3. Scope of Services

MAXIMUS offers a comprehensive multi-tenancy SaaS Provider management solution that has been successfully deployed in three states as a standalone module in the Medicaid enterprise. Our solution allows the State to overcome current system and organizational constraints, fully align with the Medicaid Information Technology Architecture, and meet the Seven Standards and Conditions for enhanced Federal Funding Participation. Our experience in modular implementations enables MAXIMUS to understand the intent of the MPATH initiative and to align our solutions to meet the goals.

SECTION 3: SCOPE OF SERVICES

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

All subsections of Section 3 require a detailed written response including a certification of understanding for Sections 3.1-3.8. The offeror must restate the subsection number and the text immediately prior to your written response for all subsections of Sections 3.

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

3.1 Purpose and Intent

3.1 PURPOSE AND INTENT

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

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

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

Regulations at 42 CFR § 433.112(c)(2) provide that COTS-related development costs at the enhanced match rate may only include the initial licensing fee and the minimum necessary to install, configure, and customize the COTS software and ensure that other state systems coordinate with the COTS software solution. When responding to a request for the 90 percent FFP rate for a COTS product, CMS will consider whether the configuration and customization of the product would be kept to minimal levels to achieve full functionality in the most cost- effective manner.

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

X MAXIMUS has read, understands, and will comply will each requirement in this section.

Provider screening and enrollment are key components of the enrollment requirements included in the Affordable Care Act (ACA). Categorizing Providers by risk level, re-enrolling Providers using the

screening requirements, and verifying licenses and other key Provider data places new operational and system challenges on Medicaid agencies as they continue to move forward with implementing the ACA provisions. These requirements call for operational staff to execute and track compliance, as well as additional system functions for data sharing, workflow management, and reporting. Providing this functionality can be taxing on the limited resources of the Medicaid agency.

MAXIMUS provides the system and technical operations necessary to fulfill the ACA requirements, provides streamlined and user-friendly functions to help Providers complete applications, implements a technical platform that aligns with CMS funding requirements, and provides a basis for additional business initiatives to support the Medicaid program.

? did you know MAXIMUS

- Has been working with the Medicaid program for more than 24 years
- Currently provides Provider management service in Iowa, Massachusetts, New Jersey, Tennessee, Nebraska, and the District of Columbia
- Currently operates Provider-facing systems in Tennessee, Nebraska, New York, New Jersey, and the District of Columbia
- Serves the Medicaid enrollment and customer service needs of 59 percent of Medicaid members nationwide
- Has developed a modular Provider Management system that includes ACA-mandated Provider enrollment and screening functions currently implemented in Tennessee, Nebraska, and the District of Columbia

Throughout our proposal, MAXIMUS describes how we use formal processes and procedures to create an operational and technology solution to support the State. We meet the ACA Provider screening and enrollment requirements and provide improved self-service by configuring and deploying our DecisionPoint™ for Provider Management system solution (referred to as our Provider Services solution in this proposal). We are committed to supporting the State's objectives for this project and will demonstrate that our solution:

- Provides a modular Provider Services component for the MPATH effort that can be seamlessly integrated with both legacy systems and new MPATH modules as they become available
- Focuses on configurability over custom development to align with 42 CRF Part 433 to support enhanced federal funding participation
- Achieves full compliance with 42 CFR Part 455 Subpart E and meets the specific business objectives listed in RFP Section 3.9–High Level Scope of Work and Section 3.10–Detailed Scope of Work
- Satisfies all elements of both the MITA 3.0 Provider Data Management Business Process and the elements of the MITA 3.0 Eligibility and Enrollment Management Business Process
- Increases automation and communication between agencies to access data timely and appropriately, removing the need for the volumes of paper that currently move between sites
- Provides software, data and interoperable interfaces enabled through the partitioning of functions into discrete, scalable, reusable components
- Provides configurable business rules, workflow, and other features

In working with clients to meet the ACA requirements and implement solutions to improve the application experience, MAXIMUS has determined that flexibility in solution delivery is critical. MAXIMUS proposes to configure and deploy our flexible SaaS solution for the State of Montana and other participating states. Our solution, which is production proven in three states, offers a system that

meets most of the RFP's functional needs through configuration rather than customization. Our Provider Services solution uses a flexible workflow engine that integrates with the Corticon Business Rules Engine, and uses a service-oriented architecture (SOA) capable, Open Interface Framework to enable reuse, data sharing and configuration.

Our solution, implemented in Tennessee, Nebraska, and the District of Columbia, gives participating States the ability to overcome current system and organizational constraints, fully align with MITA, and meet the Seven Standards and Conditions for enhanced Federal Funding Participation. We highlight the strengths of the people, process, and technology we bring successfully deliver and support the Provider Services solution.

We bring a proven transition methodology that uses an incremental delivery approach resulting in the Provider Services Module Implementation being complete within a 12-month schedule. Every requirement is traced through design, development, and testing to confirm all contract requirements for the PMES have been addressed. The MAXIMUS project management methodology is structured to incorporate best practices, consistency, and reusability by applying the documented principles from the Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK).

MAXIMUS offers a SaaS delivery solution that is realistic, attainable, and appropriate for meeting all operational requirements. Our proven Provider Services system yields the required transaction data, reports, and performance information required for program evaluation and continuous improvement in business operations and accountability. The MAXIMUS solution contains robust reporting and program monitoring capabilities.

The MAXIMUS Provider Services solution is designed to maximize Provider use of the web portal. The web portal functionality includes validation of field input, user authentication, an electronic signature, and a record of the application receipt date. The flexible workflow engine allows us to configure and optimize the business processes required for the entire Provider enrollment and screening process, including the involvement of State staff within the workflow, if required. By configuring our business processes to match the State's requirements, we are confident in our solution's ability to assist the State in processing all Provider applications accurately, and in an expedited timeframe.

Provider Services module Search functionality, combined with the drill down capabilities of the Provider Services module dashboards provide an easy-to-use, comprehensive view of the State's complete Provider community. Our solution is packaged with robust search functionality and provides both a public facing search function (for any user) along with an internal search function that is only accessible by State authorized users. MAXIMUS can extend the capabilities of the publicly available search function to display as much Provider information as is available in the system, or as specified by the state.

