REDACTED]
Name: [REDACTED]
Show

MHP PCP: N
BMP Restrictions: N
Other Insurance: N
Managed Care: E
Program Type: MA
Health Card: Y
C/SMS Restrictions: N
INDICATORS: Y

Demographic Detail

Name: [REDACTED] Race: 1-Non-Migrant White, not of Hispanic Origin Date of Birth: 07/30/1957

SSN: [REDACTED] Ethnicity: N-Non Hispanic Age: 62

SSN Validation: [REDACTED] Citizenship: A-U.S. Citizen Gender: M-Male

Spoken Language: E-English Recipient Program Type Code: 0-No other code applies Case Program Type Code: 0

Written Language: [REDACTED] Phone Number: [REDACTED] Parent: N

Case Email: [REDACTED] Individual Income: 0 Group Composition: 1

Verification Type: [REDACTED] Plan Selection: [REDACTED]

Other Details

MA Case Number: 120879757 Unique Identifier Code (URC): [REDACTED] Eligibility Status: 0-Not Eligible for FFP or MA

County of Residence: 01-VALSHTENURY RAMA Person Code: 00 ABRN Person Code: 02

County of Assistance: 01-VALSHTENURY MCHHS County Phone Number: (734) 481-2000 Date of Death: [REDACTED]

MBS Code: 00 Death Cert Number: [REDACTED] Death Indicator: [REDACTED]

Pregnancy: 0-Not Pregnant Pregnancy Due Date: [REDACTED] Number of Expected Births: 0

Pregnancy End Date: [REDACTED] Native American Premium Exempt Flag: N Worker Orit Load Number: 206067

Negative Action Date: [REDACTED] Native American Cost Share Exempt Flag: N MMP Opt Out Flag: [REDACTED]

Part D Opt Out Flag: [REDACTED] Redetermination Date: 04/30/2019 ICD Opt Out Flag: [REDACTED]

ICD Source: [REDACTED] Last CMS Transaction Number: 5119214316 Last Modified Date: 04/30/2015

Last Modified By: MA

Member Address

Eligibility Source	Address Type	Name	Third Party Type Code	Address	Start Date	End Date
MA	Case	[REDACTED]	0	[REDACTED]	04/04/2016	12/31/2099
MA	Case	[REDACTED]	0	[REDACTED]	06/12/2016	04/30/2018
MA	Case	[REDACTED]	0	[REDACTED]	04/29/2016	06/11/2016

Cancel

MTCPM-1.2.4-502

Figure 3.10.1-142. Member Details of the Claim. Team CNSI evoBrix X Core Claims module captures, maintains, and links relevant member information associated with the claim during adjudication process.



MONTANA DPHHS
Healthy People. Healthy Communities.
Transforming Healthcare.

Response to: DPHHS-RFP-2020-0254T

Claims Processing and Management Services for Montana's Program for Automating and Transforming Healthcare (MPATH)

Print Help
Name: [Redacted]
Show

Provider Details

Legal Entity Name: [Redacted] (As shown on the Income Tax Return)

Entity Business Name: [Redacted] (Doing Business As)

EIN/TIN: [Redacted]

NPI: [Redacted]

Business Status: Active

Status: Approved

Business Elig Date Range: 12/11/2017-12/31/2099

Renewal Period: 10/1/2022-12/31/2022

Vendor ID: CV918774

Contact Email Address:

Email 1: [Redacted]	Email 2: [Redacted]
Email 3: [Redacted]	Email 4: [Redacted]
Email 5: [Redacted]	Email 6: [Redacted]

Filter By: [Dropdown] [Clear]

Status	Start Date	End Date
APPROVED	12/11/2017	12/31/2099

View Page: 1 [Dropdown] [Page Count] [Save Filter]

Viewing Page: 1

[Print](#) [Refresh](#) [Next](#) [Last](#)

Page ID: ppProviderGeneralProvider

MTCPM-1.2.4-503

Figure 3.10.1-143. Provider Details of the Claim. Team CNSI evoBrix X Core Claims module captures, maintains, and links relevant Provider information associated with the claim during adjudication process.

DM144

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.

In addition, the following exceptions apply to the data retention limitations: once in a lifetime events, active SURS or TPL cases, future TPL case (e.g., members over 55 years of age that have ever been in a nursing home), drug rebates, and service frequency limits as defined by the Agency.

Team CNSI's evoBrix X Core Claims module is part of the transactional system that supports the storage of the converted/ongoing operational data. Typically, transactional systems include a defined data retention policy that is established once the target system goes live. As required, after implementation, Team CNSI retains seven years of electronically imaged documents and data. After seven years, the data is purged (deleted) from the Core Claims module. We retain 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 previous seven years. We do not retain any entity and/or case that has been continuously inactive for the previous seven years; that information is purged and is no longer accessible by users.

Team CNSI adheres to data retention limitations/requirements provided by DPHHS, including the following exceptions: once in a lifetime events; active SURS or TPL cases; future TPL case (e.g., Members over 55 years of age that have ever been in a nursing home); drug rebates; and service frequency limits as defined by DPHHS.

Team CNSI complies with the DPHHS-defined retention policy. However, it is important to note that our evoBrix X Core Claims module can exceed the data retention requirements of the RFP.

Our data retention policy provides for the systematic review, retention, and destruction of electronic documents/data received or created by evoBrix X solution in connection with the business transactions of the evoBrix X system. This policy covers all records and electronic documents, contains guidelines for how long certain documents should be kept, and how records should be destroyed. The policy is designed to promote storage efficiency while meeting business and audit data retention requirements. Team CNSI developed the data retention timeframes and purge processes based on business and audit requirements.

We considered business needs, data volumes, and type of data. The CNSI Operations Team is responsible for ensuring data is retained and purged in accordance with policy.

Recommended Retention Policy

Team CNSI Operations Team follows the retention and purge procedures outlined in Figure 3.10.1-144, which covers the following information:

- S# - This is a sequence number.
- Title – This is a functional description of the data.
- Data Source Type – This represents how data is stored in the system. Values include:
 - DB Data - for data stored in the database and
 - File (XML) – for data stored in XML file format
 - File (Flat) – for data stored in raw data file format
 - File (PDF) – for data stored in Adobe Portable Document File (PDF) format
- Retention Requirement – This represents how long the data remains active in the evoBrix X CPMS Solution prior to purge.
- Purge Period – When the data will be purged after the retention requirement has be met.
- Purge Method – Right now – only physical delete is listed. Physical delete means that the data is permanently erased from storage. At some point in the future, additional purge methods may be added.
- Archival Method – If there is an archival requirement for the data, the method is listed in this column.

S#	Title	Data Source Type	Retention Requirement	Purge Period	Purge Method	Archival Method
1	Benefits Administration	DB Data	Indefinite	N/A	N/A	N/A
2	evoBrix X Letters	File (PDF)	90 Days	Monthly (During outage)	Physical Delete	Available in evoBrix X ECM (FileNet)
3	COGNOS - Scheduled Report	DB Data	6 months	End of the calendar year	Physical Delete	Available in evoBrix X ECM (FileNet)
4	CRM Data	DB Data	7 Years of data	Daily	Physical Delete	N/A
5	Data Warehouse Outbound	File (Flat)	1 Year	End of the calendar year	Physical Delete	Available in MPATH EDW
6	EDI (HIPAA Transaction) Files	File (XML)	6 months	Monthly (During outage)	Physical Delete	Available in evoBrix X ECM (FileNet)
7	Eligibility/TPL Info	DB Data	7 Years of data	End of the calendar year	Physical Delete	Available in MPATH EDW
8	Encounters	DB Data	3 Years of data	End of each fiscal year	Physical Delete	Available in MPATH EDW
9	FFS Claims	DB Data	3 Years of data	End of each fiscal year	Physical Delete	Available in MPATH EDW
10	Interface Audit	DB Data	7 Years of data	End of the calendar year	Physical Delete	N/A
11	Interface Inbound	File (Flat)	7 Years	End of the calendar year	Physical Delete	N/A

S#	Title	Data Source Type	Retention Requirement	Purge Period	Purge Method	Archival Method
12	Interface Outbound	File (Flat)	7 Years	End of the calendar year	Physical Delete	N/A
13	Managed Care (Capitation Payments)	DB Data	3 Years of data	End of each fiscal year	Physical Delete	Available in MPATH EDW
14	Managed Care (Contract Definitions)	DB Data	Indefinite	N/A	N/A	N/A
15	Oracle Financials	DB Data	Indefinite	N/A	N/A	N/A
16	Prior Authorization	DB Data	7 Years of data	End of the calendar year	Physical Delete	Available in MPATH EDW
17	Provider Enrollment (Staging tables)	DB Data	7 Years of data	End of the calendar year	Physical Delete	N/A
18	Provider Enrollment (Maintenance tables)	DB Data	10 Years of data	End of the calendar year	Physical Delete	N/A
19	PCS screening tables	DB Data	10 Years of data	End of the calendar year	Physical Delete	N/A
20	User Audit	DB Data	3 Months of data	Monthly (During outage)	Physical Delete	N/A

Figure 3.10.1-144. Policy Definition by Functional Area and Type of Data. Team CNSI Operations Team follows the retention and purge procedures outlined in the table that can configured to meet or exceed MPATH's business needs.

3.10.1.6 Interfaces

This section addresses interface requirements. 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 their response, the Offeror must describe methods they currently use for electronic data exchange, detail the industry standard formats currently used and describe any proprietary formats used. The Offeror must also describe in detail their approach to meet each of the interface requirements in Attachment F – Requirements Response Matrix. The Contractor's solution shall include all integrations/interfaces listed in Attachment F - Requirements Response Matrix in their overall fixed price. The Offeror simply repeating the RFP requirements does not qualify as a good response as defined in Section 6.1.1 of this RFP

A resilient integration strategy enables efficient, secure, and scalable transmittal of data, and consolidation of different disparate systems as the core of Montana Core Claims Module. Team CNSI's solution includes an Integration Gateway that enables interfaces through Application Programming Interface (API), EDI, and our configurable Interface Service Repository (ISR) solution.

[REDACTED]

The Team CNSI Advantage

Team CNSI's Integration Gateway provides a flexible, resilient, and standards-based interfaces solution that has been proven in multiple states.

- Flexibility to support for secure discrete and batch interfaces
- Data-driven configuration of interface schedules, error thresholds, validations, email alerts, and robust error logging auditing features.
- Code reusability promotes faster integration
- Capacity to handle large payloads with failover cluster and end-to-end monitoring

MTCPM-1.2.4-250

[REDACTED]

[REDACTED]

[REDACTED]

Figure 3.10.1-145. evoBrix X Integration Gateway. Team CNSI's solution provides a resilient and flexible platform for data exchanges and to support industry file formats with external agencies.

[illegible]

Interfaces Features

Managing File Exchanges through Configuration Changes

o 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 Integration Gateway is based on a modular and scalable framework for resiliency and extensibility for future integrations.

Alignment to Industry Standards

Team CNSI participates in MITA, HL7 standards, and other standards-related forums to promote and adopt standards. The evoBrix X platform is aligned with 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 standard
- Interoperability Standards
 - Service endpoint definition using WADL
 - 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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

[REDACTED]

INR01

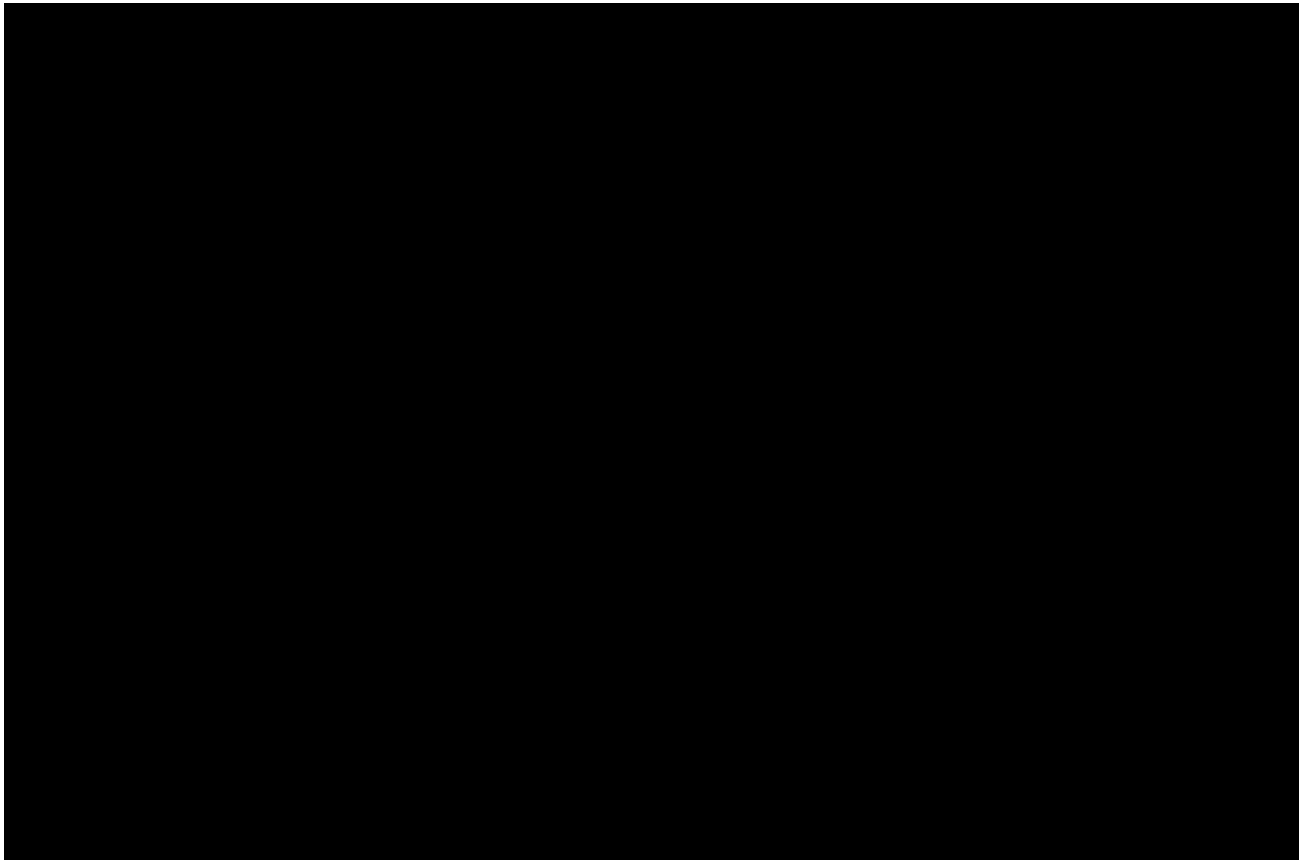
The Contractor's solution must ensure that all data exchanges including inbound and outbound interfaces shall comply with industry standards (e.g., National Information Exchange Model (NIEM), National Institute of Standards and Technology (NIST), HIPAA-compliance standards, Health level 7 (HL7), Fast Healthcare Interoperability Resources (FHIR)).

Team CNSI's evoBrix X Integration Gateway complies with applicable HIPAA and NIST standards 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. The Integration Gateway leverages Oracle SOA suite built-in adapters that comply with industry standards to process inbound and outbound interfaces.

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.

The Integration Gateway is used to connect 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 Integration Gateway 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 Core Claims Processing interfaces within timeframes as shown in Figure 3.10.1-147.



Our solution conducts 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.



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 X Integration Gateway provides an archival capability for the interface files that meets DPHHS requirements. The Integration Gateway manages multiple directories such as working, temporary, error, and completion. Files are moved to the completion directory upon successful execution; if there are any errors, files are moved to the error directory. Interface files are viewed from this directory for a configurable period depending on the requirements by DPHHS. The ISR archival process will be configured to keep raw daily files for 60 calendar days. The files can be archived, with an offsite vendor determined retention period, to the secure location up to six (6) months. Team CNSI will work with DPHHS on the archival intervals to view the raw data and archive the raw files to a 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.

The Integration Gateway 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.

INR08

The Contractor's solution shall include a process and toolset to maintain interfaces, code, and data models.

Team CNSI maintains SharePoint as online repository to store all the interface related ICD templates, design documents (DSDD) which contains 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 Oracle SOA Suite tool to support interoperability, code, and data transfer, and uses robust version control mechanism to store the code and any data objects related to data model. Team CNSI uses Subversion as the version control tool for the code changes, and erwin for managing the 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.

As a part of our solution configuration methodology, Team CNSI will develop ICDs for interfaces for the solution, including those with other State enterprise systems and external interfaces. ICDs provide the detailed technical information regarding each system-to-system interaction. ICDs provide sufficiently detailed documentation (i.e., technical, operational, and end-user configuration support) to provide a successful interoperability and exchange of data, including message structure and error messaging configurations. ICDs will include detailed documentation on the concept of operations for the interface. It will include the messaging structure and protocols that govern the interchange and the communication paths along which the data is expected to flow. Figure 3.10.1-149 shows the interface methods and patterns available in our evoBrix X Integration Gateway framework.

Type of Interface	Approach and Benefit to DPHHS
File-based Batch Interfaces	Batch interfaces are required since other external systems may not be capable of supporting other interface patterns. However, with the ISR solution services, these interfaces are managed consistently, along with other interfaces, such as Web services-based interfaces. These interfaces are submitted via the ESB layer to ensure that each interface is logged, tracked, and audited. These interfaces then leverage the same reporting and management infrastructure available on the ESB. Furthermore, these batch interfaces are scheduled and orchestrated using the same framework to enhance automation.
Web Services-based Interfaces	Web service interfaces are supported with partners who can implement Web service standards-based data exchange services. These services can be supported in a request response model or in an asynchronous mode in situations, where actual files can be wrapped around as messages between two systems. Web service interfaces are supported both in direct access mode and via a registry. The flexibility of the interface service allows for accommodating different types of external systems.
Publish/Subscribe Mode	This framework allows the system to support the 'publish and subscribe' modes for interfaces. The service bus allows the system to push out outbound data feeds in a standard format. The system has built-in subscription services that can poll for standard incoming data feeds. The transformation of the inbound subscription services uses the data translation services to minimize core system changes.

Figure 3.10.1-149. evoBrix X Interfaces Patterns. Team CNSI's evoBrix X Integration Gateway supports multiple interface methods to support ICD documentation.

ICDs include the testing requirements for the interface, which will be used to develop the integration test cases. It will also include the test protocols for the interface, including points of contact with the other entity and connectivity information for the test system for the other entity. If data needs to be provided for testing, it will be outlined in the testing protocols. Team CNSI will require State approval of ICDs before beginning any testing with third parties and will notify the State before beginning testing.

INR12

The Contractor shall ensure proprietary interfaces and protocols between modules are not used.

Team CNSI Integration Gateway leverages industry standard file protocols where applicable (i.e., HIPAA) and supports proprietary interfaces where the standards are not relevant. Also, our framework is implemented specifically to handle the volume and security needs of Medicaid systems and Core Claims Processing. Exchanges between modules as well as external systems are architected to provide secure and protected data communications that maintain confidentiality and integrity of the data. Data exchange from the Integration Gateway to external systems is handled by the ISR component by leveraging Oracle SOA suite Managed File transfer component that supports secure data exchanges using available standards in the industry such as SFTP, FTPS, and SSL.

INR33

The Contractor shall document all interfaces in the Agency's Interface Control Document (ICD) format which will include data layout documentation, data mapping crosswalk, inbound/outbound capability and frequency of all interfaces. The Agency will approve finalized interface designs detailed in the ICDs.

As discussed in our response to INR11, Team CNSI will develop ICDs to document interface designs for system-to-system interactions. Team CNSI leverages the standard ICD template developed from implementing the solution in multiple States which include data layout documentation, data mapping crosswalk, inbound/outbound capability and frequency of all interfaces. The ICD template is organized to capture the following information:

- Assumptions, constraints, and risks
- General interface requirements
- Detailed interface requirements by interface
 - Interface protocol(s)
 - Frequency
 - Interface owner
 - Data element layout
 - Data crosswalks
- Qualification methods for meeting interface requirements

Team CNSI will review the Agency's ICD format and align the content typically captured from our experience to the Agency's ICD format.

INR34

The Contractor's solution shall include all integrations/interfaces listed in Attachment F - Requirements Response Matrix in their overall fixed price.

Team CNSI has included all integrations/interfaces listed in Attachment F as a part of our overall fixed price.

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 in detail their approach to meet each of the Business Rules requirements in Attachment F – Requirements Response Matrix. The Offeror simply repeating the RFP requirements does not qualify as a good response as defined in Section 6.1.1 of this RFP.