MAXIMUS offers a proven turnkey solution that includes the configuration of our base Provider Management solution to meet RFP requirements for enrollment and screening, the conversion of data from the legacy MMIS, and a high-availability technology infrastructure to host the system. We designed our technical solution to prevent system outages and be available on 24x7 basis to Providers, the State, and operations staff. It also contains a full-time always-on replicated environment for disaster recovery that will enable MAXIMUS to meet the required recovery point and recovery time objectives.

The Provider Services solution provides robust capabilities to reduce fraud, waste and abuse through initial enhanced screening, revalidation monitoring, license monitoring, and monthly database monitoring. We built our solution to meet the CMS Provider management-related business objectives and system review criteria including the enhanced screening requirements required by CFR 455 to prevent fraud, waste, and abuse.

MAXIMUS experience in the modular certification efforts of two states demonstrates our ability to help states achieve federal certification of the Provider management module. MAXIMUS offers states a proven Provider Services module based on a modern software platform that meets the certification criteria for the Provider Management Module, as released in the Medicaid Enterprise Certification Toolkit (MECT) that includes the Medicaid Enterprise Certification Life Cycle (MECL) published by CMS and updated in July 2017.

Careful planning is the cornerstone of our successful past transfer/turnover activities —as both the incoming and the outgoing contractor. We will work closely with the State to accomplish a seamless turnover for the Provider Services module. We approach project turnover with the same meticulous planning, best practices, and communications strategies that we do for project start-ups. We tailor our closeout activities to build a complete Turnover Plan unique to each project such as that for Montana and other participating states.

3.2 State Vision, Guiding Principles and Objectives

3.2 STATE VISION, GUIDING PRINCIPLES AND OBJECTIVES

X MAXIMUS has read, understands, and will comply will each requirement in this section.

Traditionally, the components of Medicaid information systems did not always work together in an integrated fashion, making it difficult for states to administer Medicaid programs and implement initiatives that could impact the overall service delivery approach for the program. To foster better collaboration among the components of Medicaid systems and support new program implementation, the Centers for Medicare & Medicaid Services (CMS) has moved forward with a standards-based and conditions-based approach to approving enhanced Federal Funding Participation (FFP).

CMS has issued standards and conditions that states must meet for Medicaid technology investments to be eligible for enhanced FFP. We designed the MAXIMUS Provider Services solution to support the goals of the Seven Standards and Conditions for Enhanced Funding and foster better collaboration with states, reducing unnecessary paperwork, and focusing attention on the key elements of success for modern systems development and deployment.

In planning the implemetnation of Montana's Program for Automating and Transforming Healthcare (MPATH), the state is looking to leverage technology to share and exchange information as a critical aspect of their healthcare delivery. The focus on improved access to health care and ultimately improved health outcomes is supported by the requirements related to modularity, interoperability of related systems and data, and streamlined workflows to support the delivery of health care services. Through implementation of best-in-class modular solutions, care related activities can include evidence-based decision support, quality management, and outcome reporting across the modules included in the MPATH project.

To support the State's vision, guiding principles and objectives, MAXIMUS is proposing to implement a Provider Services module built on modern technologies focused on supporting data integration, functional reuse and interoperability. We support our implementation approach using a system methodology based on agile principles and industry standards. The combination of our flexible technical architecture and rapid product implementation methodology will bring Montana a Provider Services module to support the long-term objectives of the Program. It will allow the state to obtain enhanced federal funding participation both now and in the future as additional MPATH modules are implemented and connected to the overall Program infrastructure.

3.2.1 State Vision

3.2.1 State Vision

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

MAXIMUS recognizes that the Provider Services module is only one component of the Montana MPATH project; however, we will confirm the business and technical solutions are designed to work with the other systems, and meet the statutory and regulatory requirements. This will support efficient and effective operation of the program with a focus on improving access to health care services and treatment outcomes for Montanans. *Exhibit 3.2.1-1: The MAXIMUS Solution Supports the State Vision* summarizes how our Provider Services solution supports the Department in meeting their vision.

CMS Condition	How the MAXIMUS Solution Supports the Department's Vision
1. Modularity Standard	▪ MAXIMUS-developed Open Interfaces Framework supports interfaces to any partner systems ▪ Business Rules are separated from core functions via the rules engine ▪ Formal systems development methodology aligned with Montana standards ▪ Service-based framework designed with web services
2. MITA	▪ Architectural foundation is already based on the MITA maturity model ▪ Business processes optimized and flexible ▪ Standardized business model focuses on streamlining administration of the program ▪ Data-driven framework for flexible business rules and configuration ▪ Enhanced federal funding participation
3. Industry Standards	▪ HIPAA-compliant solution ▪ Follows industry standards for data exchange ▪ Robust testing plan and mitigation strategies to be followed, including use of our Regression Test Harness designed specifically for our solution ▪ Use case-driven approach for testing and validation of user stories ▪ 508(c) compliant application with periodic testing
4. Leverage	▪ MAXIMUS Provider Services solution is a production-proven system with robust functionality and a modular framework aligned with MITA ▪ Service-based architecture with open standards ▪ Integration of Commercial Off-the-Shelf (COTS) components to reduce risk ▪ Solution is highly flexible and can be implemented in other states with minimal configuration ▪ Open Source products used where practical ▪ Flexible solution promotes lower cost of ownership and reduces operations costs
5. Business Results	▪ Our solution provides for the accurate and timely processing of provider applications and revalidations using a modern framework, including automated workflow ▪ Business processes were designed first – followed by the technology implementation. This approach results in the flexibility in processes over time ▪ Provider web portal provides self-service features for providers and allows interaction between providers, the State, and MAXIMUS ▪ Dashboards and reports provide user community with up-to-date status of the program to assist the users in determining the performance of the program and what steps should be taken to improve program performance ▪ Disciplined product release methodology for future enhancements and upgrades

CMS Condition	How the MAXIMUS Solution Supports the Department's Vision
6. Reporting	▪ Our Provider Services solution provides dashboards for users and is packaged with predefined reports exportable to Word, Excel, or PDF ▪ Workflow engine provides ability to track business process outcomes and measures worker performance ▪ System dashboards provide drill down capabilities on key data within the system
7. Interoperability	▪ Our Provider Services solution Open Interfaces Framework promotes seamless integration with external systems ▪ SOA architectures enables web-service interactions through the ESB to all partner systems
8. Access to Data	▪ The web-based framework of our solution enables providers, operations users and other authorized staff to access provider information ▪ Data consolidation and web-services enable seamless integration with other partner systems either directly or through the ESB ▪ Data sharing features enable provider data to be exposed to end consumers through provider directory functions and other interface capabilities