Team CNSI’s evoBrix X platform includes RuleIT, a rules engine built on decades of experience in implementing Medicaid and Medicare claims adjudication solutions. RuleIT comes with English-like, pre-defined rules and also provides the ability to quickly configure rules to implement the state specific programs. The main advantage of this capability is to provide a solution for the MPATH Initiative that is flexible, configurable and ensures quicker implementation. RuleIT has been in production since 2009 when the State of Michigan went live with its MMIS. RuleIT is being used to process claims and is critical in maintaining high auto-adjudication rates in the states of Michigan and Washington and the high-volume CMS Medicare Encounter Data Processing System (EDPS). RuleIT, has been refined and engineered for performance based on these experiences. RuleIT is integrated in the evoBrix X platform and states have leveraged it for decision-making in Claims, Prior Authorization, Provider Enrollment, and Managed Care.

- RuleIT, a rules engine based on industry standards and built specifically to address Medicaid programs
- RuleIT, used to drive the complex adjudication logic, is highly configurable and separately maintained from the application code.
- The base version of RuleIT contains over 1,500 pre-configured edit and audit related rules.
- RuleIT provides a configuration-driven approach and acts as a centralized business rules repository, enabling business users to maintain business rules easily.
- The RuleIT Composer provides the ability to create, edit, and maintain business rules in an English-like syntax language.

RuleIT Overview

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. The approach addresses performance challenges of using RuleIT in a high-throughput environment. The approach also manages the constraints of transitioning rules from legacy code. Team CNSI believes that its approach and tool offer a great competitive advantage and minimize the risk of this implementation.

The use of English-like syntax, a predefined Medicaid dictionary, standard Medicaid edits and processing flows make RuleIT easy to implement and deploy. This reduces development time by promoting reusability. 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

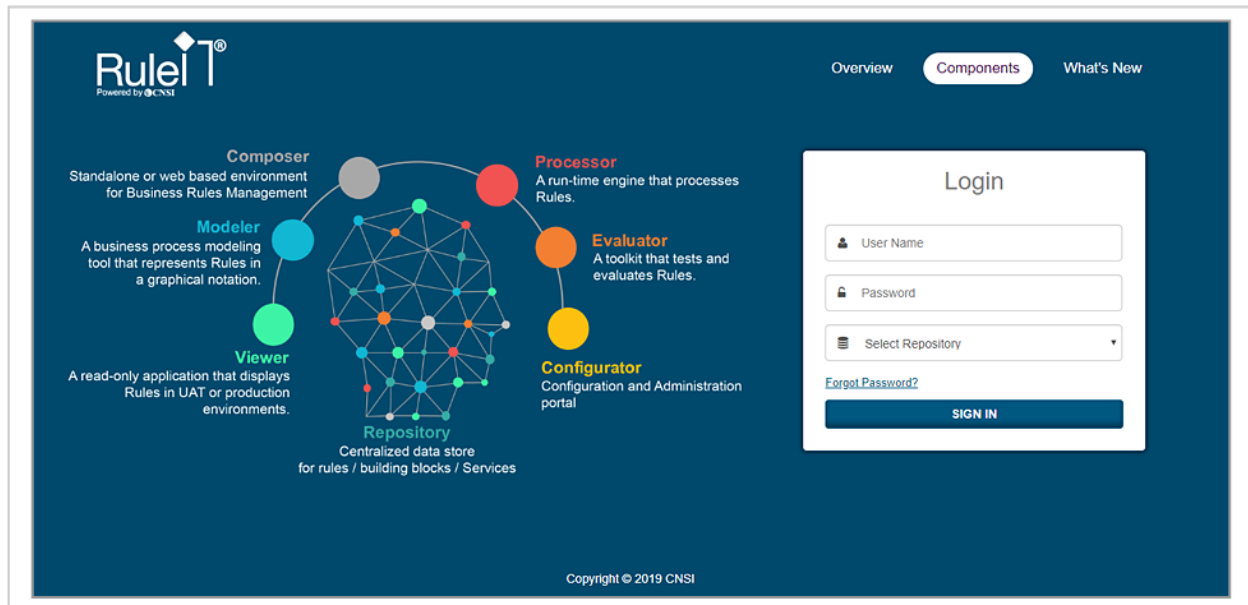
The Team CNSI Advantage

RuleIT provides a proven, high-performance, healthcare-focused rules engine.

- Provides out of the box CMS-mandatd policy rules for Medicaid
- Provides pre defined rule sets built on best practices from other states
- Reduces the implementation time frame for new rules and policies to days and weeks from weeks and months with its available Medicaid business dictionary
- Provides a balanced approach of configuration-driven changes versus coding changes that allows non-technical business subject matter experts to update or change business decisions and policies
- Reduces defects and increases accuracy in implementation of business rules

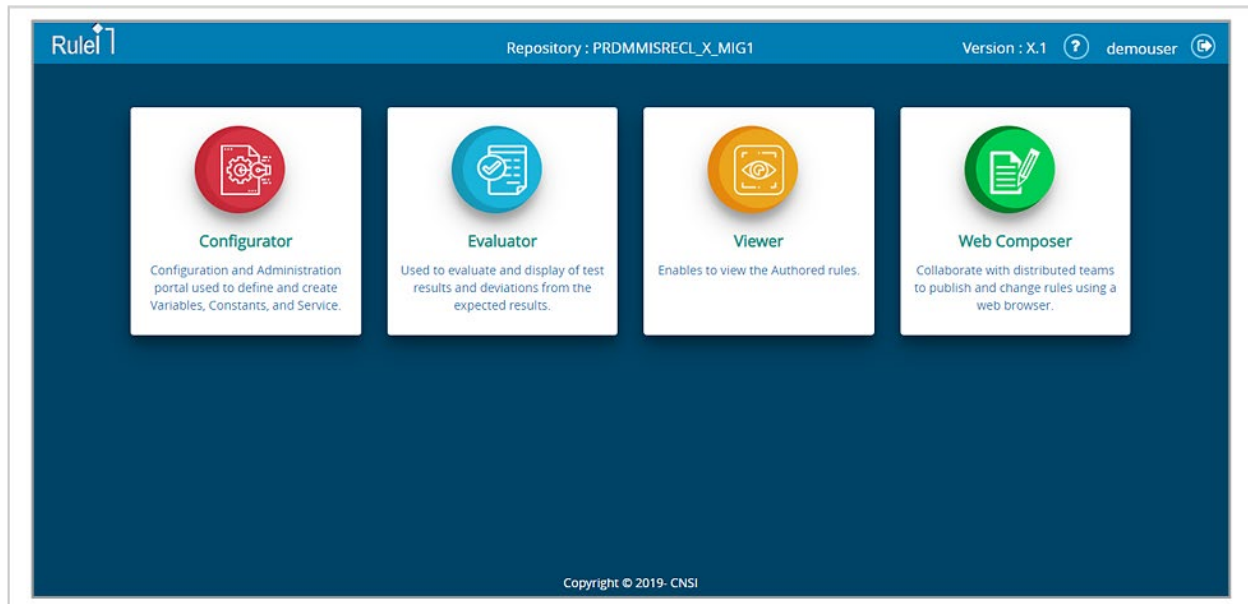
MTCPM-1.2.4-808

implement. For example, having pre-configured rules enabled CNSI to accomplish the first release of CMS EDPS within three months. This success also demonstrates the flexibility with RuleIT given it was the first implementation of existing pricing rules for a Medicare program. 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 is accessible from the web, as shown Figure 3.10.1-150 and Figure 3.10.1-151.



MTCPM-1.2.4-602

Figure 3.10.1-150. RuleIT Web Application. RuleIT Web Suite provides quick and easy access to all the different components on a single web page.



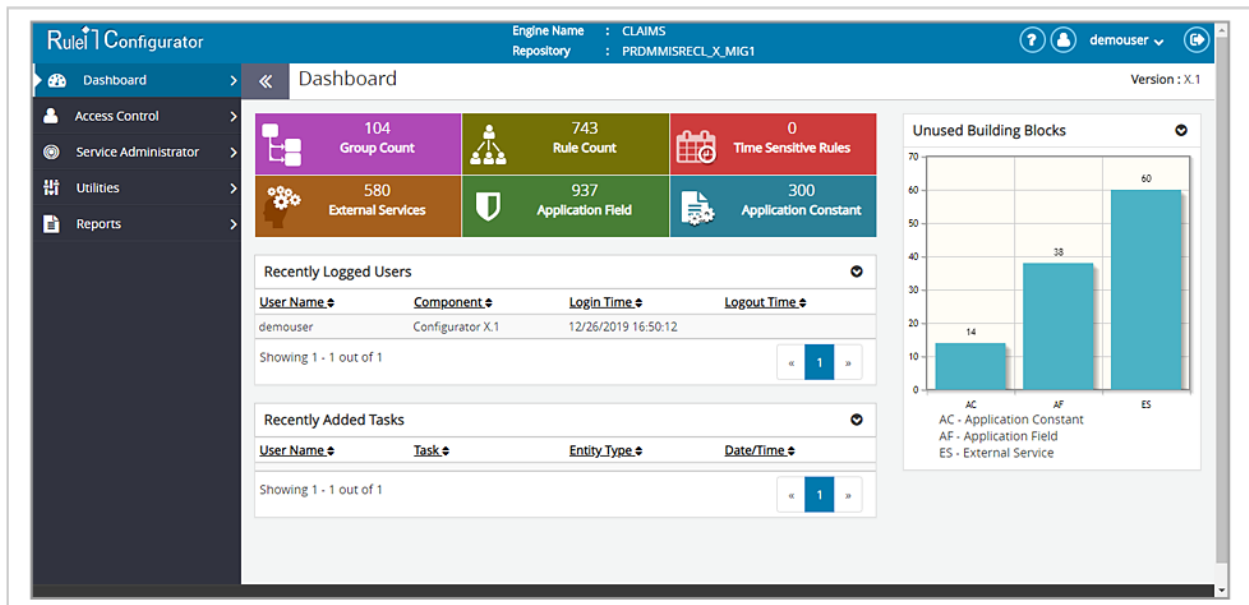
MTCPM-1.2.4-603

Figure 3.10.1-151. RuleIT Components. The different deployed components are easily accessible to the users from the RuleIT Web application.

RuleIT consists of the following major components:

- **RuleIT Viewer** - allows application developers and users to view the rules without having to install RuleIT Composer
- **RuleIT Modeler** – provides a graphical representation of the business rules flow
- **RuleIT Composer** – provides capability in 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 Processor** - 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 Web application servers and provides a public interface that integrates easily with other J2EE-compliant applications. RuleIT Processor is currently supported on WebLogic, WebSphere, and WildFly environments.
- **RuleIT Evaluator** - 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 Configurator** – shown in Figure 3.10.1-152, 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 Repository** - the centralized store for all defined rules 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 XML database.

The RuleIT product suite also includes a utility, RuleIT Migrator, to migrate rules between development environments, such as development, test, and acceptance.



MTCPM-1.2.4-604

Figure 3.10.1-152. RuleIT Configurator. Configurator allows for the administration and configuration of the business rules. Defining business rules has never been easier.

The RuleIT Composer shown in Figure 3.10.1-153 is the component of RuleIT used to add, modify, or remove/retire rules in the repository. Figure 3.10.1-154 highlights some of the key features of this tool and shows a sample rule syntax.

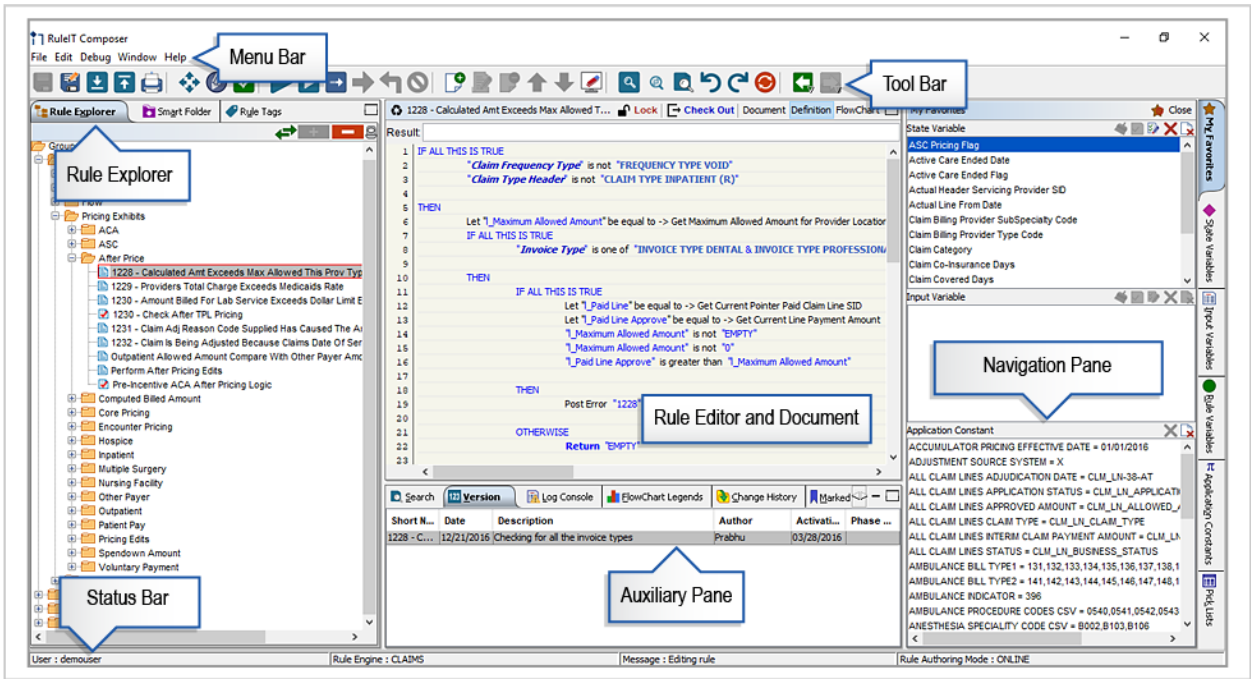


Figure 3.10.1-153. RuleIT Composer. RuleIT Composer has a user-friendly interface that makes it easy to use.

RuleIT Composer also supports other important features, for example users can quickly search the rule repository using key words to get more details on the edit functions, as shown in Figure 3.10.1-154.

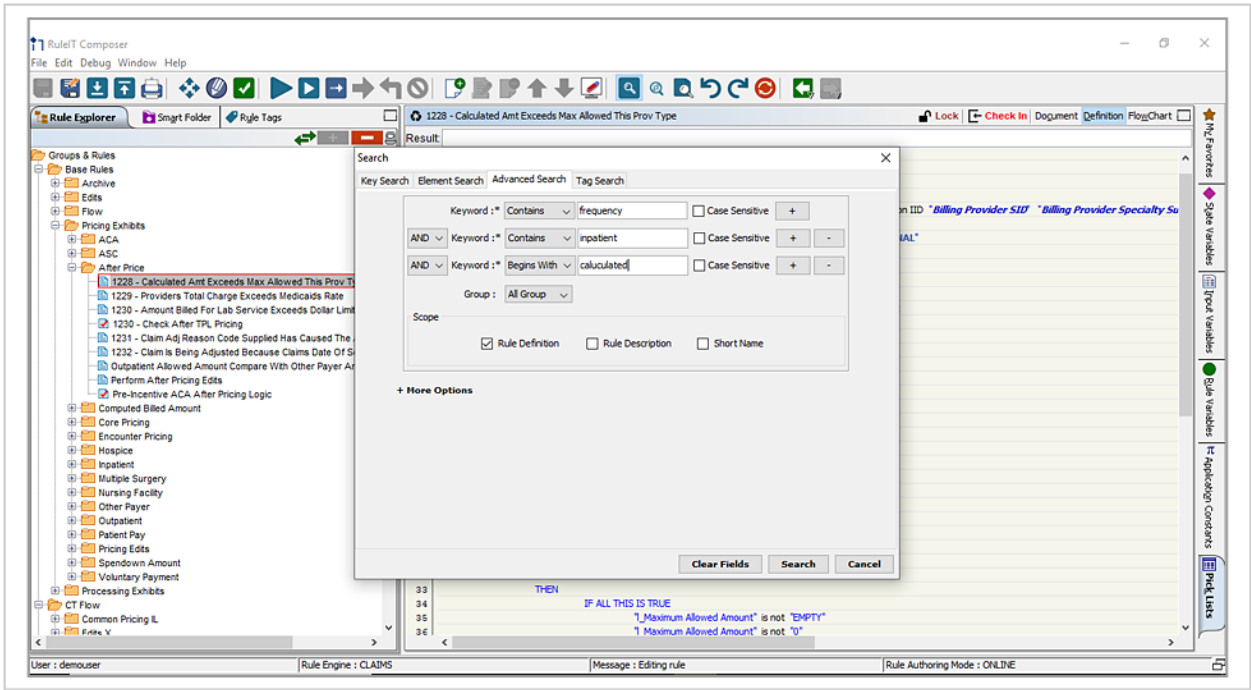


Figure 3.10.1-154. RuleIT Composer Search. RuleIT Composer search features allow users to quickly locate and search for specific rules.

RuleIT offers the flexibility to create and integrate customized rules specific to DPHHS 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, as shown in Figure 3.10.1-155, which can be useful when rules must be retired based on policy changes.

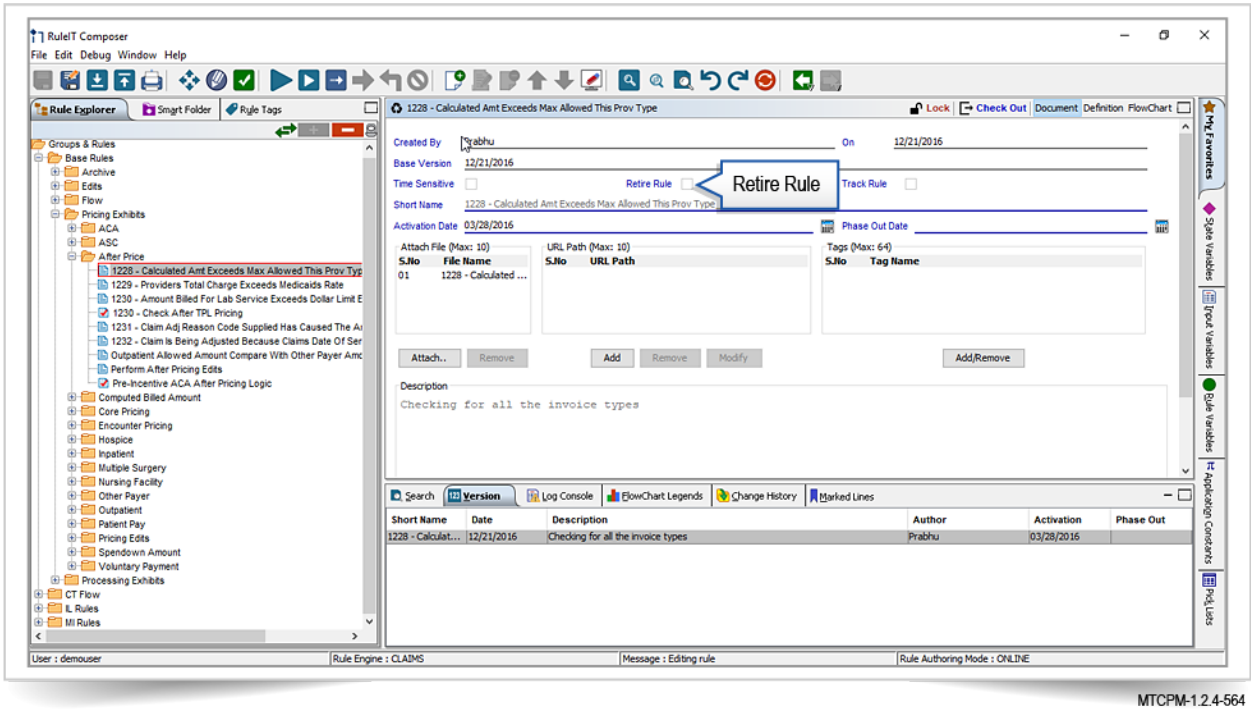
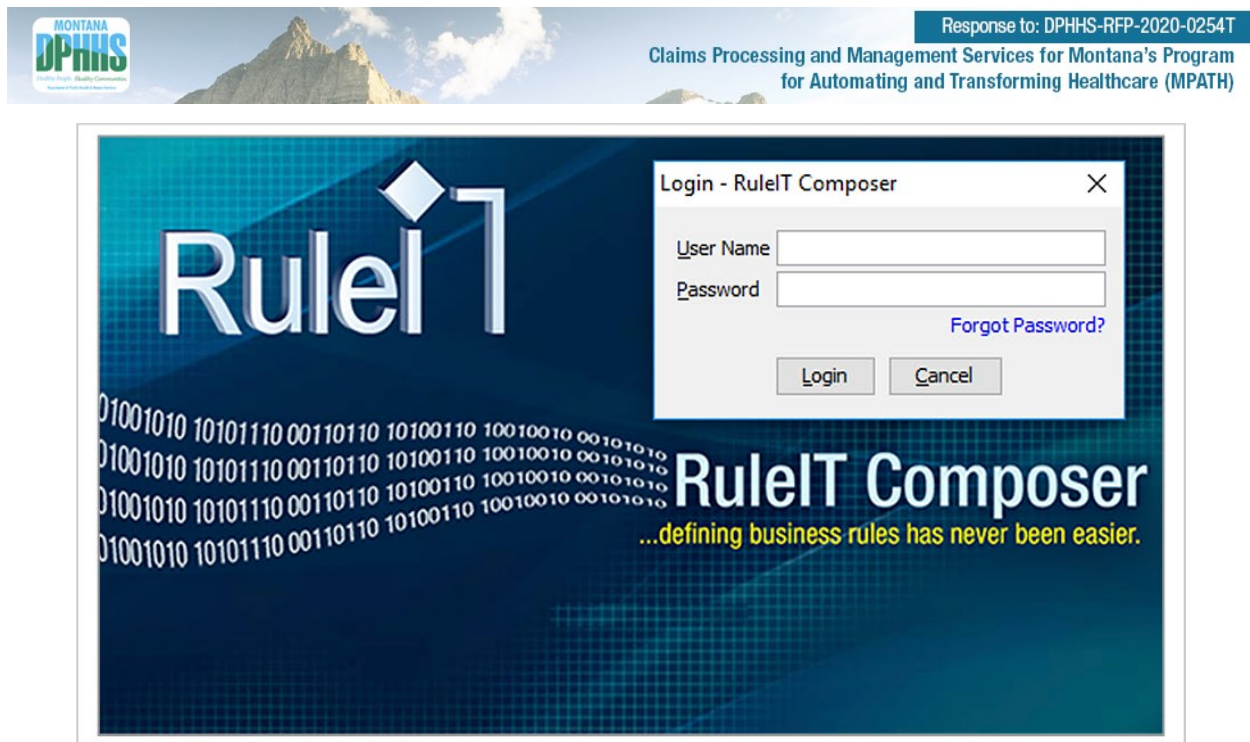


Figure 3.10.1-155. RuleIT Composer Retire Rule Configuration Screen. RuleIT supports retiring rules through an easy configuration screen.