Exhibit 3.2.1-1: The MAXIMUS Provider Services Solution Supports the State Vision. *Using technology and program expertise, MAXIMUS delivers flexibility in our business processes to support current and future integration needs.*

3.2.2 Modularity Business Objectives

3.2.2 Modularity Business Objectives

The MPATH Program objectives include:

- An enterprise system that is flexible to quickly adapt to the dynamic, evolving needs of existing programs and support new regulations, policies and innovations
- An enterprise system founded on business driven technical solutions
- An enterprise system where business processes are automated wherever possible
- An enterprise system that provides centralized access to data
- An enterprise system that includes data analytics tools to support the use of clinical data to measure treatment outcomes and the changing health status of members.
- An enterprise system that includes standardized and automated electronic communication and data exchange capabilities
- An enterprise system that includes a Master Client Index (MCI)
- An enterprise system that integrates data from disparate systems to enable enterprise wide-program management

MAXIMUS understands the business objectives that underlay the move away from large monolithic systems into modules aligned to business processes. We were the first vendor to embark on a modular Provider Services solution when we began the design and development of a modern web-based solution to support all Provider Management functions conducted by Tennessee Medicaid outside of the traditional MMIS. We implemented the first phase of this standalone functionality in late 2011 and continued to add functionality even before other MMIS modules where identified by CMS. Because we designed our system to pull provider management functions into a new system platform on a different infrastructure from the State's MMIS, our implementation model specifically allows integration between our solution and other Medicaid systems.

MAXIMUS is the only vendor to have three production modular implementations. We have proven that modularity can be achieved in a cost-effective manner that allows for growth, expansion, and configuration as the Medicaid Program requirements change.

Because of the implementation model we used, we took steps to provide seamless integration using web-services and an Enterprise Services Bus (ESB) with the MMIS. We also built a data-sharing interface with the State's Credentialing Verification Organization (CVO), CAQH, so that individual Providers could use existing registrations with Managed Care Organizations (MCOs) to facilitate enrollment into the Medicaid Program. We currently share data with the MCOs and Providers that are registered through CAQH so they do not have to submit additional application documents.

While we completed most of development work well before the latest CMS certification standards, our solution is designed to support the goals of the Seven Standards and Conditions for Enhanced Funding by fostering better data sharing and integration, reducing unnecessary paperwork, opening new communication channels and focusing attention on the key elements of success for modern systems development and deployment.

We have enhanced our system and integrated new COTS products into our solution as we implemented modular provider services solutions in Nebraska and the District of Columbia. We continue to modernize our solution so that we can provide our customers with the latest technology and functions. Using this foundation of system functions and modern day technologies, we support data integration and interoperability, and our system development methodology uses agile principles based on industry standards. The combination of our flexible technical architecture and product implementation methodology will bring Montana a fully compliant Provider Services solution with enhanced functionality designed to increase efficiency and decrease costs.

To meet Montana's modularity business objectives, we a solution that includes: the use of open interfaces and exposed application programming interfaces (API); the separation of business rules from core programming; and the availability of business rules in both human and machine-readable formats. We will configure and enhance our solution for Montana using a formal system development methodology and open, reusable system architecture to support more easily changed and maintained systems. It will integrate and interoperate with other required State systems.

The table below demonstrates how our system complies with the MPATH Project Objectives.

MPATH Program Objectives	MAXIMUS Solution Compliance
An enterprise system that is flexible to quickly adapt to the dynamic, evolving needs of existing programs and support new regulations, policies and innovations	▪ Cloud-based hosting provides cost-effective, redundant and highly scalable platform that can be adjusted based on program needs ▪ SOA architecture enables seamless integration will all MPATH components using standard web-service interfaces ▪ Business rules defined within the rule engine enable dynamic configuration of business rules as the Medicaid Program changes ▪ Support for enhanced functions using COTS products for imaging, document management and rules engine

MPATH Program Objectives	MAXIMUS Solution Compliance
An enterprise system founded on business driven technical solutions	▪ MAXIMUS solution was built specifically to manage State Medicaid Provider data ▪ MAXIMUS solution was built as a data integration platform to enable data sharing with a Credentialing Verification Organization (CVO) ▪ Business Processes are based specifically on ACA-mandated requirements and state requirements based on production use ▪ COTS products are included to meet specific business needs and integrated into the larger solution as requirements evolve
An enterprise system where business processes are automated wherever possible	▪ MAXIMUS solution is based on production use and operational performance with automation focused on productivity and accuracy ▪ Automation can be integrated with manual tasks when necessary based on partner systems and data availability ▪ Configurable workflow keeps applications and screening continuously transparent and moving
An enterprise system that provides centralized access to data	▪ Use of industry standard database management system, Microsoft SQL Server Enterprise Edition, allows the applications and support tools to connect directly for real-time updates and reporting ▪ Provider web portal provides self-service features for providers with real-time updates to data ▪ Centralized reporting solutions with Dashboard and ad hoc reporting capabilities ▪ Web services enable data to be exposed to the ESB for sharing and reporting
An enterprise system that includes data analytics tools to support the use of clinical data to measure treatment outcomes and the changing health status of members.	▪ COTS-based reporting subsystem with data analytics, standard and ad hoc reporting ▪ Dashboards and reports provide user community with up-to-date status of the program to assist the users in determining the performance of the program and what steps should be taken to improve program performance ▪ ESB integration allowing access to data across MPATH modules
An enterprise system that includes standardized and automated electronic communication and data exchange capabilities	▪ Automated communications sent to providers based on workflow steps and outstanding tasks ▪ Outreach as an integrated component of electronic communication ▪ COTS-based document management product allows customization and configuration of documents ▪ Open interface standard enables wide variety of data exchange options
An enterprise system that includes a Master Client Index (MCI)	▪ Integration with MMIS allows a single provider identifier to be used across the MPATH modules ▪ Standardization on national code sets such as NPI allow for data normalization
An enterprise system that integrates data from disparate systems to enable enterprise wide-program management	▪ Integration of the Provider Services module with the ESB enables data sharing across all MPATH modules ▪ Integration with data warehouse module supplies an enterprise-wide view of data

As a leader in implementing modular provider service solution, MAXIMUS is uniquely qualified — we understand the requirements, and more importantly, understand the issues and barriers that surface during a modular implementation. We have implemented three unique MMIS interfaces and have worked closely

with our customers to streamline functions, identify and cleanse problematic data and help the operations organization move into alignment with the new screening and enrollment requirements from CMS.