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.

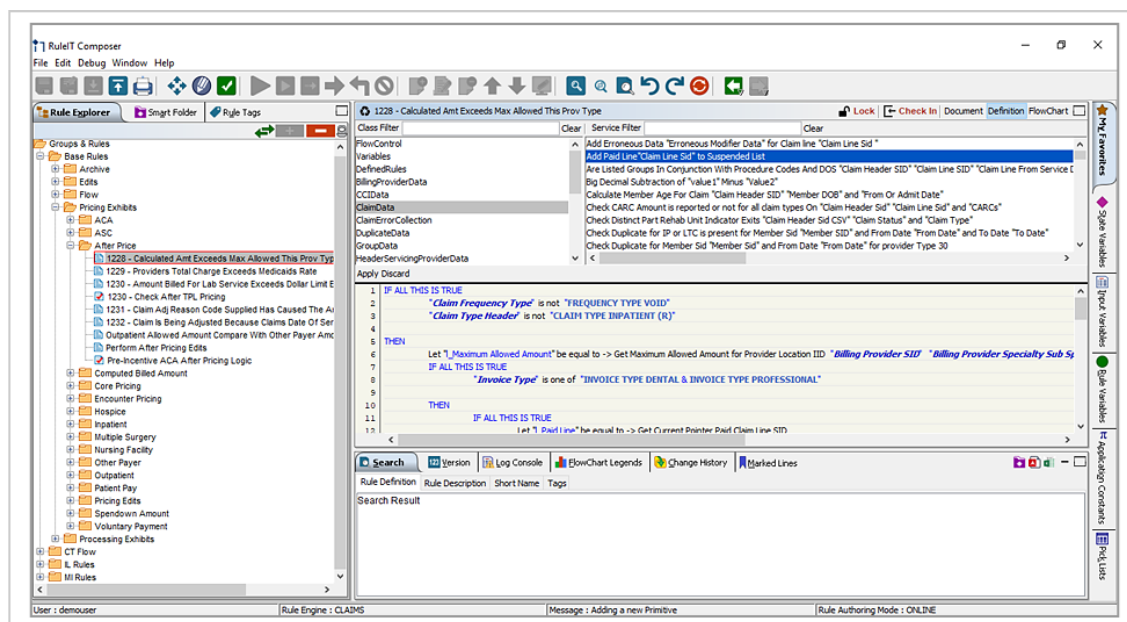
RuleIT Composer provides a username and password screen to authenticate users before they are allowed access to the application. Administration of RuleIT users is available to authorized security administrators through online screens. Users can be added and removed, and their appropriate privileges can be assigned through this interface, so it does not pose a risk of unauthorized data access. Figure 3.10.1-156 shows the Rule IT Composer login screen.



MTSPM-3-292

Figure 3.10.1-156. 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 3.10.1-157. 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 DPHHS users to apply or disable rules quickly and without programmer intervention.



MTCPM-1.2.4-688

Figure 3.10.1-157. 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.

The RuleIT Viewer provides real-time access to a Business Rules Catalog that documents all business logic used by the evoBrix X solution and provides the framework necessary to support DPHHS approval for business rule management activity. Authorized users will have the ability to access the Business Rules Catalog in real-time.

Rules can be categorized based on the business functionalities and these rules form the Business Rules Catalog. The Business Rules Catalog can be viewed in electronic format using the RuleIT Viewer as shown Figure 3.10.1-158. The RuleIT Viewer is a read-only view allowing the rules catalog to be available to a larger base of users.

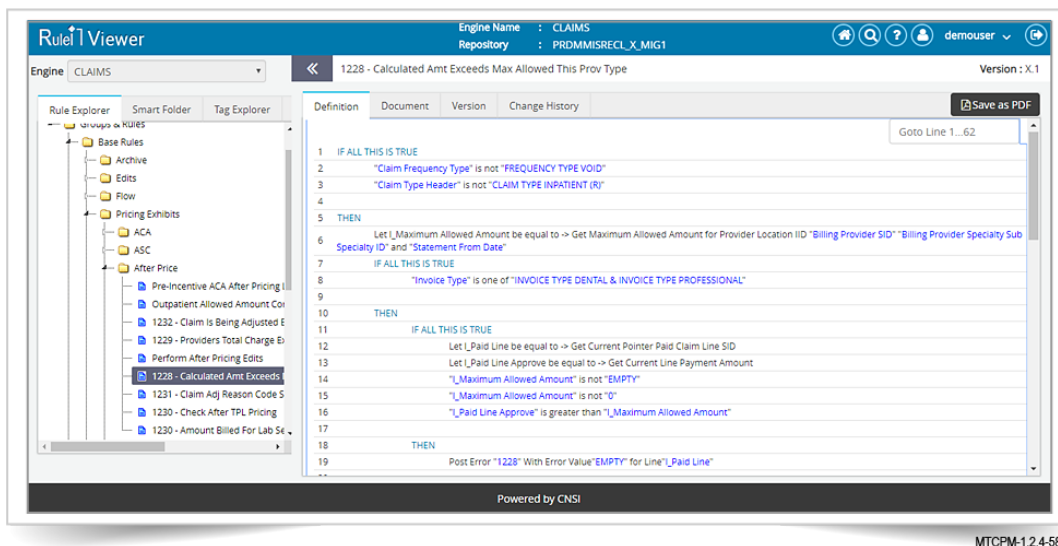


Figure 3.10.1-158. RuleIT Viewer. The RuleIT viewer allows application developers and users to view the rules without having to install RuleIT Composer.

BR04

The Contractor shall update the Business Rules Catalog with all additions or changes.

Team CNSI will maintain the Business Rules Catalog with all additions or changes to the business rules implemented in the solution. As indicated earlier in the response, Team CNSI will use RuleIT to required to operate and manage the proposed solution.

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 shown in Figure 3.10.1-159.

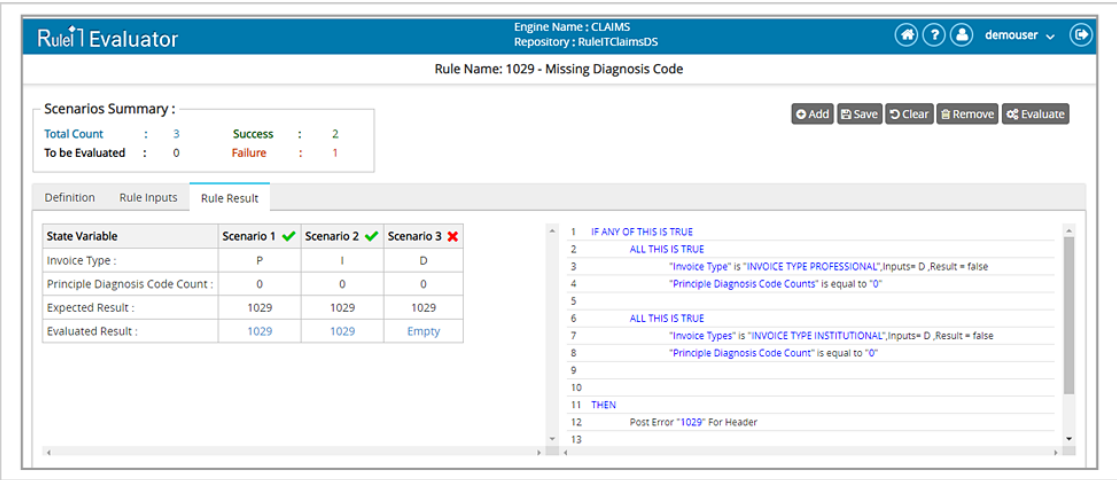


Figure 3.10.1-159. RuleIT Evaluator screen. RuleIT Evaluator performs rules testing to understand the before and after outcomes and supports what-if scenario testing.

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, as shown in Figure 3.10.1-160, to maintain configuration control of rules changes.

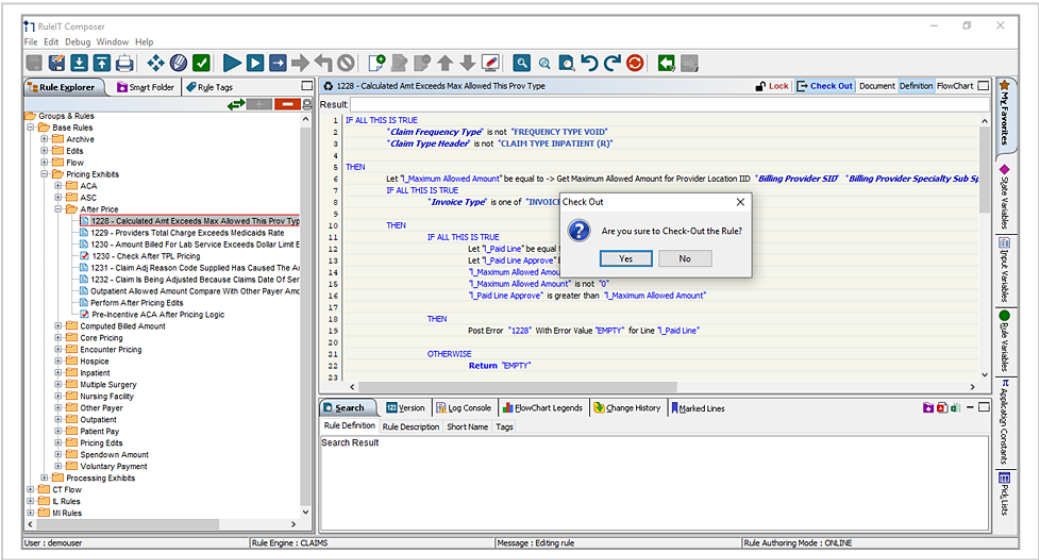
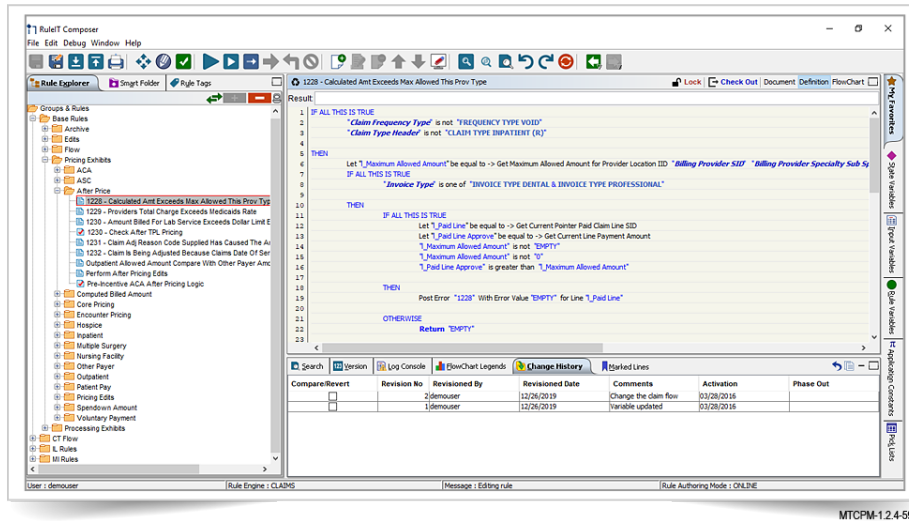


Figure 3.10.1-160. RuleIT Composer Version History Screen. RuleIT allows users to check-out and check-in rules changes with detailed audit trails.

The Figure 3.10.1-161 below shows the change history in the RuleIT Composer screen, allowing the authors to discern the different changes and revisions that were made to the rule.



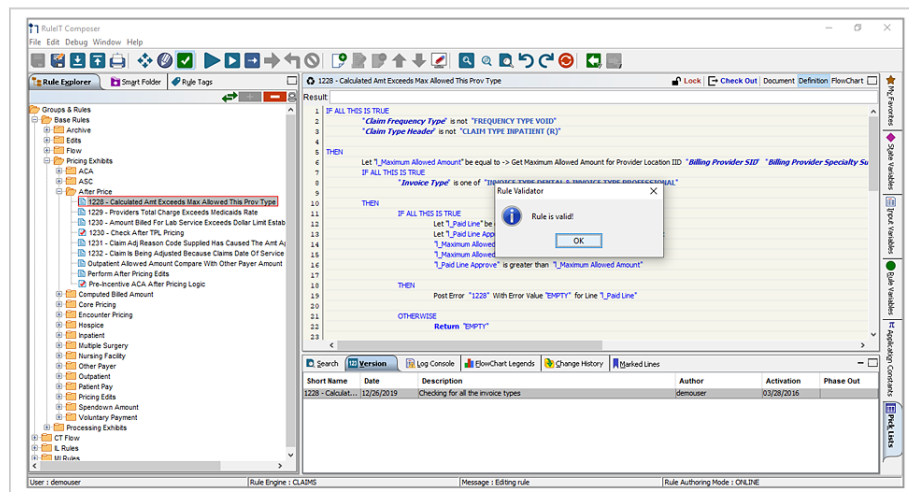
MTCPM-1.2.4-591

Figure 3.10.1-161. RuleIT Composer Change history. RuleIT Composer shows the change history to the user, providing critical information during authoring.

BR08

The Business Rules Engine shall allow changes to be made to valid values without impacting production rules engine availability and operations.

RuleIT Composer is used to modify the rules for the change in business variable values and application constants. Our solution saves time since it offers the capability to validate rules prior to publishing it in an environment. After a rule is created or modified, the user can validate the rule as shown in Figure 3.10.1-162. In addition, the RuleIT Configurator provides the ability to select multiple rules to run batch validation, as shown in Figure 3.10.1-163. Rules are developed in the development environment and promoted to higher environments such as test, user acceptance, and production using the RuleIT Migrator, as shown in Figure 3.10.1-164. The rules migration process is performed during the scheduled deployment window and will not impact production rules engine availability and operations.



MTCPM-1.2.4-592

Figure 3.10.1-162. RuleIT Composer Rules Validation Screen. RuleIT allows users to easily access to validate the rules.

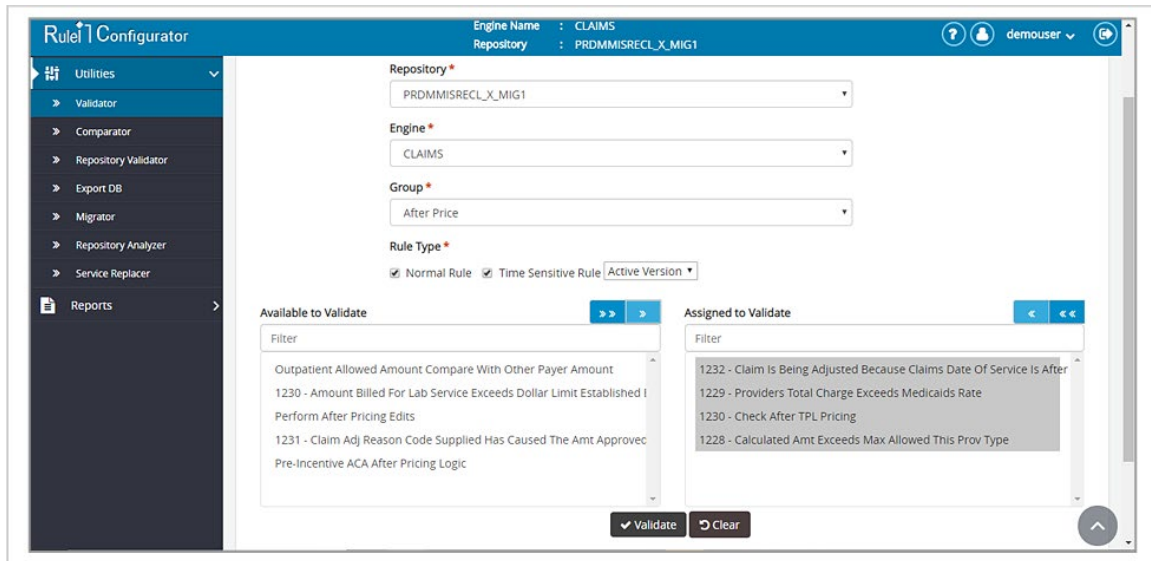


Figure 3.10.1-163. RuleIT Configurator Rules Validation Screen. Multiple rules can be selected based on criteria chosen to validate rules.

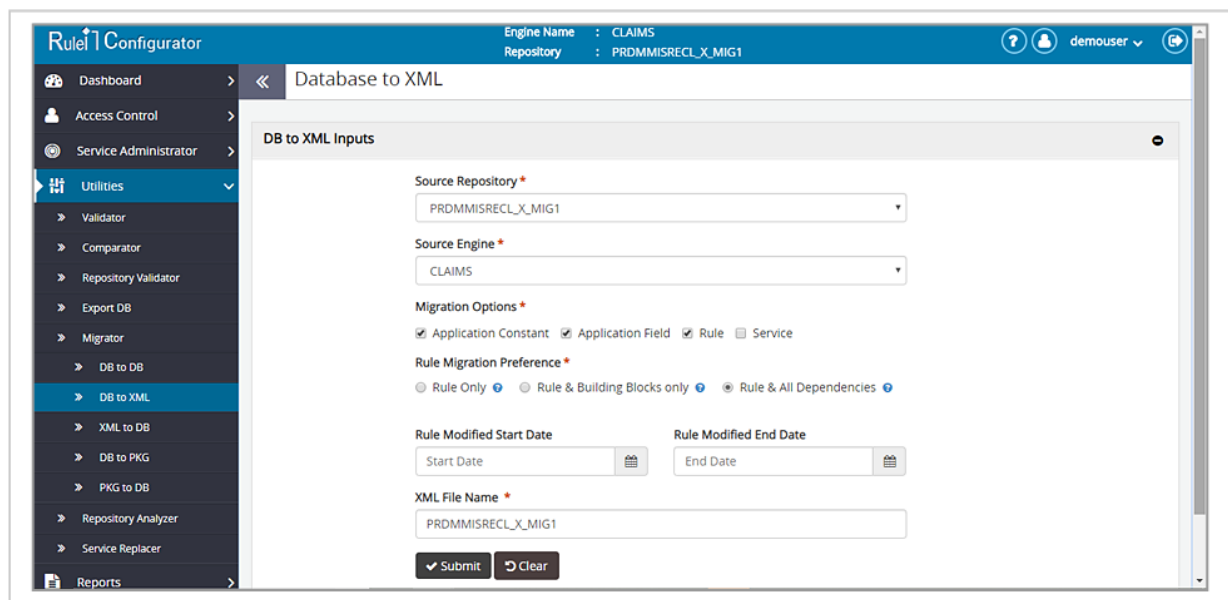
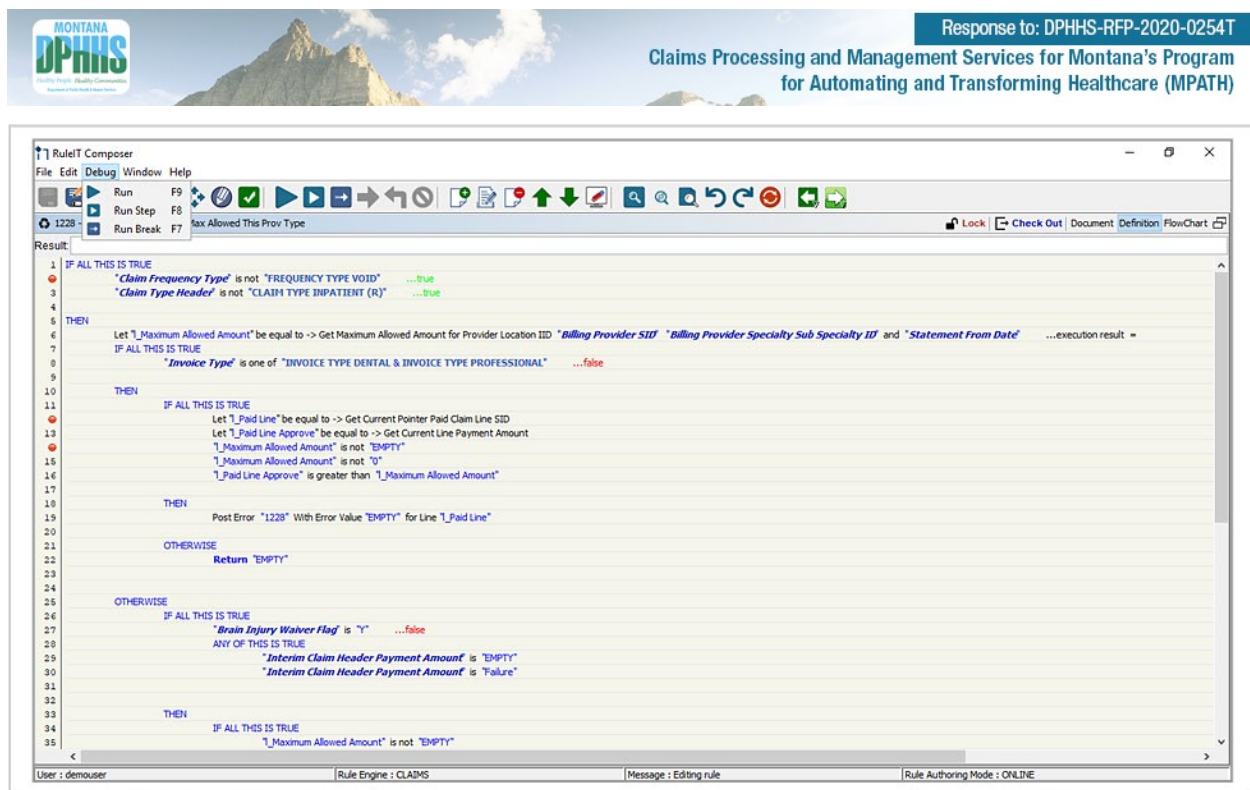


Figure 3.10.1-164. RuleIT Migration. RuleIT allows rules to be migrated from development to other environments seamlessly to eliminate disruptions during deployments.

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 3.10.1-165 shows the debugging screen, with RuleIT Composer’s various debug options.



MTCPM-1.2.4-593

Figure 3.10.1-165. RuleIT Composer Debugging Options. RuleIT provides 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 3.10.1-166. 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.

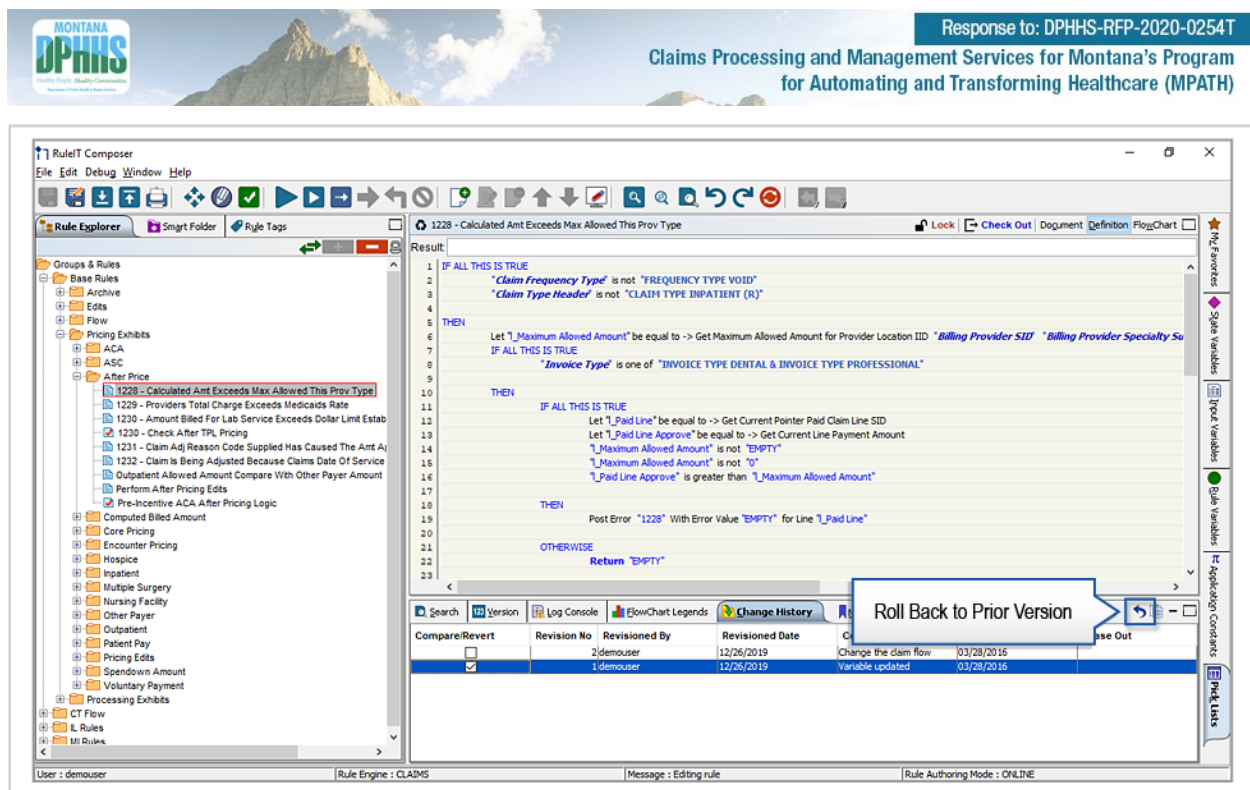


Figure 3.10.1-166. RuleIT Composer Change History Screen. RuleIT allows users to roll back changes and retrieve older versions of the rule.

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 as shown in Figure 3.10.1-167. 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.

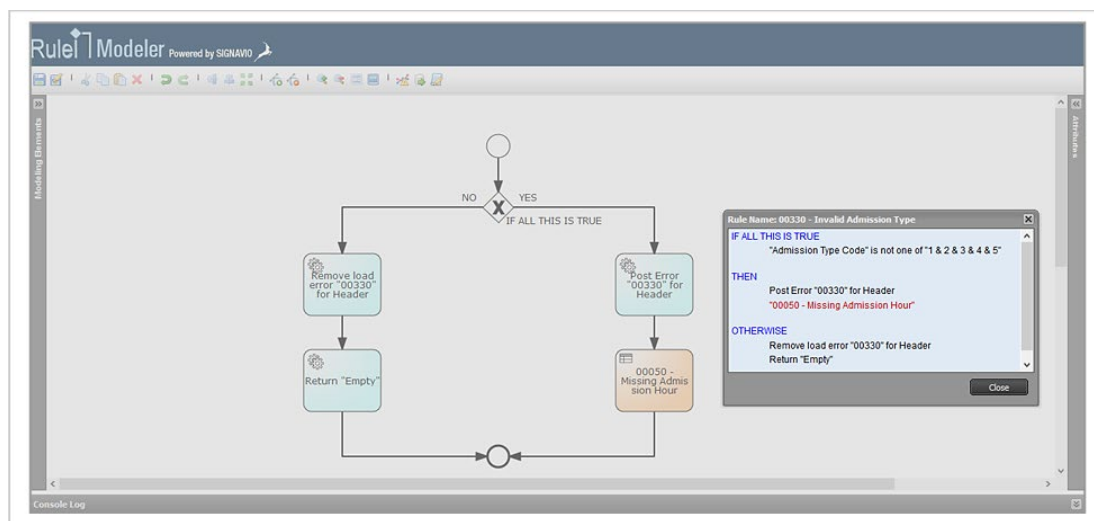
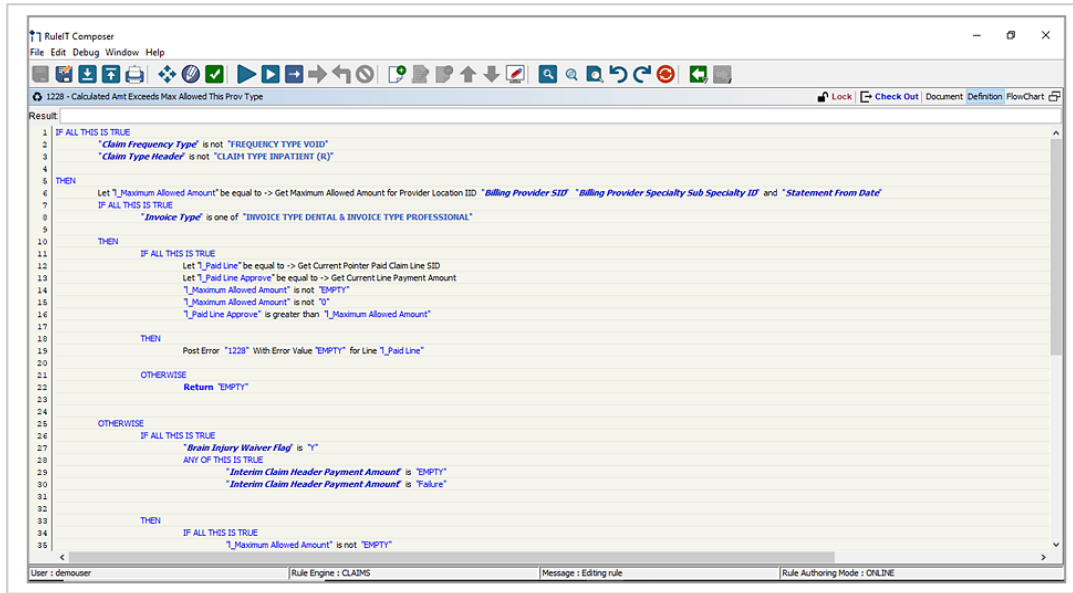


Figure 3.10.1-167. RuleIT Modeler Screen. RuleIT Modeler provides a graphical representation of the rules flows.

BR13

The Business Rules Engine shall have mechanisms to identify which rules are executed for each specific business process.

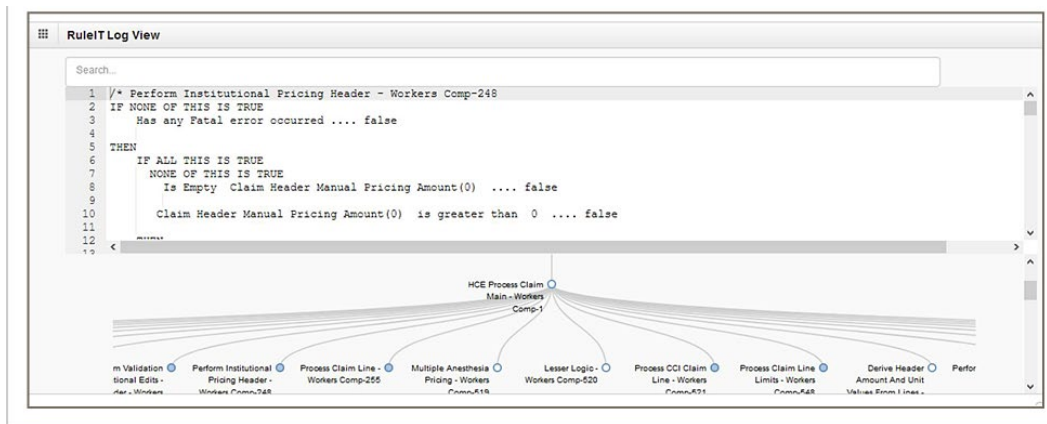
RuleIT uses a “sequential process” algorithm, in which the rule flow and the evaluation is controlled by the rule, its conditions, and the associated branching. This provides the user to identify and foresee the rule execution flow for the various business process as shown in Figure 3.10.1-168.



MTCPM-1.2.4-596

Figure 3.10.1-168. Rules Sequential Flow. Complex rule flows can be identified and implemented quickly, and these rule flows are simple to read and edit.

Team CNSI’s also provides the capability to analyze rules after execution of the rule. Users have the ability to view a claims processing log from the user interface. While viewing the log, the user can open a log entry and view details as shown in Figure 3.10.1-169. This is a powerful capability given it enables the user to view areas of a business process that were executed and view the specific rule. This capability is available for Service Authorization and Claims Processing business processes.



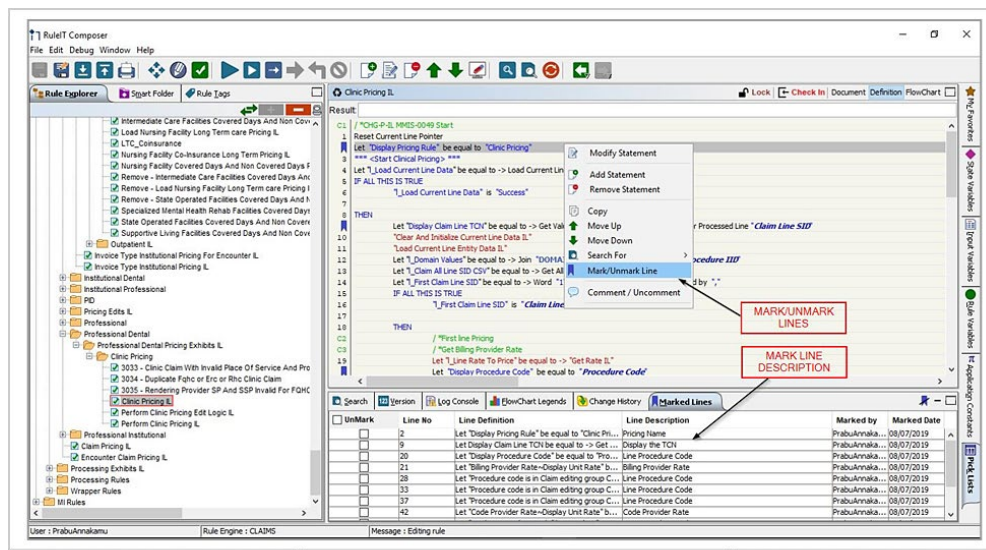
MTCPM-1.2.4-809

Figure 3.10.1-169. Rules Log Viewer. Team CNSI’s solution provides valuable insight into rules execution results.

BR14

The Business Rules Engine shall be able to produce a report on rules passed or failed for all transactions.

The 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. In addition, RuleIT also provides the ability to track the rules that were executed in the processing of adjudicating a claim. RuleIT provides the option to mark or unmark the rules, rule statement, variables or services as shown in Figure 3.10.1-170. The RuleIT Processor during rules execution captures these results of rules statements and the details of whether they passed or failed during the transaction flow. Figure 3.10.1-171 and Figure 3.10.1-172 shows the result of rules evaluation and the variable values derived and computed during execution.



MTCPM-1.2.4-608

Figure 3.10.1-170. Rules Tracking. RuleIT provides the ability to track the rules that were executed in the processing of adjudicating a claim.

TCN : 31192191000005000

Claim Type : S - FQHC

Pricing Flow

Toggle All

Computed Billed Amount	\$70.00
Line - Computed Billed Amount	\$70.00
Clinic Pricing	\$105.00
Copay Pricing	\$105.00
Non Medicare Pricing	\$55.00
Non Medicare Co-Ins, CoPay And Deductible Pricing	\$55.00
Lesser Of Logic	\$55.00

MTCPM-1.2.4-609

Figure 3.10.1-171. Rules Evaluation Results. RuleIT provides the powerful capabilities to view specific results of rules evaluation.

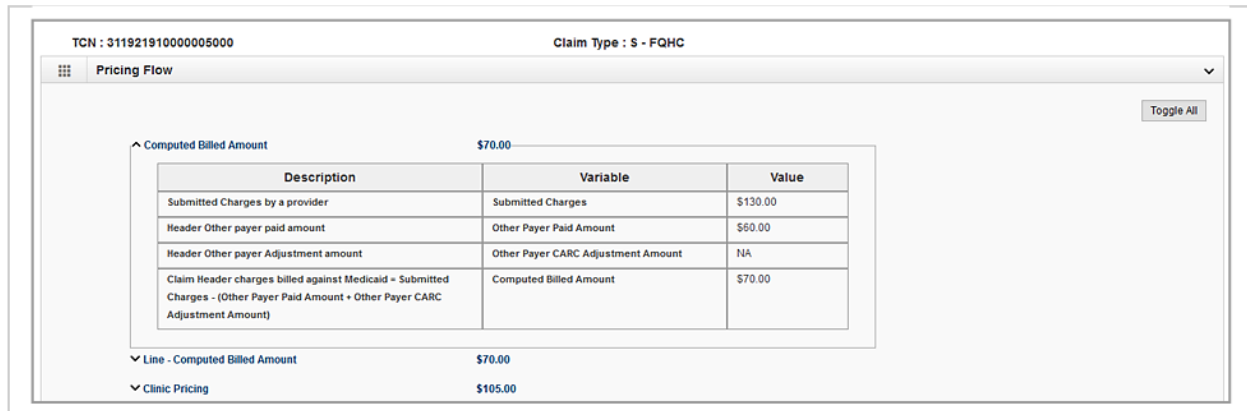


Figure 3.10.1-172. Rules Evaluation Results – Expanded View. RuleIT provides the powerful capabilities to view specific results of rules evaluation.

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.

RuleIT sends notifications based on error codes for 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 3.10.1-173 shows the application alert messages along with the error code. Error codes are stored in the database, allowing the messages themselves to be modified for business needs. During rules creation, RuleIT Composer saves time since it offers the capability to validate rules prior to publishing it in an environment. After a rule is created or modified, the user can validate the rule.

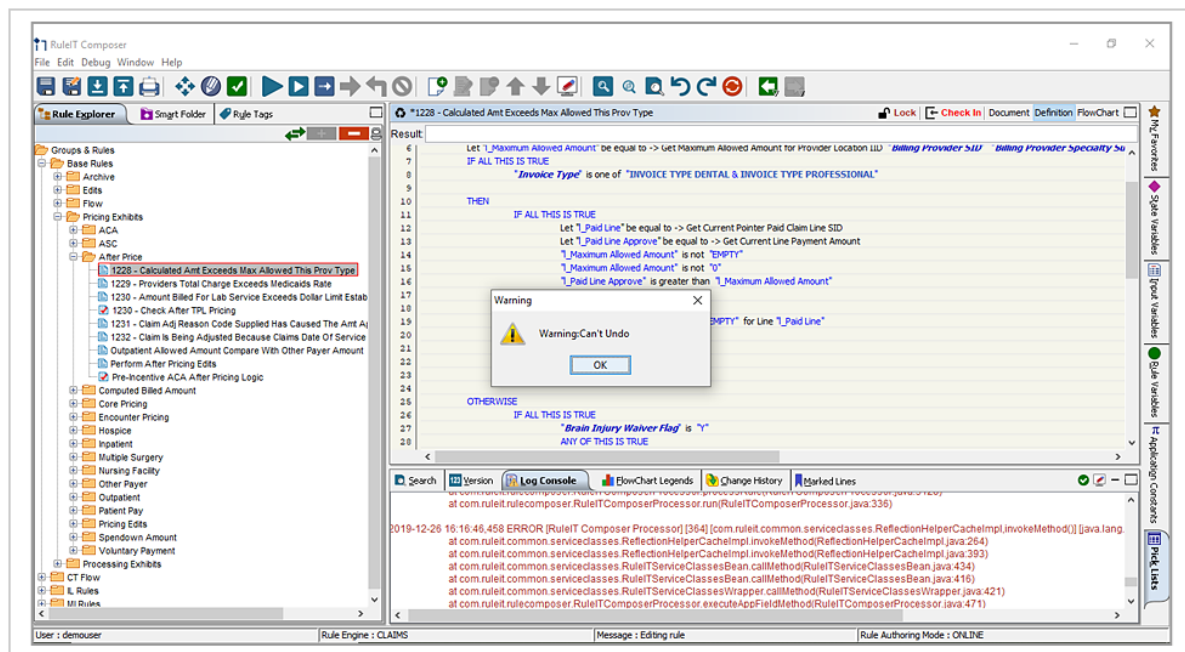
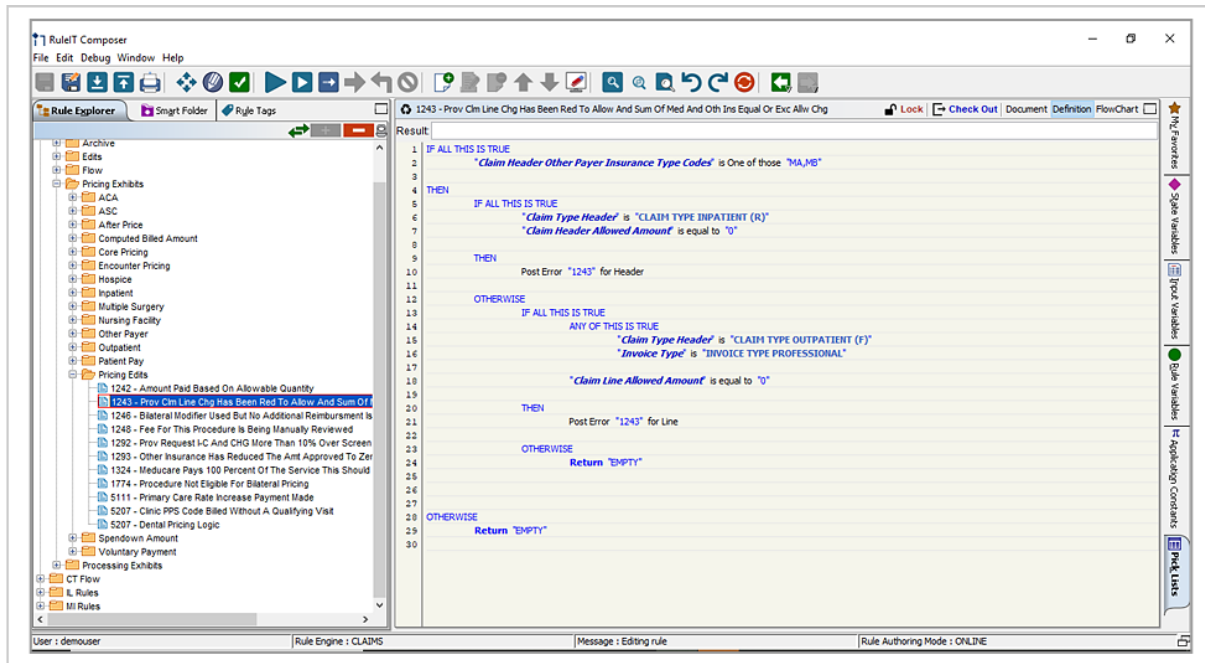


Figure 3.10.1-173. RuleIT Composer Alerts Screen. RuleIT issues are shown to the users with details of the errors.