3.2.3 Guiding Principles

3.2.3 Guiding Principles

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

Table 3.2.3 MPATH Guiding Principles

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

The use of a modular approach to replacing the various components of the legacy MMIS environment brings upon the need for extensive planning, coordination and partners who understand and agree with the approach. MAXIMUS focuses on supporting our customers in changing the Medicaid Program so there is more emphasis on service delivery and enabling technology that simplifies many of the administrative functions. With a proven record, MAXIMUS has demonstrated that we understand how to implement a modular solution, and we support data integration and system interoperability through mechanisms that support SOA and legacy installations. Based on our experience, we fully expect to need to provide some data integration outside of the ESB. Our flexible solution will enable the Provider Services module to be implemented ahead of the other MPATH modules and then integrate using the ESB as new modules are implemented.

The table below addresses each of the MPATH Guiding Principles and provides details on how we aligned our solution with the MPATH project guiding principles. MAXIMUS has reviewed each item and we fully understand and will comply with each requirement.

MPATH Guiding Principles	MAXIMUS Solution Alignment
Flexible Enterprise Technology Platform	▪ Cloud-based hosting ▪ ESB integration ▪ Multiple access methods
Centralized Data Repository	▪ SQL Server repository ▪ Data integration with Data Warehouse
Business-driven Enterprise transformation	▪ Rules engine with business rules defined ▪ Workflows customized to each state using configurable business rules ▪ Customizable data requirements to align with state-specific applications and various program requirements
Process Automation	▪ Automated workflows for all operational tasks ▪ Automated inbound and out bound interfaces ▪ Automated provider communications
Data Integration and Interoperability	▪ SOA-based architecture with ESB integration ▪ Open Interface standard allows additional data integration options for use with legacy systems
Data Consistency Across the Enterprise	▪ Data conversion and cleansing as part of initial implementation ▪ Data governance compliance in conjunction with the System Integrator
Progressive Technology	▪ Industry-standard products for development and database environments ▪ COTS products for add on functions including document management, imaging and rules engine ▪ Cloud-based hosting allows scalable hosting environments
Member and Provider Centric Focus	▪ Provider self-service tools ▪ Provider data sharing across MPATH modules ▪ Ability for members to access provider directory
Cost Efficiency and Effectiveness	▪ Fixed price module based on RFP requirements ▪ Pricing variables based optional components ▪ Fixed maintenance and operational costs

3.3 Modularity Approach and Blueprint

3.3 MODULARITY APPROACH AND BLUEPRINT

X MAXIMUS has read, understands, and will comply will each requirement in this section.

As a vendor who has already implemented a Provider Services solution in a modular fashion, MAXIMUS understands the complexity of implementing a module where connection points are with both legacy and new system components. Often times this is made more complicated when interface points start out with legacy systems but the long-term vision requires the ability to utilize SOA-based exchanges. Our experience in Tennessee, Nebraska and the District of Columbia have lead us to develop a project schedule and methodology specifically focused on implementing the Provider Services solution in a manner where it can seamlessly integrate with the legacy environment and then move to modern integration when the ESB and other components are ready. We understand the challenges of implementing our solution in conjunction with the System Integration Module and will work closely with DPHHS and the System Integrator to align the work schedules to minimize the rework necessary and

reduce the overall project risk of updating functions already in production. Each of our three implementations supports both legacy interfaces as well as modern web service integrations. MAXIMUS has extensive experience in integrating our system in this manner and we will use lessons learned to support the State and their other module vendors in successfully implementing the vision for the MPATH.

3.3.1 Modularity Approach

3.3.1 Modularity Approach

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

MAXIMUS fully supports DPHHS modularity approach where multiple, strategically timed procurements and implementations will take place. We agree that this approach will allow Montana to pick "best in breed" solutions for particular services and will open up competition to a much broader set of vendors. As the first vendor to implement modular provider services solutions, MAXIMUS has been an early partner with numerous states in planning and implementing modular provider service solutions.

We have been successful in implementing our provider services module into legacy environments with the specific plan to expand the options for data sharing and system interoperability as new modules are implemented. In Tennessee, our module utilizes the ESB to trade data with the MMIS as well as provide an interface with the EDIFECS platform to enable providers to initiate and receive HIPAA mandated transactions directly from the provider portal. We are also continually implementing new data sharing and recently integrated data sharing with the state's new dental benefits manager.

MAXIMUS is committed to working closely with DPHHS to implement our solution as quickly as possible while minimizing risk and providing a platform that is proven to support enterprise-wide integration.