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 3.10.1-174.



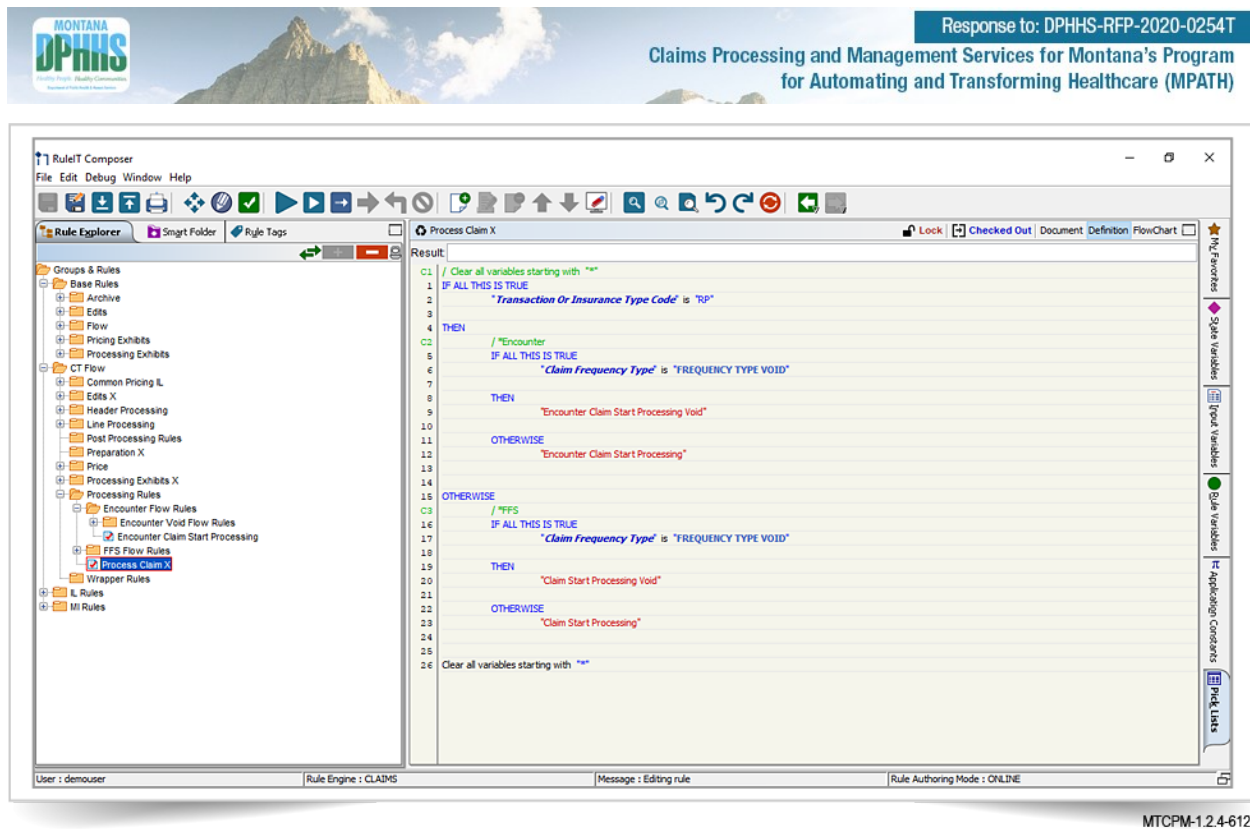
MTCPM-1.2.4-599

Figure 3.10.1-174. 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 flow, 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. The Figure 3.10.1-175 shows a sample rule, the execution of this rule flows from top to bottom, evaluating each line as it processes. The business analyst can therefore prioritize and sequence the flow of the rule based on their business needs.



MTCPM-12.4-612

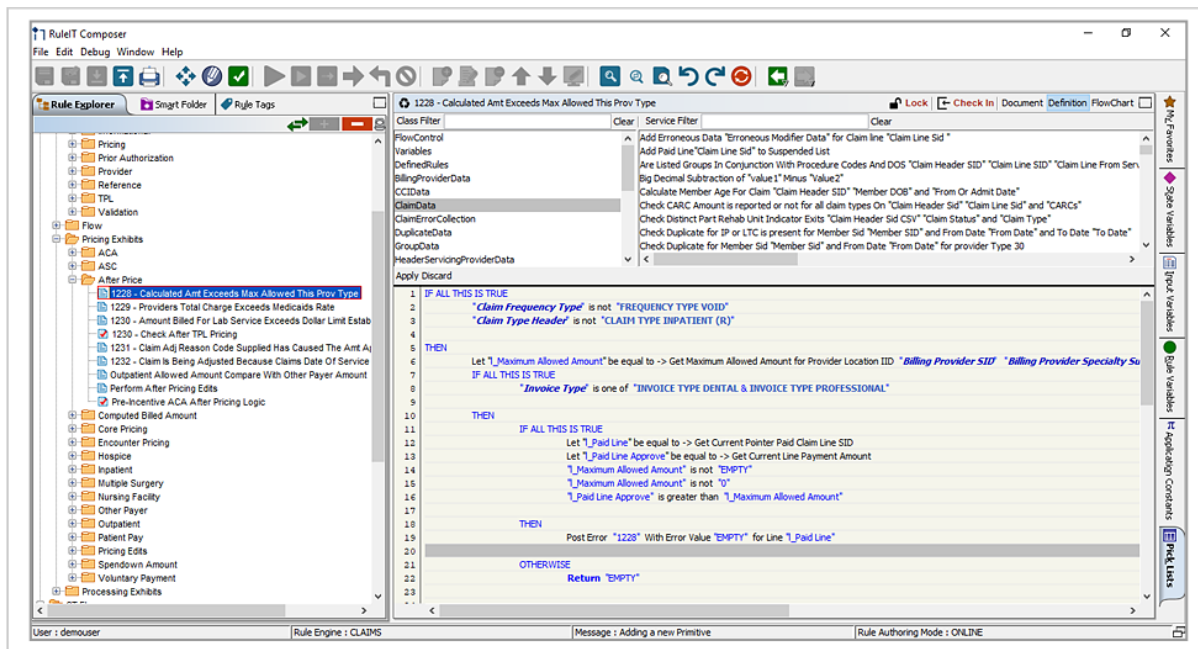
Figure 3.10.1-175. RuleIT Sequential Flow Processing. Business rules are executed top-down, in a sequential manner.

BR20

Where applicable, the business rules engine shall use standardized business rules definitions.

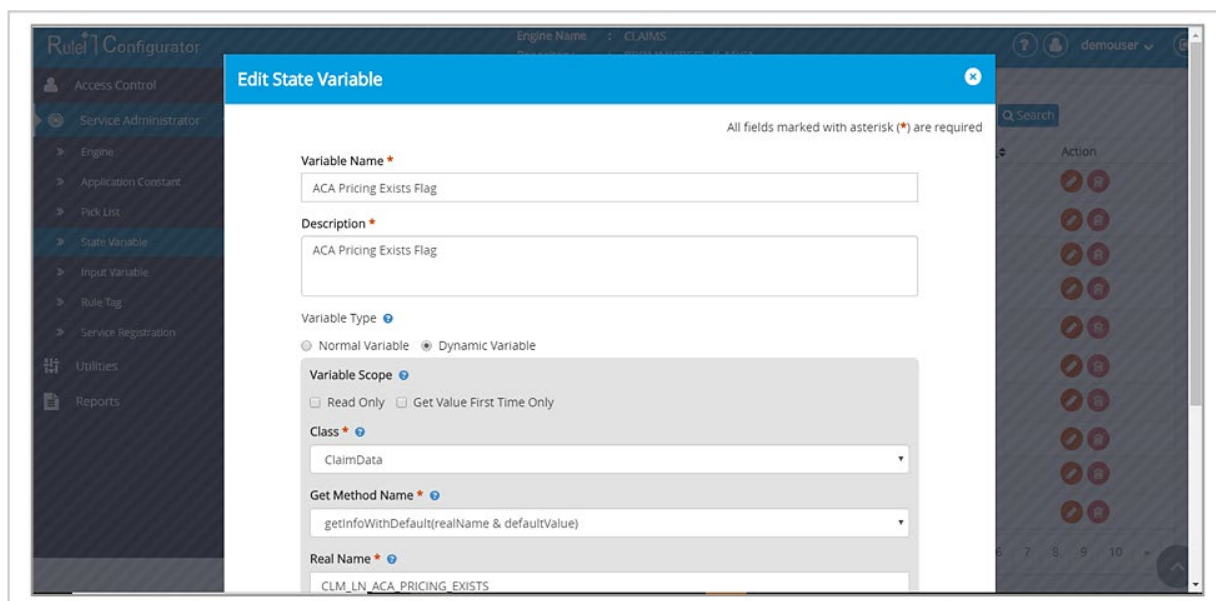
RuleIT provides comprehensive authoring capabilities that support standardization of the business rules definitions. The standardized business rules are available as a library of resources as internal services for users who are developing the rules. The RuleIT Composer as shown in Figure 3.10.1-176 allows the user to choose the existing defined business rules to create new business edit or other rule flows.

The RuleIT Configurator as shown in Figure 3.10.1-177 provides the ability to define new business definitions that can be leveraged in the Composer and Modeler etc. to create rules. While configuring basic building blocks, i.e., definitions, the names can be customized to meet the business needs, enabling the rules created to be more meaningful to read and understand.



MTCPM-1.2.4-600

Figure 3.10.1-176. RuleIT Internal Services Screen. Users can search and use standardized business rule definitions while authoring the rules.



MTCPM-1.2.4-601

Figure 3.10.1-177. RuleIT Internal Services Definition. New Variables and Services Classes can be defined, the names can be customized to needs of the business.

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 WildFly runtime environments.

BR27

The Contractor shall configure, support and maintain a business rules capability (e.g., add, modify, or remove/retire rules) based on the Service Architecture (SOA).

The evoBrix X system, with its SOA-based integration engine, seamlessly integrates data from other systems, external agencies, and business partners in the DPHHS enterprise environment. The Provider Enrollment and the broader Core Claims modules enable DPHHS to manage the business processes for provider enrollment and balance it with real-time data access and support. The evoBrix X 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.

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. This integrates well with the design of the SOA-based MPATH Integration Platform.

3.10.1.8 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, print, and mail enterprise correspondence. The Contractor must describe the proposed solution's capacity to configure, support and maintain correspondence management functionality (i.e., add, modify, or remove correspondence), the type of resource and necessary skill set(s) required for correspondence management functionality (i.e., add, modify, or remove correspondence), the type of resource and necessary skill set(s) required for correspondence management functions, and the change management processes associated with correspondence management. In addition, the Offeror must describe in detail their approach to meet each of the Correspondence Management requirements in Attachment F – Requirements Response Matrix. The Offeror simply repeating the RFP requirements does not qualify as a good response as defined in Section 6.1.1 of this RFP.

Team CNSI offers the DPHHS a robust solution to generate, manage, print, and deliver customer communications. Correspondence is a critical part of an organization's day-to-day activities and business processes.

[REDACTED]

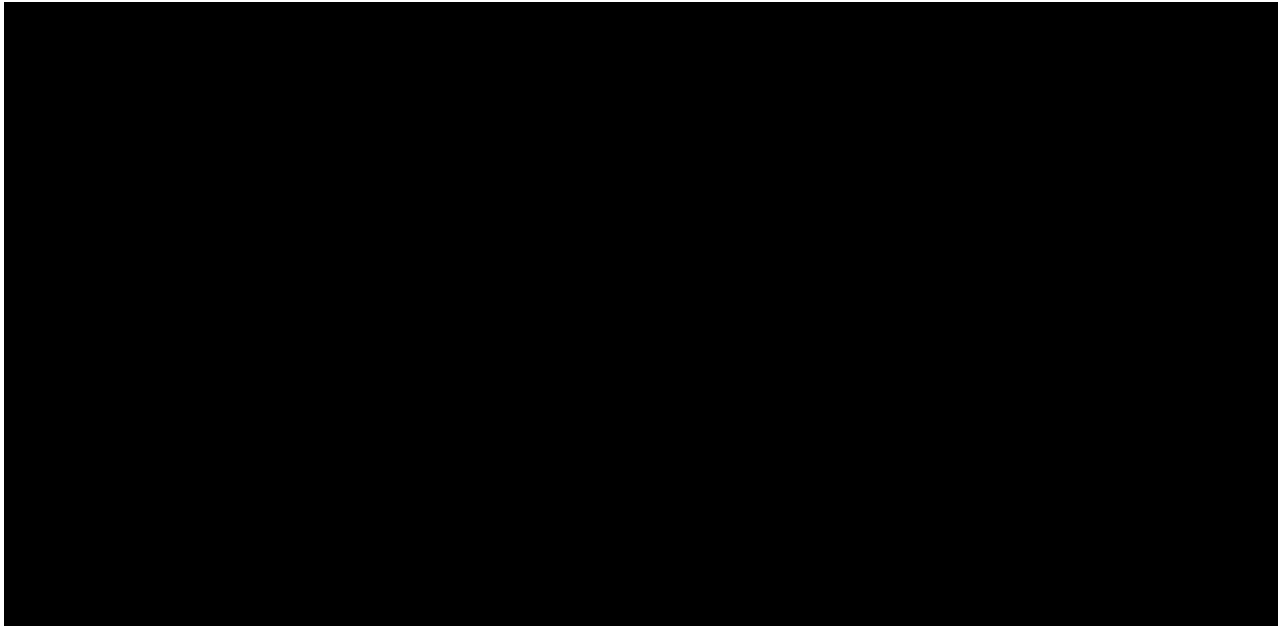
The Team CNSI Advantage

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 X portal or printed on demand.

MTCPM-1.2.4-123

[REDACTED]



All centrally printed and user-authorized on-demand letters comply with State and US Postal Service (USPS) guidelines for economical postage use, which includes standardizing letters and validating addresses against the most current USPS address database. Team CNSI stores claims letters, provider-supporting documents, State policies and procedures manuals, and training materials in the integrated evoBrix X Enterprise Content Management (ECM) solution, which users can access through the portal or print on demand. We can send all documents archived in the ECM solution to the DPHHS ECM repository by using ECM application programming interfaces (APIs) through the System Integrator. The following are the most commonly used automated letters/notices:

- **Remittance Advice Report.** The system generates this letter for providers to receive a paper Remittance Advice (RA)
- **Gross Adjustment Correspondence.** The system generates this letter for gross adjustments (GAs)

[REDACTED]

[REDACTED]

- [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]

[REDACTED]

Change Management

Team CNSI follows a standard change management process for correspondence management. Our process includes methods for communicating, evaluating, and approving or rejecting changes throughout

the State of Montana Claims Processing and Management Services (MT CPMS) project. This process ensures that we evaluate proposed changes for impact to system, schedule, scope, cost, and resources, which in turn facilitates informed decision-making by all involved parties. As a part of our process, we maintain a log of changes in the project repository and indicate the disposition and status of all change requests. We also institute a similar process to handle changes post-implementation.

New correspondence letter requests involve designing letters in EngageOne Designer and identifying the dynamic fields/free form text of the letter and then map it to the corresponding data elements. Changes to the existing correspondence involves evaluating scope and performing applicable required changes.

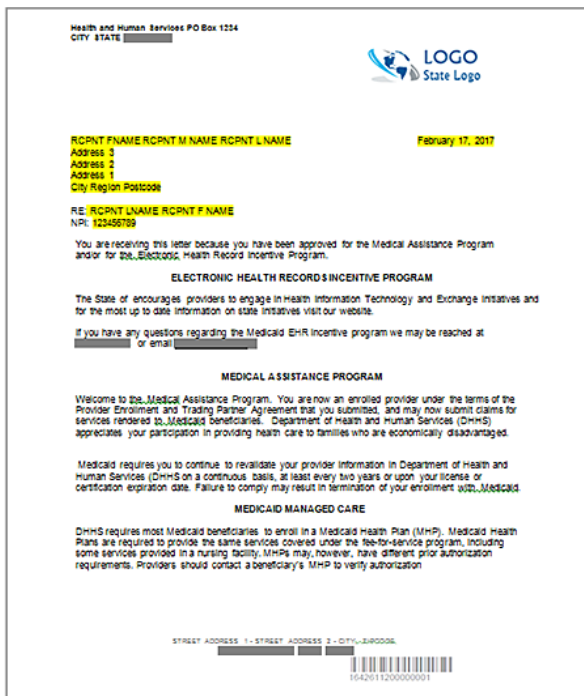
COR01

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 X Correspondence solution features Print Central and Print Local capabilities to generate correspondence (e.g., scheduled and ad-hoc correspondence and bulletins) using standard letters or forms, templates, and free-form letters. Our solution sends Print Central letters to the State's Print and Mail Services; however, authorized staff edit and mail out Print Local letters locally. Our solution can configure documents sent for centralized printing as scheduled letters or base them on system events. Our solution also designs pre-defined document templates based on business requirements, using standard letter templates or forms, that we can populate with dynamic content before sending them to the central print facility.

Our solution can also configure free form letters, which provide users the flexibility to change specific parts of a letter before printing, as a template. Users can provide dynamic content through the evoBrix X screens. The content is then added to the template and the letter is generated with the dynamic content, which users can then locally view and print. The evoBrix X document template design adheres to standards defined by the State's Print and Mail Services.

Figure 3.10.1-180 depicts the first page of a sample letter, where we have highlighted the dynamic content in yellow. It shows address blocks, logos, and barcodes typical to all evoBrix X correspondence.



Health and Human Services PO Box 1234
CITY STATE

LOGO
State Logo

RCPT FNAME RCPT M NAME RCPT L NAME February 17, 2017
Address 3
Address 2
Address 1
City Region Postcode

RE RCPT LNAME RCPT FNAME
NPI: 123456789

You are receiving this letter because you have been approved for the Medical Assistance Program and/or for the Electronic Health Record Incentive Program.

ELECTRONIC HEALTH RECORDS INCENTIVE PROGRAM

The State of encourages providers to engage in Health Information Technology and Exchange initiatives and for the most up to date information on state initiatives visit our website.

If you have any questions regarding the Medicaid EHR Incentive program we may be reached at [redacted] or email [redacted]

MEDICAL ASSISTANCE PROGRAM

Welcome to the Medical Assistance Program. You are now an enrolled provider under the terms of the Provider Enrollment and Trading Partner Agreement that you submitted, and may now submit claims for services rendered to Medicaid beneficiaries. Department of Health and Human Services (DHHS) appreciates your participation in providing health care to families who are economically disadvantaged.