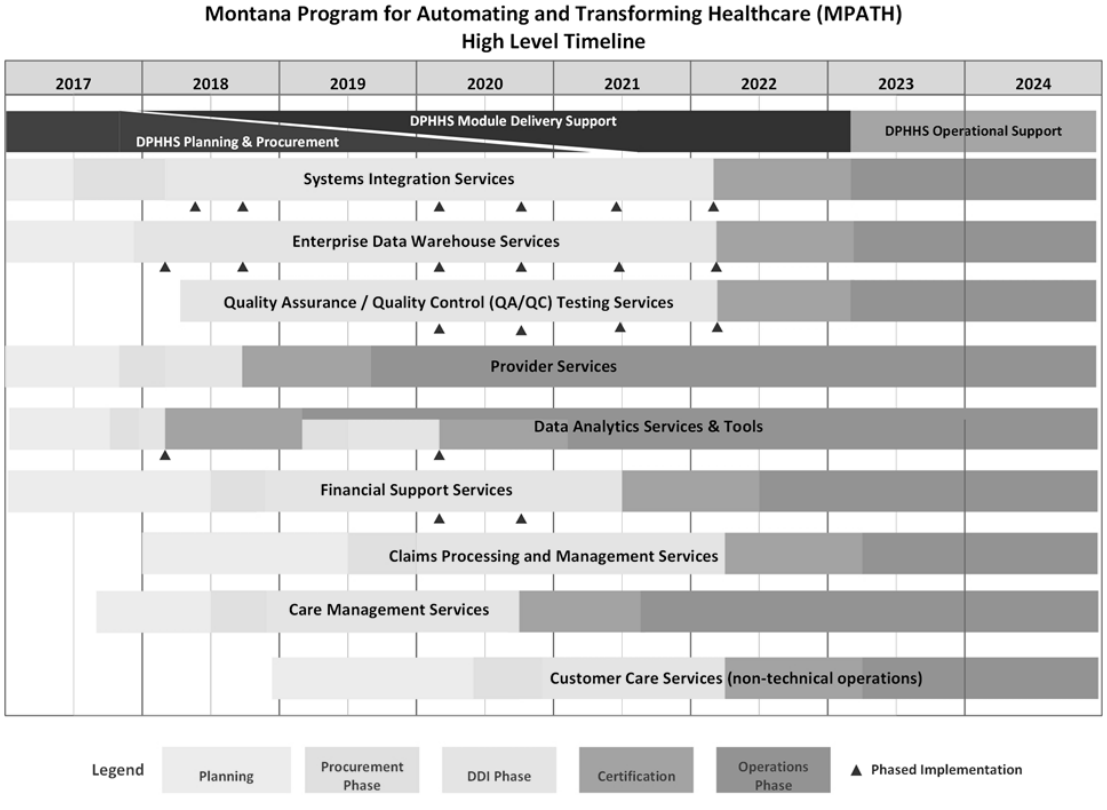
3.3.2 Modularity Blueprint

3.3.2 Modularity Blueprint

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

Figure 3.3.2.1 MPATH Modularity Groups

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



MAXIMUS has closely studied the State's plan for implementing the MPATH modules. We believe it represents a well thought-out strategy and aligns the various modules according to their ability to be implemented in relation to the other modules. We agree that the Provider Services Module makes sense to implement early given the ability of MAXIMUS to implement the solution within the legacy environment. We have proven that our system can be implemented as an integrated but standalone service of the MMIS while offering the State the ability to configure the data requirements and business process workflows according to Montana policy. By implementing the Provider Services module early, the State can apply lessons learned from the effort to future procurements, enable data sharing through the ESB as the System Integrator provides governance and access, and help pilot enterprise-wide functions before they are rolled out to the remaining MPATH Modules.

Specifically, implementing the MAXIMUS Provider Services module in the planned timelines will:

- Provide the ability to align the provider services module with legacy system requirements
- Enable online provider self-service for new applications, revalidation and data updates based on specific edits related to provider and application type
- Offer expanded capabilities and options for providers including the ability for expedited applications for MCO-only providers or other provider types
- Pilot web-services data integrations through the ESB as the system integrator provides governance and access
- Document lessons learned as functions are moved to the ESB and legacy interfaces are deactivated

The experience MAXIMUS has with modular implementations makes us uniquely qualified to not only implement the provider services module but to understand how the other module implementations might affect our schedule and plan. Because we have experienced firsthand the issues that surround modular implementations, our approach and plan includes services that will help us minimize the overall impact of new modules being added to the overall enterprise and take into account new requirements related to modular projects. We believe it is critical for the State to understand that decisions made as part of the implementation of other MPATH modules could have major implications for the Provider Services module and the rework that may need to occur. We also think that understanding and planning for the uncertainty of being the first business module implemented using the new SOA infrastructure is critical.

MAXIMUS has reviewed the implementation plan for the Provider Services module taking into account the RFP requirements and our experience in Tennessee, Nebraska, and the District of Columbia. Based on our assessment, we believe that seven months is not adequate to ensure a successful implementation of the Provider Services module. Our major concerns around the proposed schedule include:

- **MMIS interface coordination** – the design, development and testing for the MMIS interface takes regular meetings, extensive coordination, and constant focus. Due to the constraints on the MMIS vendor, our experience indicates that extending the available timeframe is necessary to verify the interfaces can operate without issue.
- **Deliverable review and comment** – there are a large number of deliverables that will continuously be developed and submitted for review and approval. We have found that large documents take review meetings and walkthroughs that consume valuable schedule time. Extending the overall timeline allows adequate review and approval to occur.

- **Conversion clean up and testing** – we have found in every modular implementation that the legacy MMIS data contains anomalies that must be resolved. Providing enough testing cycles using conversion data is the best method for identifying anomalies and allowing the data to be cleansed prior to production conversion.
- **Integration testing** – there never seems to be enough time for testing. We have found that a minimum of 6 weeks of UAT and an additional period for operational readiness is generally needed for the State to approve production. This realistic time period for testing exceeds what would be permitted within a seven-month schedule. As the schedule is extended, additional testing cycles can be conducted which reduces risk, improves quality, and benefits the overall implementation effort.
- **System integration requirements** – the Provider Services module will be the first business application to use the MPATH SOA infrastructure. Since the integration requirements will be defined during the implementation effort, additional time will allow processes to be properly defined, vetted, and adequately tested. An additional concern is the potential that a large amount of functionality will have to be developed to cater to the legacy environment and then redone when the infrastructure and governance is completed.
- **Experience** – it is important to note that no modular Provider Services implementation has been completed in seven months. While some modules, such as the PBM, might be implemented in seven months, the requirement review effort and SOA integration items would make it difficult if not impossible to implement the Provider Services Module in seven months.

MAXIMUS has closely reviewed the RFP requirements, made assumptions about the unknown items in the system integration area, and planned the data conversion and MMIS interface tasks. As described in the questions and answers, the Department expects the vendor to submit, as part of its proposal, a plan and approach that supports a successful implementation. Therefore, MAXIMUS is proposing a schedule and approach we believe supports the successful implementation of the Provider Services module. We believe a twelve (12) month timeframe provides the best alternative for implementing the module taking into account the risk associated with the parallel implementation of the System Integration module and the realistic amount of time a regular Provider Services implementation requires. In addition, there are unknown variables present for states outside of Montana that will use this procurement. We believe this timeframe also accounts for any discrepancies related to how the project must be executed for each state.

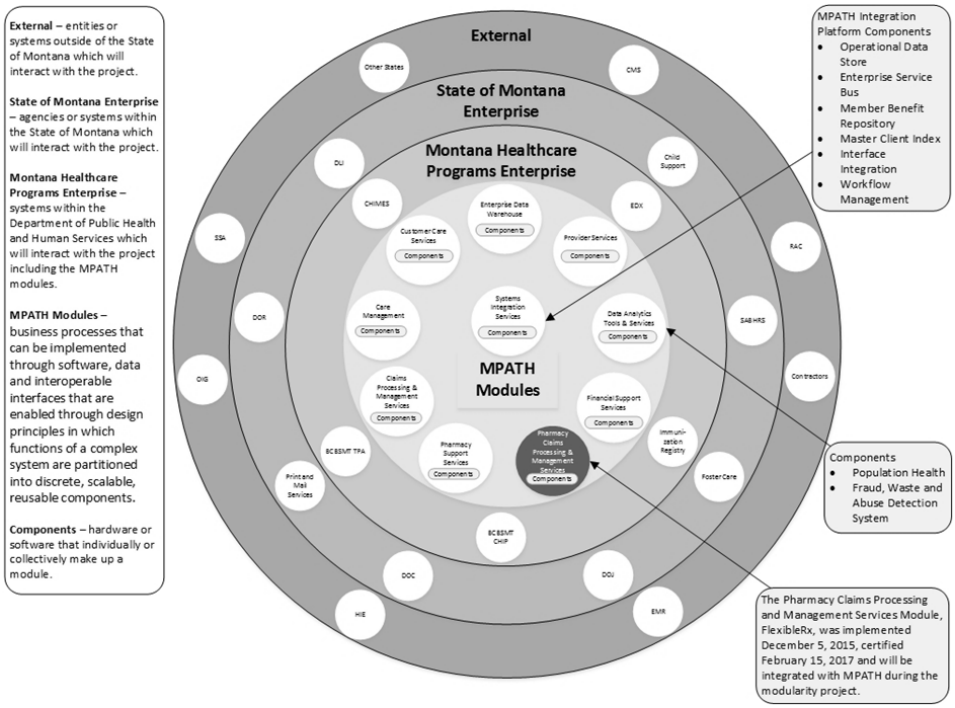
MAXIMUS is committed to meeting this timeframe and delivering the best solution for both the short and long-term goals of the Program for Montana and the Participating States.

3.3.3 MPATH Modules

3.3.3 MPATH Modules

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

Figure 3.3.3 MPATH Integration Layers



Systems Integration Services (SI)

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

Provider Services (PS)

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

Enterprise Data Warehouse (EDW)

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

Data Analytics Services and Tools (DA)

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

Financial Support Services (FSS)

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

Claims Processing and Management Services (Claims)

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

Care Management Services (CM)

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

Customer Care Services (CCS)

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

Pharmacy Claims Processing and Management Services (PBMS)

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

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

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

Pharmacy Support Services (PSS)

The Pharmacy Support Services module (PSS) encompasses two objectives. DPHHS will procure new components to replace the legacy Drug Rebate Analysis and Management System (DRAMS) and Retrospective Drug Utilization Review (RetroDUR) systems. Additionally, in order to reduce the dependency of FlexibleRx, the pharmacy claims processing and management system on the existing legacy MMIS, the current pharmacy claims processing and management services

> contractor, Conduent will complete enhancements to integrate multiple services including member eligibility, provider, financial transaction processing, and centralized data storage and reporting into the MPATH Integration Platform.

As a long-term partner with states in supporting their Medicaid Programs, MAXIMUS understands each component of the Medicaid Program, and how the various components work together within the larger program. As a company, we work closely with states assisting with the management of both member and provider communities. Our existing contracts necessitate close coordination with other partner vendors, especially the MMIS and eligibility systems where we have already implemented bi-directional interfaces. Our detailed understanding of the different business areas prepare us for implementing our Provider Services module in a manner where it fully supports provider management but also includes data sharing interfaces with a variety of other partners.

Throughout our history, we have been required to implement our solutions within the larger context of the Medicaid program. Our existing projects require extensive data integration to both the MMIS and Medicaid eligibility systems and we often must provide our data to a variety of external partners including the state's decision support systems and managed care organizations. In addition, the implementation of our modular solution results in the creation of a central Provider directory that has allowed us to provide public-facing search features to assist members in finding health care providers. We currently support Enrollment Broker and Member Management modules in 21 states and Provider services in an additional 9 states. Each of these contracts requires MAXIMUS to implement standalone solutions that operate within the Medicaid Enterprise. This unique blend of experience provides gives us a solid understanding of the business process lines and data sharing requirements for each module.

The Provider Services module is planned to be the first of the business modules that is implemented as part of the MPATH initiative. It is a great candidate to lead the modernization effort since normalized clean provider data is a building block for many of the other modules. We expect to work closely with the System Integrator and the Enterprise Data Warehouse vendors as the ESB is implemented and we pilot the use of the ESB to share data with the data warehouse. Along with the implementation of the Provider Services module, we anticipate the System Integrator will be implementing data exchange capabilities that we will use to enable connectivity to the Pharmacy Claims Processing module as well as to prepare for the implementation of the remaining MPATH modules. As the Claims Processing Management Services and Customer Care Services modules are being implemented, MAXIMUS will work closely with those partners to confirm accurate provider data is available and to expose web service interfaces so that data can be shared.

We believe that accurate provider data is pivotal for the success of the overall MPATH project. MAXIMUS is committed to working with DPHHS and all of the MPATH partners to successfully implement the various modules and confirm interoperability and data sharing.

3.3.4 Exclusions

> 3.3.4 Exclusions
>
> The Montana Department of Public Health and Human Services (DPHHS) will release a number of RFPs for software, components and services to replace legacy Montana Healthcare Programs services and components. Contractors awarded the Systems Integration Services, Quality Assurance/Quality Control Testing Services and Independent Verification and Validation Services contracts are precluded from bidding on any other module within the MPATH Program scope
>
> DPHHS identified exclusions for the Quality Assurance/Quality Control Testing Services contractor to ensure independence from any and all module prime or subcontractors.