Medicaid requires you to continue to revalidate your provider information in Department of Health and Human Services (DHHS) on a continuous basis, at least every two years or upon your license or certification expiration date. Failure to comply may result in termination of your enrollment with Medicaid.

MEDICAID MANAGED CARE

DHHS requires most Medicaid beneficiaries to enroll in a Medicaid Health Plan (MHP). Medicaid Health Plans are required to provide the same services covered under the fee-for-service program, including some services provided in a nursing facility. MHPs may, however, have different prior authorization requirements. Providers should contact a beneficiary's MHP to verify authorization.

STREET ADDRESS 1 - STREET ADDRESS 2 - CITY - ZIP CODE
1642611200000001

MTCPM-1.2.4-1

Figure 3.10.1-179. Sample Welcome Letter. Users populate dynamic content during letter generation.

COR03

The Contractor's solution shall utilize industry standard barcode technology that is approved by the Department.

The evoBrix X Correspondence solution uses industry-standard, DPHHS-approved barcode technology to generate letters. Our solution also supports a wide range of standard barcodes, including UCC/EAN128 (Code 128), which applies a set of application identifiers and associated rules to define a code and Interleaved 2 of 5 (ITF), which is a numeric-only barcode used to encode pairs of numbers into a self-checking, high-density barcode format.

Our Correspondence solution uses ITF for all evoBrix X correspondence, which is compatible with the Brainware optical mark recognition (OMR) engine used by the State. We embed the barcode in all batch print letter jobs and Print and Mail Services can use it for automated sorting, separation, and stuffing of letters into envelopes.

Figure 3.10.1-181 shows a sample barcode, which we can adjust to meet DPHHS-specific requirements. In the sample barcode, barcode positions 1 to 12 (blue color) hold the unique ID generated for each letter recipient. Barcode position 13 (green color) marks the end of a set; the “1” determines the end of the page for each letter recipient. Positions 14 to 16 (purple color) specify the page numbers.



MTCPM-1.2.4-667

Figure 3.10.1-180. Sample Barcode. This barcode includes the standard ITF symbol.

COR04

The Contractor shall utilize letter, notification and other templates for correspondence that are approved by the Department.

The evoBrix X Correspondence solution uses Pitney Bowes EngageOne Designer to create State-approved letters, notifications, and other templates for correspondence. We can configure letters, notifications, and templates to include cover sheets, forms, verbiage, other dynamic content (e.g., return address), and optional run-time attachments at Print Central. We can also design documentation for use with standard mailing or e-mailing based on State requirements.

We provide all templates to DPHHS for formal review and approval prior to implementation. Any subsequent changes made by the State are also subject to the review and approval process before we implement the final versions according to Team CNSI’s standard change management process.

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).

The evoBrix X Correspondence solution sends all documentation and indexing metadata to the DPHHS ECM repository for storage in the centralized ECM solution. The Correspondence solution archives all generated correspondence within the evoBrix X integrated ECM solution. The system uses document metadata and index parameters during the archival process to link the correspondence to business entities to meet regulatory requirements and allow for easy search and retrieval.

COR07

The Contractor's solution shall store all sent or received documents in the ECM.

The evoBrix X Correspondence solution archives all incoming and outgoing documents to the evoBrix X integrated ECM as part of the Correspondence solution. Team CNSI can store documents in FileNet per State requirements (e.g., seven to 10 years). In addition, the evoBrix X system can send all documentation/letters, as well as indexing metadata, to the DPHHS-centralized ECM solution by using the APIs exposed through the System Integrator.

COR08

The Contractor's Correspondence Management Solution must be able to integrate variable data to maximize efficiency.

Document templates designed as part of the evoBrix X Correspondence solution are reusable modular components. As such, our proposed solution integrates variable data (ex: system data, free form text etc.) to maximize efficiency and generates letters based on various input data and system events. The solution couples document templates with conditional logic to produce effective personalized communications.

COR10

The Contractor shall generate applicable notices to members, providers, and other entities (e.g., enrollment/disenrollment notices, requests for information, and program information).

The evoBrix X Correspondence solution generates applicable notices (e.g., generation of RAs for billing providers) to members, providers, and other entities based on system-generated billing payments. The system generates correspondence based on letter templates configured for a specific system event and applies user- and/or event-specific data to generate dynamic letters. Our solution includes automated processes to identify providers that warrant notifications and applies queue-based mechanisms to ensure we generate and distribute correspondence in a timely manner.

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

Team CNSI can fully customize the letter templates, including headers, footers, and verbiage within the letter body, generated by the evoBrix X Correspondence solution to meet DPHHS-specific needs. As such, the Correspondence solution supports State-approved materials for all reading levels (specifically between a sixth and eighth grade level) and for a culturally diverse population using standard forms, templates, and custom verbiage. Team CNSI reviews all letters/correspondence to ensure we meet all DPHHS readability requirements.

COR24

The Contractor's correspondence engine shall be configured to generate, print, and mail enterprise correspondence.

Team CNSI offers extensive experience setting up and configuring EngageOne. The evoBrix X system features a robust framework, which integrates with EngageOne to handle low to high volume letters. Team CNSI provides optimal setup of the evoBrix X Correspondence solution in support of the MT

CPMS project, which includes establishing and maintaining the Pitney Bowes EngageOne Base to generate, print, and mail enterprise correspondence with State-approved Print and Mail Services.

The evoBrix X system uses Pitney Bowes Spectrum Universal Addressing Module to ensure provider postal addresses are current and accurate. Team CNSI also provides optimal setup of the Pitney Bowes Universal Addressing Module to handle high volume transactions. In addition, we can perform periodic patching activities.

In order to keep up with changes in USPS addresses, the Correspondence solution performs updates to the product address database on a regular basis. The evoBrix X system applies address validation processes to ensure increased business efficiency, reduce costs associated to returned mail handling, and ensure associated regulatory and compliance requirements are satisfied.

COR25

The Contractor shall ensure that correspondence, printing, and mailing expenditures that are approved by the Department will be handled as pass-through expenditures.

Team CNSI offers extensive experience configuring, supporting, and maintaining our correspondence engine, EngageOne, to generate correspondence and coordinate the print and distribution services through State Print and Mail Services. As such, we ensure that we handle DPHHS-approved correspondence, printing, and mailing expenditures as pass-through expenditures.

3.10.1.9 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, the type of resource and necessary skill set(s) required for enterprise content management and configuration, and the change management processes associated with enterprise content management. In addition, the Offeror must describe in detail their approach to meet each of the Enterprise Content Management requirements in Attachment F, Requirements Response Matrix. The Offeror simply repeating the RFP requirements does not qualify as a good response as defined in Section 6.1.1 of this RFP.

An Enterprise Content Management (ECM) solution that is configurable, centralized, integrated, and secure, and provides the agility required to adapt to change while ensuring accuracy and timeliness of information, is imperative to the overall success of the MT CPMS project. In addition, a centralized ECM system must accurately and securely support all facets of document management including common and generic features (e.g., ingestion, storage, retrieval, filing, and retention) as part of the MPATH Integration Platform.

Team CNSI's evoBrix X Claims Processing and Management Services (CPMS) solution meets—and often exceeds—the State's ECM requirements. In addition, we offer state-of-the-art technology, in-depth health care experience, and specialized Medicaid subject matter expertise to the MPATH Initiative.

The Team CNSI Advantage

Team CNSI's evoBrix X 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. Our Solution:

- Supports high-speed ingestion and retrieval of imaged and non-imaged content
- Reduces errors in transformation and supports future accessibility and migration to other platforms
- Supports all facets of document management, including ingestion, storage, retrieval, filing, and retention
- Ensures that documents are accessible and distributed only to authorized users through integrated security features

MTCPM-1.2.4-003

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

which are compliant with WS-I Basic Profile 1.0 and WS-Security. The ECM platform is built on these

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Change Management

Team CNSI follows a standard change management process that includes methods for communicating, evaluating, and approving/rejecting changes. This process ensures that we evaluate proposed changes 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, we maintain a log of all changes in the project repository that indicates the disposition and status of all change requests. We employ a similar process to handle changes post-implementation.

Please refer to Proposal Section 3.10.2.1, Project Management, 328 to 365 for more information on change management.

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 X solution allows business users to submit documents related to the Core Claims module through multiple channels, including the secure web portal, email, traditional mail, phone, or fax. This includes all freeform or HIPAA attachment documents that are submitted with or in reference to claim submission activity. Business operations staff scan or manually enter documents received as an email attachment, by fax, or by traditional mail into the system. The image of the paper application is then uploaded and linked to the claims record. See ECM01 for additional information on the OCR/ICR capabilities related to our solution.

ECM01

The Contractor will configure, support and maintain Enterprise Content Management (ECM) functionality (including Document Management, Workflow, OCR/ICR) to meet the business needs of the State's enterprise.

Team CNSI offers extensive experience configuring, supporting, and maintaining our ECM solution to store all system-generated documents or those received by the system using IBM FileNet. A CNSI administrator creates and manages document classes, properties, storage, and metadata that form the

foundation of the ECM solution when handling and managing high volume documents. Our processes meet the business needs of the State's enterprise.

Team CNSI also offers the MAXIMUS ConnectionPoint Customer Relationship Management (*CRM*) system, which comes pre-configured with an ECM, including functionality from Hyland OnBase. OnBase is both a Forrester Wave™ and Gartner Magic Quadrant leader for content management systems. Together, we refer to this functionality as ConnectionPoint throughout this response. ConnectionPoint provides advanced Optical Character Recognition (OCR)/Intelligent Character Recognition (ICR), data perfection for metadata accuracy, and automated linking and transmission to trigger claims and correspondence workflows.

Once sorted and ready for scanning, ConnectionPoint workflow guides the scanning process by assigning a document control number, electronic data, and time stamp. After scanning, the system processes all documents through an initial OCR/ICR process that identifies the document type based on recognized templates, pulls essential metadata (e.g., member name and provider name), and runs basic quality control checks such as looking for the correct number of digits in a member ID or Social Security Number. The advanced OCR/ICR capabilities can recognize form data, handwriting, checkboxes, and multiple font styles. ConnectionPoint provides clear, readable images that meet conditions of acceptability as evidenced in a court of law under Evidence Code §1500 et seq. The images meet all applicable standards of the Association for Information and Image Management (AIIM) (i.e., MS52 1991 and MS53 1993).

Once captured, ConnectionPoint then presents this data to staff member who confirms the data pulled from the document. The system flags potential errors and required fields that could not be automatically pulled. This step, known as data perfection, is significantly faster and more accurate than traditional data entry and supports higher quality data capture in a more efficient process. Together, these validated fields become the metadata used to link each stored document image to the appropriate case within ConnectionPoint and the evoBrix X Core Claims module. This document linking initiates the claims management workflow or a correspondence review task and updates the case record status within ConnectionPoint.

Team CNSI collaborates with DPHHS to confirm the business rules for required metadata, data perfection, and standard document types that need to be individually recognized and coded. As providers often send multiple claims within a single envelope, including claims from more than one patient, our team provides systematic and manual quality control to verify they properly separate and store claims as individual documents with the correct member information. During the imaging process, Team CNSI provides three quality control checks:

- Physical inspection before scanning
- Inspection of all images in the batch post-scanning
- Data perfection of associated metadata used for indexing and retrieving the image

In addition to receiving mailed documents and forms, Team CNSI accepts electronic documentation and claims through the secure inbox on the website, fax, and MedChat in chat upload. We also offer DPHHS an optional, unpriced Provider Mobile App where providers can use their smartphone cameras to digitally capture and upload images of additional or missing claim information directly into ConnectionPoint from anywhere. If selected, we provide both IOS and Android versions of the mobile app. This functionality offers a new level of convenience for providers and reduces the time and burden required when users request additional claims data. Electronic documents go through the same OCR/ICR and data perfection processes as scanned documents to confirm information is accurate and complete before we initiate workflow.

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 Team CNSI ECM solution stores a wide variety of document formats including, but not limited to, Word, PDF, Visio, Excel, PowerPoint, TIFF, and JPEG. Authorized users can download documents directly to their desktop and mobile devices. Additionally, users can also use the document viewing capabilities of IBM FileNet's ICN tool to examine the documents.

Users access and manage downloaded documents from anytime and anywhere across the enterprise on their desktop and mobile devices. Users edit documents using standard document viewing and editing tools used across various enterprises (e.g., 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.

As stated, IBM FileNet features the ICN tool that enables users to access and manage enterprise content across multiple platforms, including desktop, web, and mobile, using a standard web browser without requiring the use of a plug in. Users can also use ICN to download documents 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 Team CNSI ECM solution supports defining role-based access using the concept of Groups or Business Areas. Only authorized staff members can upload, access, preview, edit, and share information relevant to their Business Area through the evoBrix X business user portal. We can also customize and control access 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 DPHHS policies specific to the document they attempt to access and based on roles and privileges.

We support auditing processes 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 works with DPHHS to create an auditing framework, track events pertaining to security, content management, and business transactions, enforce security policies, and track unusual activity.

The Team CNSI ECM solution also enforces automatic document expirations in adherence with DPHHS-defined document retention policies. Team CNSI works with DPHHS to identify the content deemed sensitive and establish document expiration and removal procedures.

Our comprehensive solution enables us to streamline records-based activities, enforce compliance with retention policies, and track unusual activity (e.g., unusual document access activity and sharing of

documents with sensitive information of uploads/downloads of prohibitive data). Using FileNet, the ECM solution captures, classifies, stores, and disposes electronic records according to regulatory requirements.

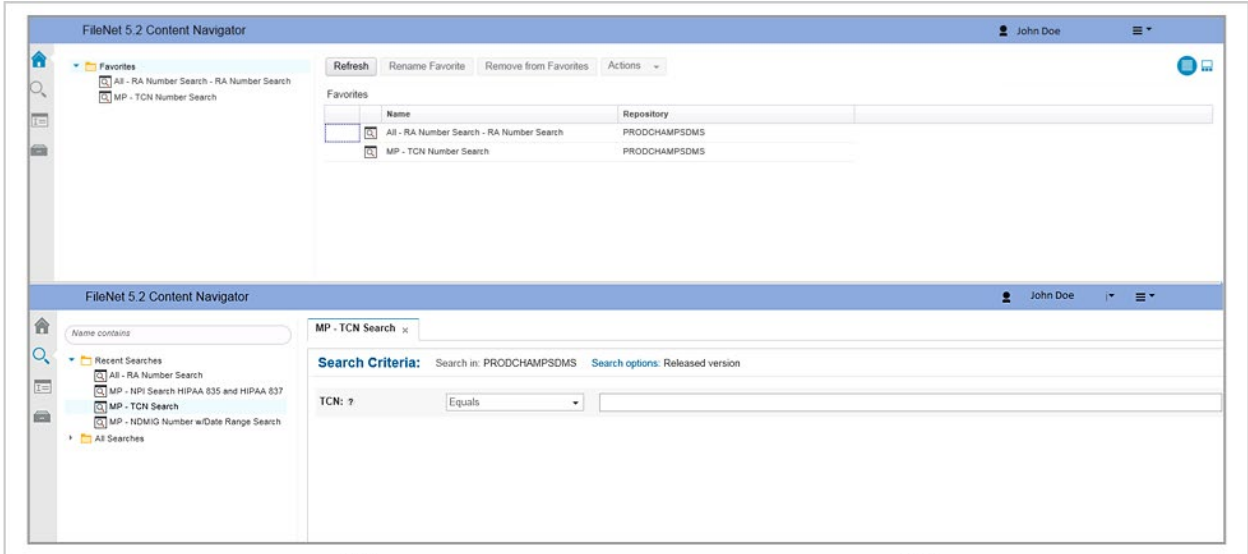
ECM05

The Contractor's ECM solution must include a flexible search engine, including document and content search capabilities.

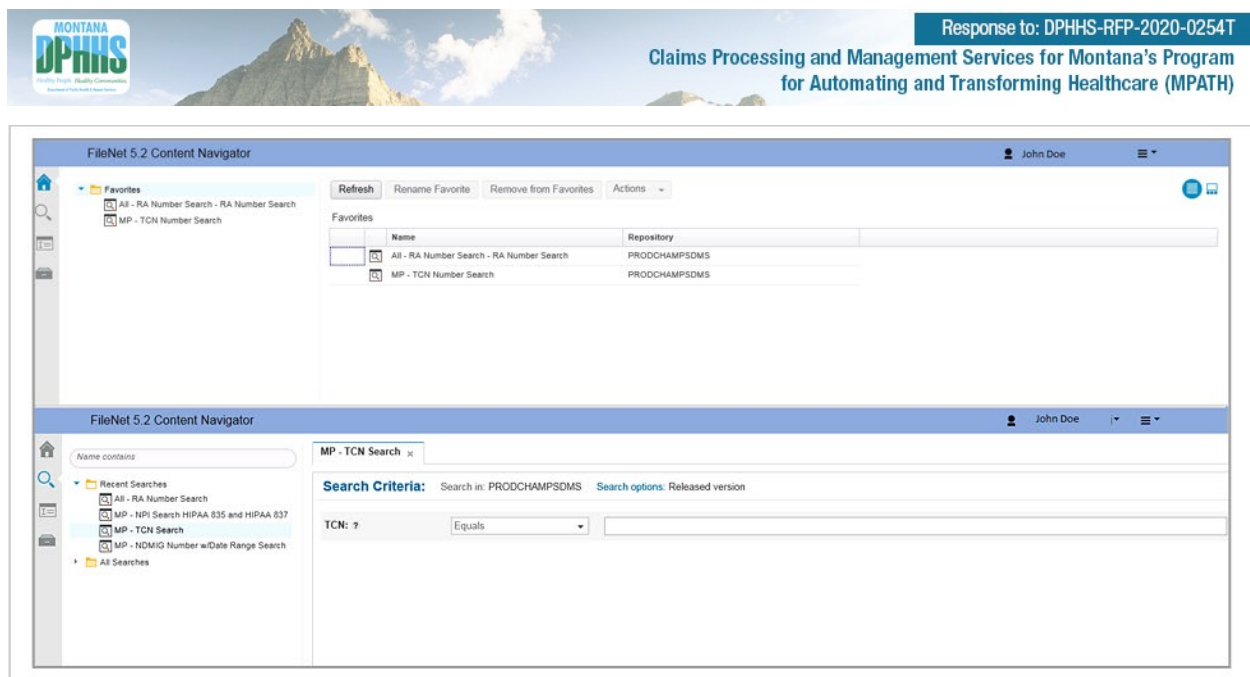
ICN is equipped with several content search options for users, including document search and content search using the indexed parameters. Users perform searches against one or more Document Classes and can include or exclude certain terms, match terms exactly, or search within a specific proximity of words.

Team CNSI stores documents in the ECM solution and tags them with appropriate metadata or document properties, which serve as index parameters. These are used to search for, and retrieve, specific documents at a later date and time. Document Classes are entities (or document types) that are pre-defined 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.

The top portion of Figure 3.10.1-182, shows the ICN landing page, which is customizable by user. The bottom portion shows the Search screen, which users can use to search for specific documents.



MTCPM-1.2.4-143



MTCPM-1.2.4-143

Figure 3.10.1-182. The Team CNSI ECM Solution - ICN. The ICN Home page view and 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 Team CNSI ECM solution. The solution supports a wide range of metadata, including character metadata and dates. These metadata are leveraged during search and indexed for enhanced performance. Associating metadata and indexing are key features in our solution, which enable Team CNSI 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).

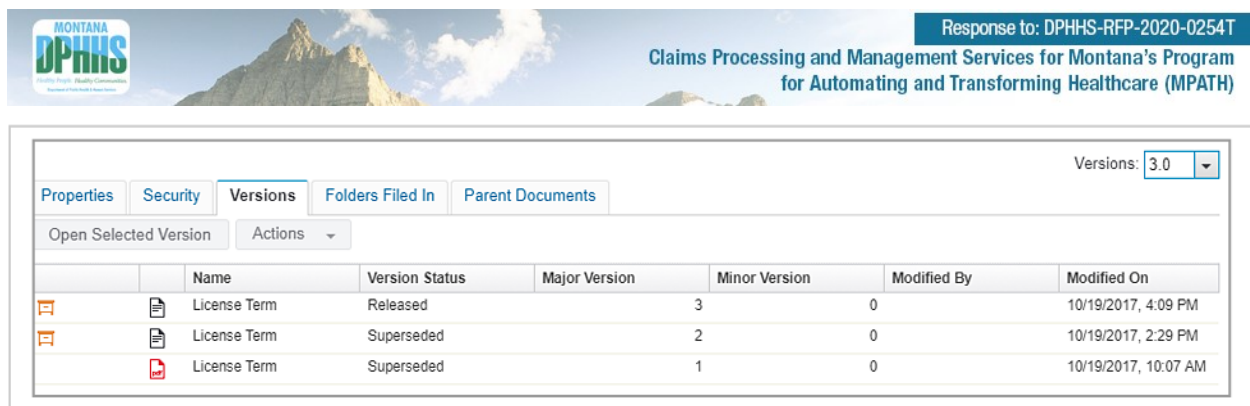
The Team CNSI ECM solution integrates with our Scan and OCR solution, which can connect to a fax server or manual scanning options to process either a document or bulk documents based on DPHHS requirements. Our Scan and OCR solution scans bar codes, associates metadata to scanned documents and archives them in the ECM repository.