DPHHS used the following key principles to make exclusionary decisions:

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

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

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

Table 3.3.4 MPATH Contractor Procurement Exclusions

Module Name	SI	QA/QC	PS	DA	FSS	Claims	CM	CCS	PSS	EDW
Systems Integrator (SI)	Open	Excluded	Excluded	Excluded	Excluded	Excluded	Excluded	Excluded	Excluded	N/A
Quality Assurance/Quality Control (QA/QC) Services	Excluded	Open	Excluded	Excluded	Excluded	Excluded	Excluded	Excluded	Excluded	N/A
Provider Services (PS)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Data Analytics, Tools and Services (DA)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Financial Support Services (FSS)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Claims Processing and Management (Claims)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Care Management Services (CM)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Customer Care Services (CCS)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Pharmacy Support Services (PSS)	Excluded	Excluded	Open	Open	Open	Open	Open	Open	Open	N/A
Enterprise Data Warehouse (EDW)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Legend
Excluded: Awarded vendor(s) are excluded from bidding on subsequent modules within the overall program.
Open: Awarded vendor(s) are not excluded from bidding on subsequent modules within the overall program.
N/A: Not applicable. Service will be provided by the State of Montana Information Technology Services Division.

MAXIMUS understands the need for a variety of partners to provide services to support a large modernization effort like the MPATH initiative. We agree that the State must verify that no conflicts of interest exist and that different project functions remain independent from other components. We understand and agree that the State will release a number of RFPs for software, components, and services to replace legacy Montana Healthcare Programs services and components. We agree that Contractors awarded the Systems Integration Services, Quality Assurance/Quality Control Testing Services, and Independent Verification and Validation Services contracts are precluded from bidding on any other module within the MPATH Program scope. MAXIMUS certifies that we will adhere to the exclusion standards defined in the RFP and will take steps to eliminate any potential conflicts of interest. We do not intend to submit proposals for the Systems Integration Services, Quality Assurance/Quality Control Testing Services and Independent Verification and Validation Services contracts.

MAXIMUS has successfully worked within the Medicaid Program for many years and our core competency is providing independent quality services. We have read and understand the DPHHS key principals used to make exclusionary decisions and certify that we will comply with each requirement in this section. We have verified that our subcontractor on this project does not have potential conflicts of interest, and will not be submitting proposals for the Systems Integration Services, Quality

Assurance/Quality Control Testing Services, and Independent Verification and Validation Services contracts. We certify that our subcontractor will comply with each requirement in this section.

3.4 Technology Standards

3.4 TECHNOLOGY STANDARDS

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

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

Table 3.4 High Level Requirements for the MPATH Program

Requirements	Requirement Definition
Alignment with the Seven Standards and Conditions	Comply with the Standards and Conditions, set forth by CMS, in order to receive enhanced FFP.
Flexible Enterprise Technology Platform	Utilize enterprise architecture governance process that incorporates MITA standards to accommodate future programs and initiatives.
Automated workflow management	Provide centralized, configurable workflow solution that allows for workflow creation, execution and automation.
Enhance program reporting and data analytics	Implementation of Data Analytic tools and services to enable accurate, real-time data and reporting that will meet changing business and management needs. The solution should be enterprise centric, which would enable other health care and program data typically not found in an MMIS to support enterprise decision-making.
Centralized access to data	Provide real-time and centralized access to members, providers, benefit plan(s), claims, and case management data for the Department's programs including Medicaid, Healthy Montana Kids Plus (HMK Plus), Healthy Montana Kids (HMK) (the state's Children's Health Insurance Program CHIP)), Montana Health and Economic Livelihood Partnership Plan (HELP), Mental Health Services Plan (MHSP), Passport to Health, Patient Centered Medical Home (PCMH) and waiver services. Ability to enhance decision-making and increase management efficiencies.
Data integration and interoperability	Provide interfaces and components that are reusable and follow industry and national standards for data exchange. Procured solutions will include exposed APIs for easy integration with other enterprise solutions.
Standard Communication Protocols	Standardized protocols for electronic communication will allow DPHHS to move to electronic options for communications using modern services such as Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) including a Web Portal. In addition, standardization will support the ability to provide messaging in Multilanguage and multi-literate formats.
Progressive technology	Provide progressive technology, e.g., mobile apps, text messaging, etc., that increase communication venues and encourages member and provider interaction with Montana Healthcare Programs.
Automate Manual Processes	Automate a majority of manual processes to replace human interactions with automated configurable business rules.
Administrative Simplification	Adhere to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II).
Mechanized Claims Processing and Information Retrieval Systems Final Rule	Meet requirements specified in the Mechanized Claims Processing and Information Retrieval Systems (90/10) Final Rule (42 CFR 433), specifically related to configuration and customization of COTS software.

Requirements	Requirement Definition
Standards and Implementation Specifications for Health Information Technology Final Rule	Modularity approach is aligned with industry standards adopted by the Office of the National Coordinator for Health IT described in Final Rule (45 CFR part 170, subpart B).
HIPAA and HITECH	All solutions and services shall be fully compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-1919) and Administrative Simplification (Subset of Title II) requirements in effect as of the date of release for the RFP and with any changes that subsequently occur, unless otherwise noted. The Contractor shall sign a Business Associate Agreement, included in the contract, which is subject to HIPAA and HITECH regulations CFR 45 parts 160 and 164.

X MAXIMUS has read, understands, and will comply will each requirement in this section.

State Medicaid Agencies have the difficult task of providing quality health care services to diverse populations of members taking into account rural versus urban differences as well as confirming all members have access to required services. These activities are supported currently by numerous systems that have been implemented to manage Medicaid populations and pay providers for their services. As the Medicaid Program has shifted toward improved access to health care and begins to focus on quality treatment outcomes, the current set of systems and data sharing functions are not adequate to support the major shift in health care focus that states like Montana are making. The approach of creating a program to implement components and services that improve access to healthcare and treatment outcomes for Montanans is the next step in the evolution of how Medicaid and health care services are provided with the added benefit of setting up technology infrastructure that focuses on business process, data sharing, and system interoperability. This approach will make it possible for Montana to implement an enterprise-wide program management system that utilizes claims and clinical data to measure treatment outcomes, improve the health status of Montanans, and reduce healthcare costs.