The Team CNSI ECM solution derives index parameters based on barcodes and coversheets. Team CNSI offers extensive expertise in fax and scanner integration, including in the State of Michigan, which uses RightFax and high-speed scanners for document intake.

ECM08

The Contractor's ECM solution must support version control.

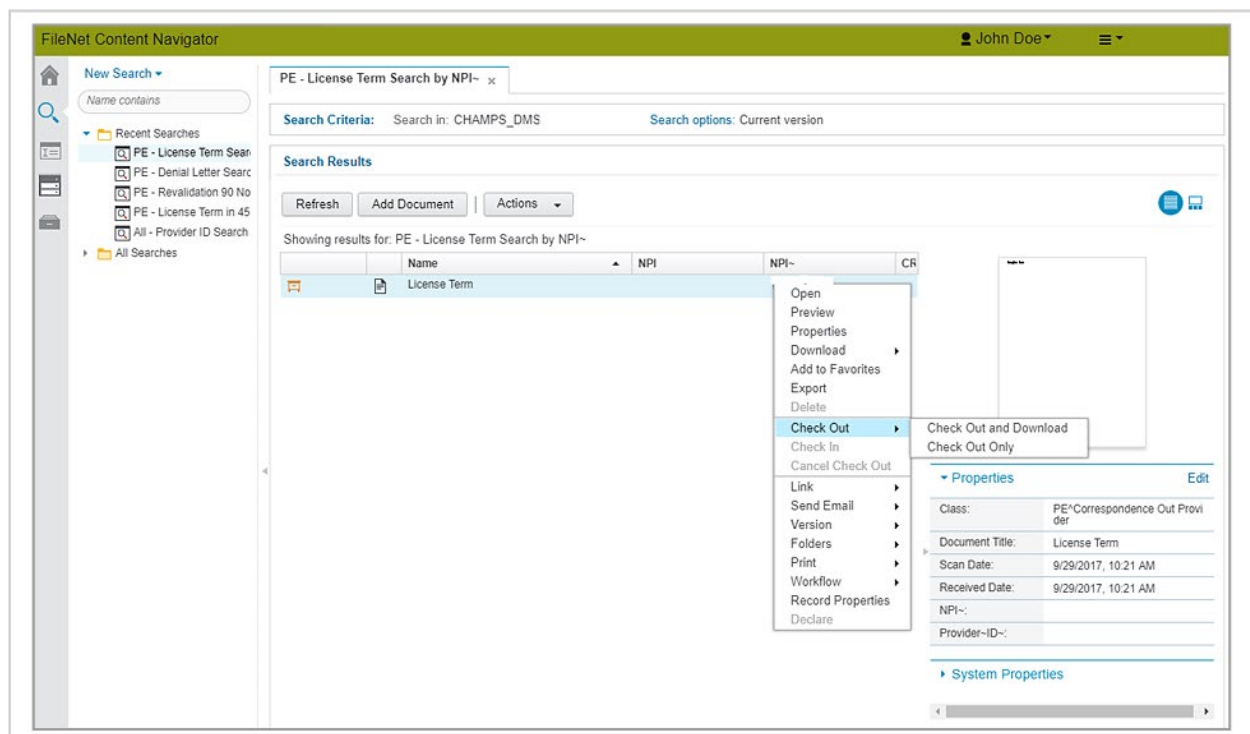
The Team CNSI ECM solution maintains the history of changes to a document and controls the ability of users to change its content. The solution maintains a set of versions for a single document as a version series. Users can check out documents, perform revisions, and check them in. Changes are maintained through version history. Figure 3.10.1-183 shows the version history of a sample document.



MTCPM-1.2.4-679

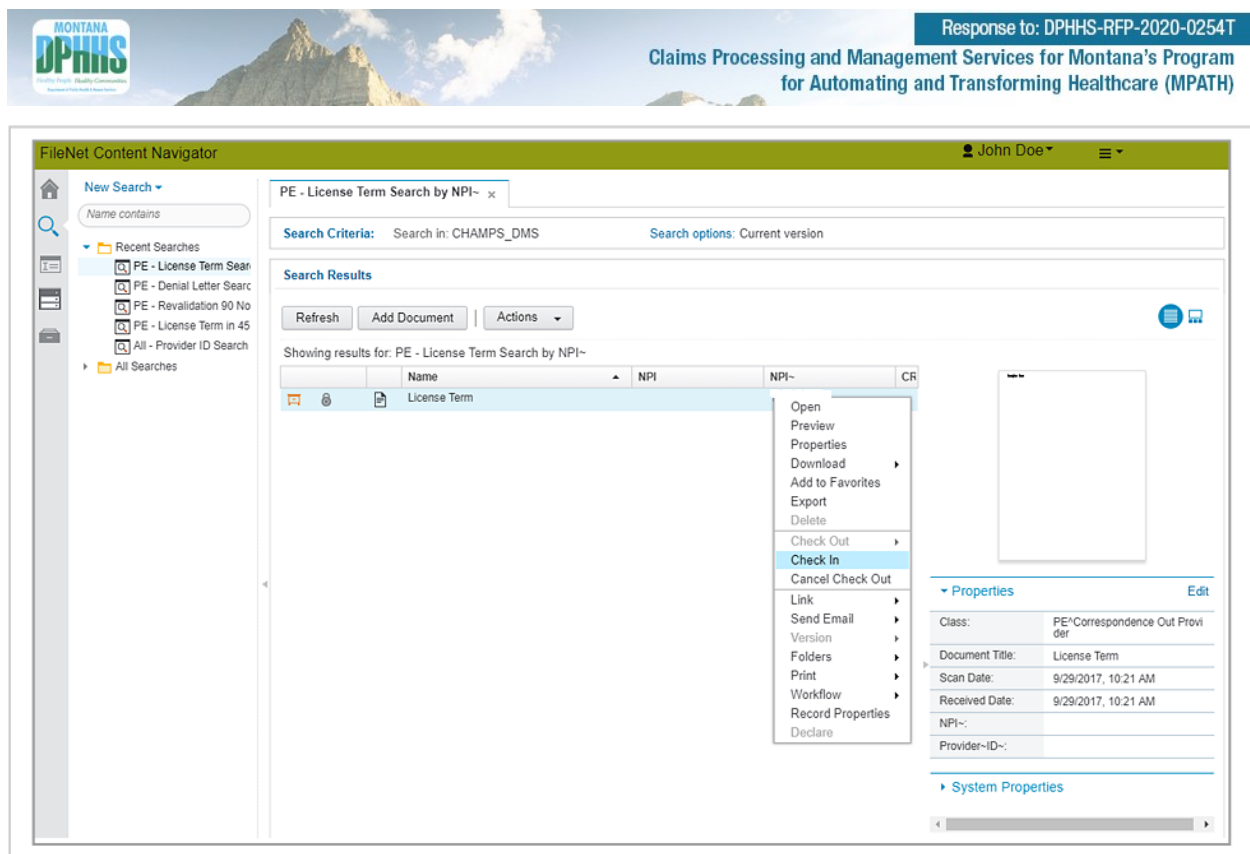
Figure 3.10.1-183. The Team CNSI ECM Solution. This screenshot shows the version history of a document.

Figure 3.10.1-184 and Figure 3.10.1-185 highlight the check-out and check-in functions that users can perform against a document.



MTCPM-1.2.4-681

Figure 3.10.1-184. The Team CNSI ECM Solution. This screenshot shows the permissible actions against a document, including the check-out action.



MTCPM-1.2.4-682

Figure 3.10.1-185. MTCPM-1.2.4-682. The Team CNSI ECM 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 Team CNSI ECM solution supports configuring and streamlining records-based activities and enforces compliance with State and federal document retention policies.

Team CNSI works with DPHHS to determine appropriate retention policies. Once determined, we then configure the Team CNSI ECM solution accordingly.

ECM11

The Contractor's ECM solution must scan all uploaded documents for viruses prior to storage.

The Team CNSI ECM solution scans uploaded documents for viruses based on State requirements by integrating with Symantec Protection Engine 7.8 software through API calls. User-uploaded documents are scanned prior to being archived to the document repository, thereby ensuring their security.

ECM12

The Contractor's solution shall be able to index, link and display incoming correspondence or uploaded documentation with the entity record.

The Team CNSI ECM solution integrates with a fax/scanning solution, reads barcodes, and stores incoming correspondence or uploaded documentation into IBM FileNet along with corresponding index parameters. The documents are also linked to the corresponding business entities based on the index

parameters. Authorized users can view the uploaded documentation through ICN, which uses a powerful, easy-to-use interface to capture, create, organize, and manage correspondence and documentation.

Team CNSI works 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 Team CNSI ECM solution.

ECM13

The Contractor's solution shall send all documentation to the Systems Integration Services module for storage in the centralized ECM.

The Team CNSI ECM solution uses APIs exposed by the System Integrator to send all documentation for storage in the centralized ECM solution. We then archive the documents per DPHHS requirements. By default, Team CNSI archives all generated/received documents to IBM FileNet. Our solution uses document metadata and index parameters during the archival process to link the correspondence to business entities to meet regulatory requirements and allow for easy search and retrieval.

ECM17

The Contractor's solution shall have an integrated electronic document management solution to meet the business needs of the State's healthcare program enterprise.

By default, Team CNSI archives all generated/received documents in IBM FileNet. As stated, we use document metadata and index parameters during the archival process to link the correspondence to business entities to meet regulatory requirements and allow for easy search and retrieval.

In addition, the solution uses APIs exposed by the System Integrator to send all documentation for storage in the centralized ECM solution. We then archive the documents per DPHHS requirements.

ECM18

The Contractor's ECM solution must support event-based document workflows with configurable reviews/approvals (e.g., work type, role, priority, dollar amount) with the ability to collect digital signatures.

The Team CNSI ECM solution provides a user interface for authorized users to search, retrieve, and upload documents. In addition, our solution includes event-based workflows for authorized users to define the rules for reviews/approvals for uploaded documents. Our solution records edits made to document metadata for audit purpose. Usernames are collected and timestamped as digital signatures, which are linked to the document(s) and stored in the solution.

3.10.1.10 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 in detail their approach to meet each of the Workflow requirements in Attachment F, Requirements Response Matrix. The Offeror simply repeating the RFP requirements does not qualify as a good response as defined in Section 6.1.1 of this RFP..

Team CNSI's integrated workflow Application Programming Interfaces (API) leveraging Business Process Model and Notation (BPMN) 2.0 standards supports DPHHS requirements for process definition, execution, monitoring, and management. The evoBrix X platform delivers a proven workflow solution with table-driven configurable rules, task routing, assignment, and tracking capabilities.

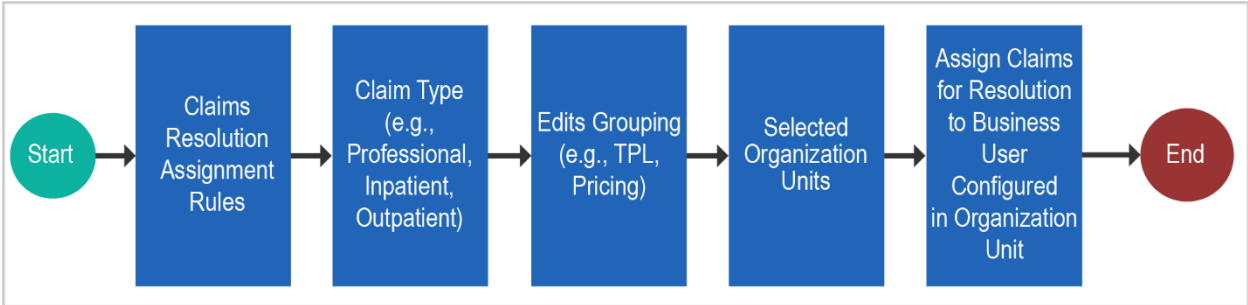
Team CNSI's solution includes a configurable workflow/work queue process that provides the flexibility to define State-specific business process rules, as shown in Figure 3.10.1-186. Our evoBrix X solution includes the Activiti BPMN engine that is configured to support specific processes such as claims resolution. The integration of the Activiti BPMN engine is purpose-driven to meet specific state requirements we have encountered to date and to meet the high-performance requirements for large volume, multi-user claims business processes. We continually update the API related to workflow/work queue as a part of our product roadmap in a careful manner to ensure all our customers can take advantage of its capabilities. Hence, our workflow/work queue capability is not a general use application that supports workflow capabilities of typical commercial off the shelf software products that specialize in just that capability. For any workflow needs outside of meeting claims processing functional requirements, we will collaborate with DPHHS or other state stakeholders as necessary to determine the most efficient approach to address the functionality through the change management process. We mention this to provide context and insight for our proposed solution. Our goal is to meet the requirements with the currently available APIs that is available in the system. Over time, we will execute our product roadmap to continually increase functionality based on DPHHS (and other customer) requirements priorities.

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

MTCPM-1.2.4-195



MTCPM-1.2.4-196

Figure 3.10.1-186. evoBrix X Configurable Workflow Process. The evoBrix X Workflow solution provides the flexibility to configure and automate business processes.

During the DDI Phase, we will coordinate integration elements with the MPATH Systems Integrator to ensure that the necessary elements of the CPMS solution are fully integrated with the MPATH Integration Platform and can exchange data with other MPATH components.

As mentioned, a primary use of our workflow/work queue processes is for Claims Resolution. Claims Resolution items are forwarded to specific Business Organization Units and to a specific user within a group. Different combinations of Claim types will be configured to route the claims resolution to departments specialized in that area.

Workflow Features

Real-time Configuration

Our solution balances the flexibility of workflow configuration changes with the performance requirements of a production claims processing system. The evoBrix X 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 X online screens provide users the ability to modify any existing rule and allow claims resolution to be routed to another business unit/owner. New rules can be defined at any point, allowing additional claims resolution 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 are able to see if any claims resolution 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 X Role Based Access Control (RBAC) security framework that allows or restricts access to specific screens within evoBrix X.

The user will be able to view task items in the task list page in evoBrix X and act upon the queued task. 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 X reporting framework houses various Claims Resolution reports that provide statistics of Claims resolution time taken on a daily, weekly, and yearly timeframe. Reports are scheduled and are available for State-authorized users through online screens.

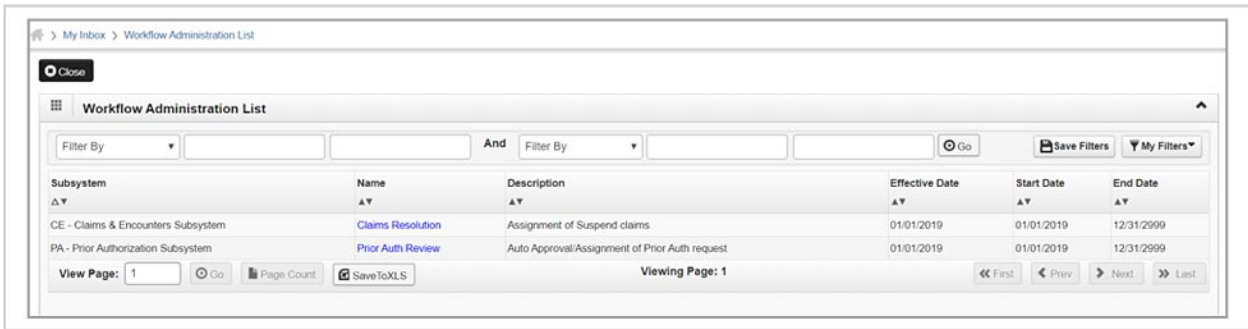
Online Screens

The evoBrix X workflow rules can be configured via a Web portal as shown in Figure 3.10.1-187, Figure 3.10.1-188, and Figure 3.10.1-189. State-authorized users are able to maintain and modify rules based on business process requirements. The evoBrix X 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.

Resource Support

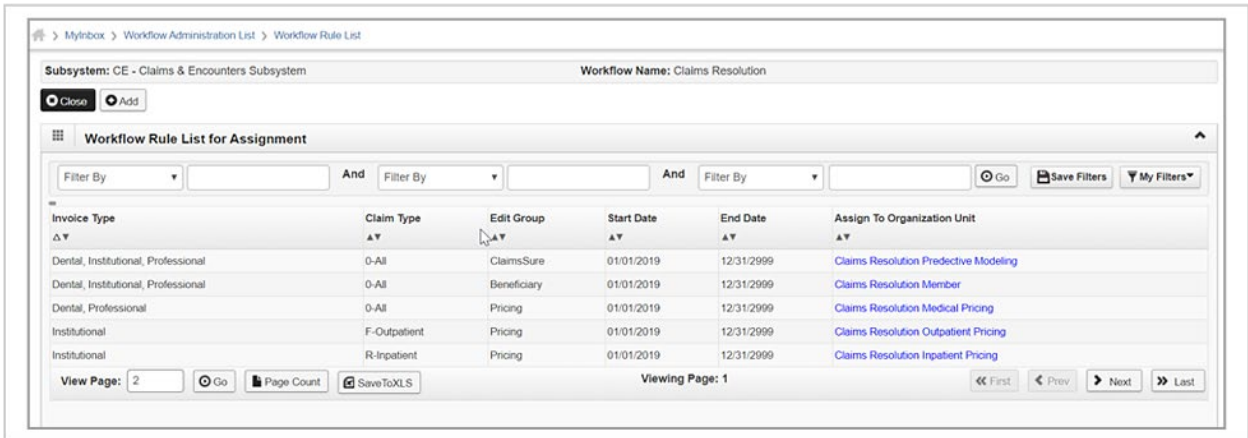
Team CNSI will utilize resources with the following skill sets to effectively manage the configuration, administration, and maintenance of the evoBrix X Workflow solution.

- State staff who will define the process flows and workflow rules will need training on the evoBrix X Workflow solution to ensure they are conversant with the system capabilities
- Familiarity with BPMN 2.0 notation is helpful but not required



MTCPM-12.4-558

Figure 3.10.1-187. Auto Assignment Rules Screen. This screen allows business users to define/modify the workflow process.



MTCPM-12.4-559

Figure 3.10.1-188. Auto Assignment Rules List. This screen enables business users to define/modify the workflow rules for processing.



MONTANA DPHHS
Healthy People. Healthy Communities.
Transforming Healthcare Services

Response to: DPHHS-RFP-2020-0254T

Claims Processing and Management Services for Montana's Program for Automating and Transforming Healthcare (MPATH)

Add Workflow Rule
⌵

Workflow Name: Claims Resolution

Assign To User: Ferguson, Robert

Escalate to Organization Unit: Claims Resolution Escalation 2

Escalation Frequency in Days: 15

Action Type: Assignment

Notify on Assignment: Yes

Start Date: 01/01/2019

Assign To Organization Unit: Claims Resolution Default

Reminder Frequency in Days: 2

End Date: 12/31/2999

Rule Parameter	Relational Operator	Values
Invoice Type	IN	Available - D-Dental - I-Institutional Selected - P-Professional
Claim Type	IN	Available 1-Medicare Hospice 2-Adult Foster Care 3-Family Planning Clinic 4-LHD - A-ICF/MR Selected - G-School Based Services
Edit Group	IN	Available - After Price - Beneficiary - CCI - CO - Duplicate/Conflict Selected - Informational

✓ OK ✕ Cancel

MITCPM-1.2.4-560

Figure 3.10.1-189. Auto Assignment Rule Details Screen. This screen allows business users to assign Organization Units to a workflow process.

Change Management Processes Associated with Workflow

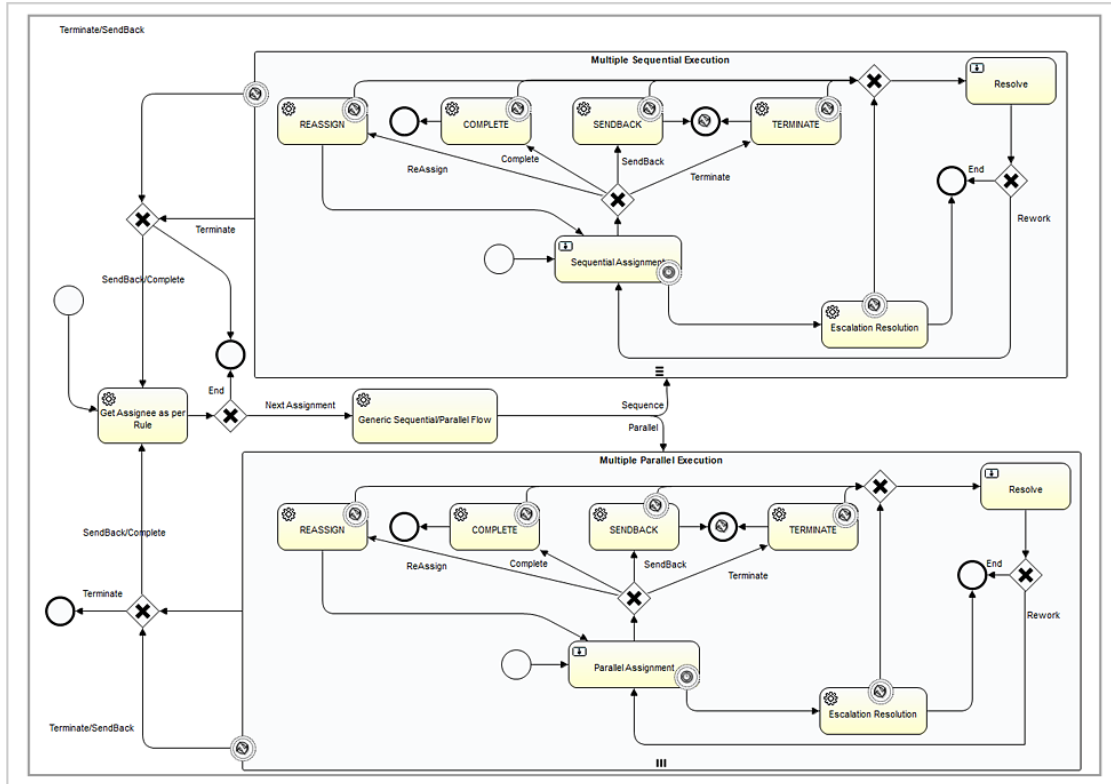
evoBrix X workflow rule maybe made in real time in production by authorized State staff. However, the state or CNSI staff can configure and test workflow rules in a test environment prior to placement in production. This process may be required for complex rules that involve many users and where the state may wish to validate or train staff regarding a change prior to production implementation. For these situations, Team CNSI follows a standard, state-approved Change Management process for the evoBrix X workflows. We handle configuration changes formally through this Change Management processes – workflows are an example of a configuration change. 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.

WKF01

The Contractor's workflow solution shall provide a runtime engine that facilitates process events throughout the work type lifecycle.

The evoBrix X workflow engine processes work queues in real-time, assigns tasks, sends notifications, and provides escalation to management and/or supervisors. Authorized users are able to view their task item in the task list page within evoBrix X 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 X 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.

Workflows executed by the workflow engine are defined by authorized users using a graphical user interface as shown in the sample in Figure 3.10.1-190 The proposed version of our solution makes available the capability to modify workflows that are currently implemented in the evoBrix X solution. Our approach is to add workflows and additional, more general capabilities, as a part of the product roadmap lifecycle. We will seek inputs from DPHHS and other customers regarding requirement priorities and provide additional releases of the capability as a part of our product lifecycle.



MTCPM-1.2.4-197

Figure 3.10.1-190. Sample Process Flow Definition. This screen provides a visual representation of a process flow definition using BPMN notation.

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. evoBrix X online screens provide authorized users the ability to modify any the pre-configured 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 resolutions to be assigned to the right business units or owners.

The evoBrix X workflow screens allow configuration of user assignments to work queues/locations based on attributes of Claim Type and Groups as shown in Figure 3.10.1-191. The combination of Claims Type and Groups define the work types in evoBrix X. In addition, the system has the flexibility to create user roles that are mapped to worker skill and priority. For example, the role "claims resolution – high priority" may be defined to manage high priority claims that require timely action. The role definition enables our solution to place work items in the proper queue based on rules. Team CNSI will define user roles and work in collaboration with the state and map worker skill and priorities in the role scheme. The role scheme will be defined during solution configuration.

Configuration administration screens support the creation of business logic embedded in rules. Rules are maintained by an administrator in real time and support distributions of work based on workloads. The capability to manage work distribution by to age of work is driven based on rules as well. In addition, task dates used for age of work are presented in each user's Inbox for sorting and viewing.

Team CNSI’s evoBrix X 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

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 X workflow rules are configured using online screens. Authorized staff maintains rules based on business process requirements. The evoBrix X 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 view pending applications and re-route them to another business unit or owner. Figure 3.10.1-190 (page 321) a sample of a process definition for a workflow created using our user-friendly Graphical User Interface (GUI). Our solution also provides online screens to monitor workflow status and administer processes.

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 business processes and sub-processes to evoBrix X workflow solution during the solutioning phase. Our evoBrix X CPMS solution comes with pre-defined workflows to automate the business processes. Our API provides the configuration capability of making certain modifications such as workflow steps and triggers. Our team will leverage existing capabilities in addressing DPHHS business processes and subprocesses in order to manage the scope and schedule.

Team CNSI will produce a design artifact called the Detailed System Design Document (DSDD) during solutioning activities to outline the workflow configuration for business processes. Any business processes that cannot be mapped to existing evoBrix X APIs or functionality will be flagged for discussion with the Department to determine the most effective approach to delivering the desired business outcomes. If any of the business processes would require customization of the system, we will collaborate with the Department to determine if the originating process can be changed so that no customization is necessary. If customizations to the evoBrix X solution is needed, these will be best handled through the change control process. Our team will also evaluate new process automation solutions and provide solution recommendations during design. In addition to mapping business processes and subprocesses during DDI, our team will analyze the business processes and provide recommendations on how evoBrix X can improve business performance through automation. If required, changes will be submitted through the project’s approved change control process for DPHHS review and approval. For the state of Utah, we identified more than 500 potential business processes for improvement through the evoBrix X platform. The design information captured in the DSDD’s are used by our staff when creating training materials to support transitioning today’s manual processes to automated processes.

WK F05

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. Workflows 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. Internal dependencies include claims, member, and provider data attributes to support workflow rules. The workflow solution is based on the Activiti framework which provides the capability to integrate external dependencies at the step level for a workflow. Workflow state changes are managed using the Activiti framework. Team CNSI will customize the workflow solution to incorporate external dependencies into the Activiti framework to support the state's business rules.

WK F06

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 3.10.1-192, and can navigate directly to the item that needs action. In addition, access to the reminder content is controlled by evoBrix X RBAC security configuration.

My Reminders						
Filter By		And	Filter By			
Read Status Go			Save Filters		My Filters	
☐ Alert Type ▲▼	Alert Message ▲▼	Alert Date ▲▼	Due Date ▲▼	Read ▲▼	Completed ▲▼	
☐ Approve/Reject User	User (bragg) request for approval	09/14/2009	12/29/2999	Y	Y	
☐ Approve/Reject User	User (bragg) request for approval	09/14/2009	12/29/2999	Y	Y	
☐ Approve/Reject User	User (bragg) request for approval	09/14/2009	12/29/2999	N	Y	
☐ Approve/Reject User	User (bragg) request for approval	09/14/2009	12/29/2999	Y	Y	
☐ Approve/Reject User	User (bragg) request for approval	09/14/2009	12/29/2999	N	Y	
☐ Approve/Reject User	User (bragg) request for approval	09/14/2009	12/29/2999	N	Y	
☐ Approve/Reject User	User (bragg) request for approval	09/14/2009	12/29/2999	N	Y	
☐ Approve/Reject User	User (bragg) request for approval	09/14/2009	12/29/2999	Y	Y	
☐ Approve/Reject User	User (bragg) request for approval	09/14/2009	12/29/2999	N	Y	

Delete View Page: Go Page Count SaveToXLS Viewing Page: 1 << First < Prev Next > >> Last

Figure 3.10.1-191. *Inbox View. The evoBrix X workflow solution provides alerts or messages for a specific user.*

Figure 3.10.1-193 describes the task list view assigned to a user for their action.

Business Process Identifier	Template Name	Subsystem	Start Time	End Time
PA1000001197	Generic Workflow Template - PA	PA	2017-04-19 11:49:50.0	
PA1000001183	Generic Workflow Template - PA	PA	2017-04-13 18:51:27.0	2017-04-13 19:17:06.0
PA1000001182	Generic Workflow Template - PA	PA	2017-04-13 15:28:59.0	2017-04-13 15:36:53.0
PA1000001181	Generic Workflow Template - PA	PA	2017-04-13 14:21:40.0	2017-04-13 14:26:11.0
PA1000001179	Generic Workflow Template - PA	PA	2017-04-13 13:55:56.0	2017-04-13 13:59:03.0
PA1000001178	Generic Workflow Template - PA	PA	2017-04-13 13:48:30.0	2017-04-13 13:51:59.0
PA1000000924	Generic Workflow Template - PA	PA	2017-03-15 20:32:58.0	
PA1000000920	Generic Workflow Template - PA	PA	2017-03-15 17:59:17.0	
PA1000000919	Generic Workflow Template - PA	PA	2017-03-15 17:45:58.0	
PA1000000916	Generic Workflow Template - PA	PA	2017-03-15 16:12:46.0	2017-03-15 16:29:07.0

MTCPM-1.2.4-872

Figure 3.10.1-192. Tasks View. The evoBrix X workflow solution 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 provides the capability to set alerts and reminders. Alerts and reminders are set by authorized users by work types. Rules defined for the workflow determine conditions and triggers for alerts such as new task assignments. Tasks are presented to the user, based on roles, using the My Inbox capability. My Inbox has options to manage the alerts and reminders for each user.

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.

The evoBrix X workflow rules enable workflows to change state based on workflow steps. Status and state information are driven by rules that are maintained by authorized staff who are able to maintain rules based on business process requirements.

WKF09

The Contractor's workflow solution shall provide supervisors access and control of work by type and by user.

Each activity in the process is controlled based on the work by type and by user. Supervisors can be granted a higher level of access within the RBAC security settings which allows them to have access to and control of work by type and work by user.

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 3.10.1-194 shows a sample process flow depicted using BPMN.

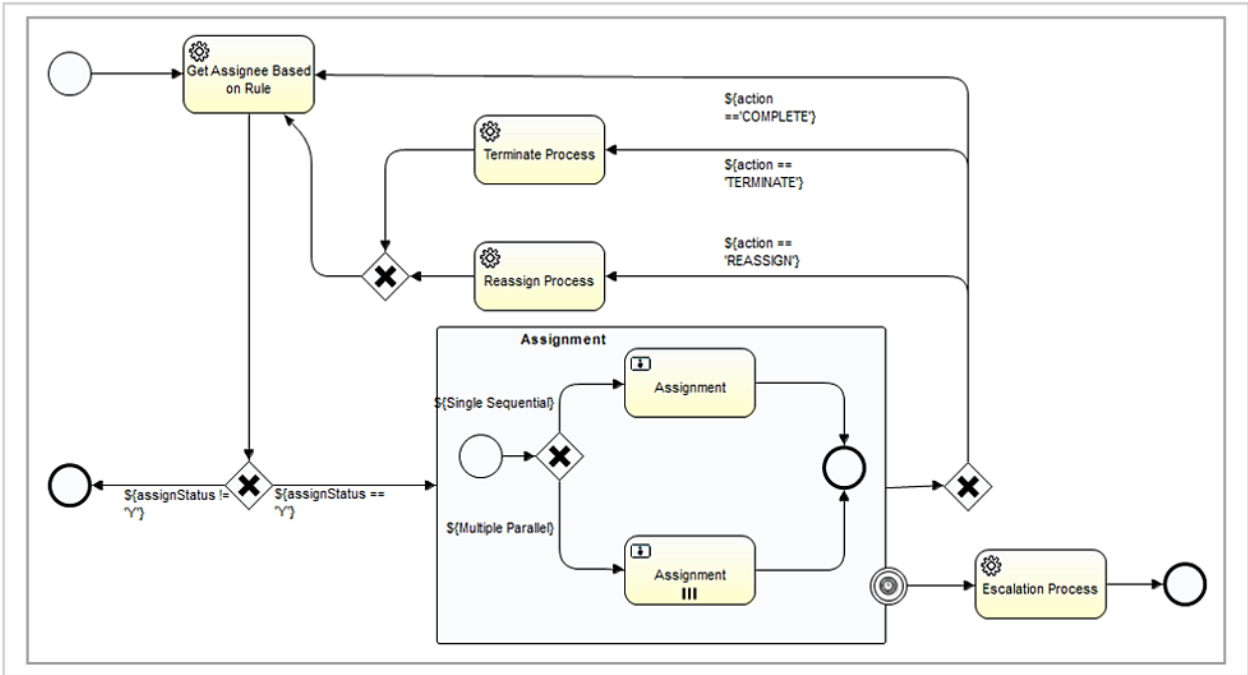


Figure 3.10.1-193. BPMN Notation Usage. A sample process flow using BPMN.

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.

As shown in Figure 3.10.1-194, Sample workflow process, each activity in the workflow will have the state and control within it, which helps to identify the task at various state and allow to present it in various queues. The integration of the Activiti BPMN engine is purpose-driven to meet specific state requirements we have encountered to date and to meet the high-performance requirements for large volume, multi-user claims business processes. Our workflow/work queue capability is not a general use application that supports workflow capabilities of typical commercial off the shelf software products that specialize in just that capability. Workflow knowledge, data, and documentation is shared within Team CNSI’s CPMS solution modules.

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. evoBrix X delivers a proven workflow solution with table-driven configurable rules, task routing, assignment, and tracking capabilities. With these features, evoBrix X 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.

WKF14

The Contractor shall configure, support and maintain a configurable document management, workflow, and ICR/OCR solution that meets the State's requirements. If the Contractor's solution does not include an integrated content management solution that meets the state's requirements, the Contractor will be required to leverage the State of Montana's Perceptive Content Management solution with their overall solution.

Team CNSI's solution provides an integrated, configurable, document management system, IBM FileNet to store, retrieve, and manage documents and images associated with core claims processing. Team CNSI also offers the MAXIMUS ConnectionPoint which provides advanced Optical Character Recognition (OCR)/Intelligent Character Recognition (ICR), data perfection for metadata accuracy, and automated linking and transmission to trigger claims and correspondence workflows. Once sorted and ready for scanning, ConnectionPoint workflow guides the scanning process by assigning a document control number, electronic data, and time stamp. After scanning, the system processes all documents through an initial OCR/ICR process that identifies the document type based on recognized templates, pulls essential metadata (e.g., member name and provider name), and runs basic quality control checks such as looking for the correct number of digits in a member ID or Social Security Number. The advanced OCR/IVR capabilities can recognize form data, handwriting, checkboxes, and multiple font styles. ConnectionPoint provides clear, readable images that meet conditions of acceptability as evidenced in a court of law under Evidence Code §1500 et seq. The images meet all applicable standards of the Association for Information and Image Management (AIIM) (i.e., MS52 1991 and MS53 1993).

Once captured, ConnectionPoint presents this data to staff member who confirms the data pulled from the document. The system flags potential errors and required fields that can't be automatically pulled. This step, known as data perfection, is significantly faster and more accurate than traditional data entry and supports higher quality data capture in a more efficient process. Together, these validated fields become the metadata used to link each stored document image to the appropriate case within ConnectionPoint and the evoBrix X Core Claims module. This document linking initiates the claims management workflow or a correspondence review task and updates the case record status within ConnectionPoint.

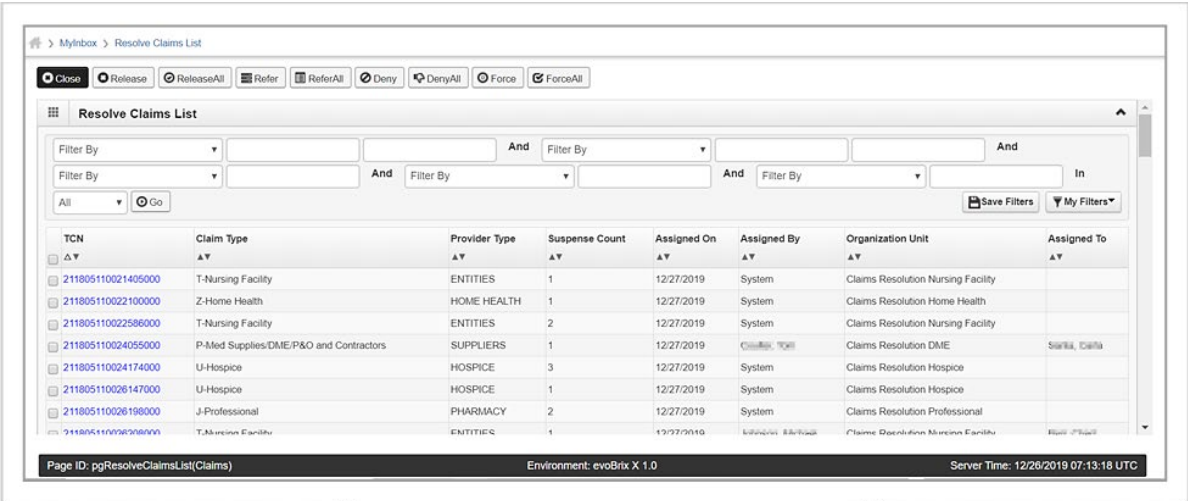
A unique transaction control number (TCN) is assigned to each claim or piece of correspondence and printed on the physical document. As part of our intake process, Team CNSI captures, labels, indexes, and maintains all claims and associated documents, correspondence, and attachments in FileNet. This documentation is easily retrieved by state staff by running a search on FileNet, which is integrated with the Core Claims Module. The Core Claims Module provides intuitive search criteria and permits searches based on file name, TCN, document type, and other related data. Once scanned, the image is saved and uploaded into FileNet for retrieval as needed.

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 evoBrix X solution provides a high-performance, automated, business process/workflow management capability. Our capability includes the establishment of work queues by authorized users

through on-line Web screens. Workflow process steps include state and control information to help to identify the task at various states and to present it in appropriate queues. Since each activity has its own control and data, our solution enables the passing of knowledge and data as an item traverses a workflow queue. Figure 3.10.1-195 provides a view of a workflow task list showing claims that require resolution.



TCN	Claim Type	Provider Type	Suspense Count	Assigned On	Assigned By	Organization Unit	Assigned To
211805110021405000	T-Nursing Facility	ENTITIES	1	12/27/2019	System	Claims Resolution Nursing Facility	
211805110022100000	Z-Home Health	HOME HEALTH	1	12/27/2019	System	Claims Resolution Home Health	
211805110022586000	T-Nursing Facility	ENTITIES	2	12/27/2019	System	Claims Resolution Nursing Facility	
211805110024055000	P-Med Supplies/DME/P&O and Contractors	SUPPLIERS	1	12/27/2019	System	Claims Resolution DME	Startel, Delta
211805110024174000	U-Hospice	HOSPICE	3	12/27/2019	System	Claims Resolution Hospice	
211805110026147000	U-Hospice	HOSPICE	1	12/27/2019	System	Claims Resolution Hospice	
211805110026198000	J-Professional	PHARMACY	2	12/27/2019	System	Claims Resolution Professional	
211805110026198000	T-Nursing Facility	ENTITIES	1	12/27/2019	System	Claims Resolution Nursing Facility	Startel, Delta

Figure 3.10.1-194. Task Listing Screen. Tasks can be reassigned from one worker queue to another.

Workflow tasks can be reassigned from the workflow task list as shown in Figure 3.10.1-196.

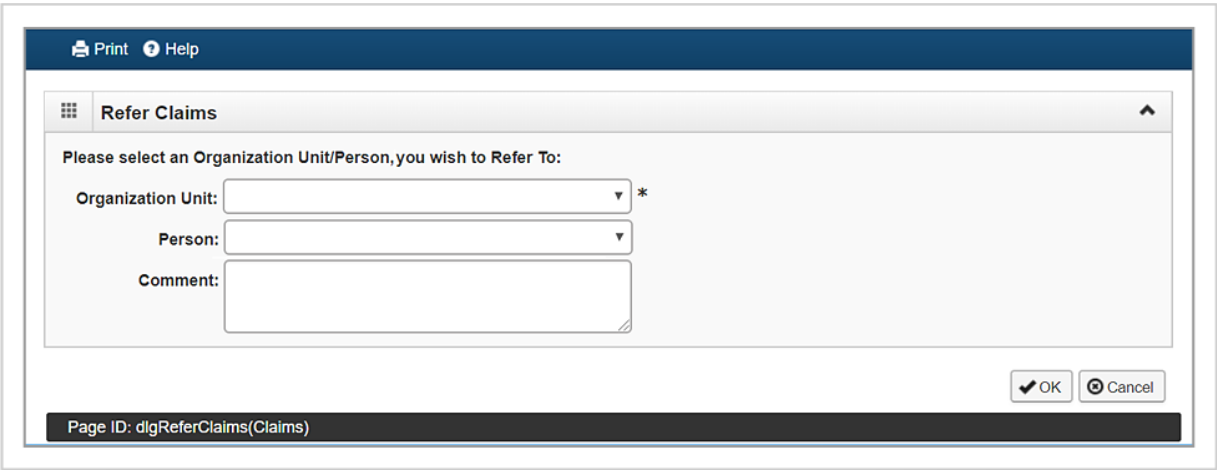


Figure 3.10.1-195. The evoBrix Workflow - Task Reassignment Screen. Tasks can be reassigned from one worker queue to another through this screen.