MAXIMUS is in full agreement on the Montana system replacement approach. We have been an advocate of separating business processes from the legacy support systems to increase flexibility, enable program design changes, and provide a variety of service models that can be tailored to each state's unique needs. Both our member and provider solutions have always been separated from the legacy systems and we have always worked closely with our customers and other vendors to create data integration and sharing processes between our systems and the legacy Medicaid systems. To support the MPATH Program goals of implementing components and services that improve access to healthcare and treatment outcomes for Montanans, MAXIMUS offers several modular components within the MPATH Program that utilize flexible enterprise technology platforms. This will enable Montana to more effectively meet current business objectives with platforms to support the evolving complexities of individuals served by Montana Healthcare Programs.

To align with the technology standards of the MPATH initiative, MAXIMUS is offering a Provider Services module built on a modern technology platform designed with a variety of functional capabilities to enable a comprehensive yet streamlined provider management process. We are proposing a SaaS implementation which provides a proven turnkey solution that includes the configuration of our base Provider Services solution to meet DPHHS requirements for provider services. We also provide the conversion of data from the legacy MMIS and a high-availability cloud-based technology infrastructure to host the system. Our technical solution is design for high-availability to prevent system outages and will be available on a 24x7 basis to Providers, DPHHS, and operations staff. It also contains a full-time always-on replicated environment for disaster recovery that will enable MAXIMUS to meet the required recovery point and recovery time objectives.

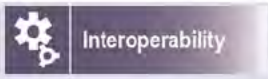
MAXIMUS Provider Services Solution

- *User-Experience Focus*
- *Workflow Driven*
- *Configurable System*
- *Reporting and Business Intelligence*
- *Open Interface Design*

The MAXIMUS Provider Services module provides a flexible design with a focus on user experience and configurability. We achieve this by taking advantage of a mixture of mature technologies, COTS products and a system architecture built to change and adapt. Our solution uses Progress Corticon Business Rules engine and MicroStrategy to support business intelligence in a loosely coupled manner. To further enhance our ability to provide a configurable solution, we support the COTS products with a custom built Business Process (workflow) engine built on the .NET framework. To provide interoperability with other systems, we expose well-defined service components based on SOA interoperability to support data exchanges using any method that a trading partner prefers. The MAXIMUS solution takes advantage of open standards to efficiently integrate with disparate systems and we have successfully integrated with all required trading partners in our three current Provider Services modular implementations. We intend to implement our solution within the MPATH framework and will work closely with DPHHS and its partners to deliver the seamless integration of our system.

We designed our modular architecture using a service-oriented model with a variety of technical components to enable ease of use by bringing web-based functionality to both Providers and internal users. Our solution adheres to HIPAA and NIST standards, which enables the secure storage, transport, and use of data. We have incorporated modern tools that enable data sharing from a variety of sources using an open interface platform. Our data management features provide all data in a robust repository supported by a business intelligence software suite. In reviewing the technical standards required by the RFP, we believe we closely match the requirements. The following table identifies how our solution aligns with the MPATH technology standards.

	MPATH Standard	MAXIMUS Solution Alignment
CMS 7 Compliant	Alignment with the 7 Standards and Conditions	Our solution follows the guiding principles of MITA 3.0 and is compliant with the CMS 7 Standards and Conditions for Enhanced Funding. We have proven our system can be implemented outside of traditional MMIS in a modular fashion while acting as a functional conduit to support data integration and interoperability between legacy systems and Medicaid data partners. Our SOA and web services design allows for flexibility in interface technology, which enables the quick integration with any new MPATH module implementation.
Flexibility	Flexible Technology Platform	We designed our Provider Services solution using a series of business rules that trigger workflow steps to move Provider applications through the enrollment, screening, and decision-making processes. We have focused on making these items configurable so they can be changed quickly and efficiently to align with Program needs. The flexibility in business rule and workflow definition aligns the system with program requirements, enables new initiatives to be supported immediately, and allows process improvements to be continually implemented. We aligned our approach directly with the MITA standards.
Workflow	Automated Workflow Management	Our solution has a business process framework, which we refer to as the Business Process Engine, which enables execution and maintenance of process workflows. The Business Process Engine automatically executes the appropriate business process model based on the inputs from the business rules engine. The flexible workflow engine allows us to configure and optimize the business processes we support. Configurable business workflows guide users — both Providers and internal operations staff — through the tasks and activities necessary to complete required processes for reviewing enrollment and screening results and finalizing the enrollment process. We use business service orchestration to enable these workflows, and include external communication processes to allow automated reminders, notices and other documentation to be distributed electronically to Providers based on their actions in the system and the associated status of those actions.
Reporting	Enhance Program Reporting and Data Analytics	We package the MAXIMUS solution with an analytics and reporting platform. For reporting and analytics, we use two COTS products: Microsoft SQL Server Reporting Services (SSRS) and MicroStrategy BI. These two applications serve closely related purposes and play a very important role in Provider service processing. Our system provides dashboards, standard reports, custom reports, ad hoc reports, and analytics that we developed over the course of system implementations in Tennessee, Nebraska, and District of Columbia. Together the products and features enable program reporting and data analytics for all aspects of the Provider Service module.

	MPATH Standard	MAXIMUS Solution Alignment
	Centralized Access to Data	The MAXIMUS solution includes a consolidated data repository that houses all data and information produced during the Provider application, enrollment, certification and licensing processes as well as all related data generated by multiple State agencies and Trading Partners. Authorized users are able to store, retrieve, and report on all data generated by functional processes and activities. Our reporting platform will enable reporting across all data contained in our data stores.
	Data Integration and Interoperability	Our Open Interface Framework will provide DPHHS with existing interface functionality "out-of-the-box," with the ability to easily configure any unique interfaces required for the Project. Our experience with connecting our solution to legacy MMIS applications allows us to cross-reference the data in our system to the key values needed by our trading partners. Our data integration approach exposes APIs and web services for easy integration. We also support legacy interfaces through secure FTP file exchanges and/or other methods that trading partners support. MAXIMUS understands that flexibility is key to success and we focus on new technology but also understand the limitations of legacy systems.
	Standard Communications Protocol	Our solution contains a communications layer that controls the flow of information among the other layers within the system. A diverse mix of communication processes are supported by the application including a variety of modern services such as Simple Object Access Protocol (SOAP) and Representational State Transfer (REST), stored procedures, database triggers, XML, XPath, and internal communications protocols included in SQL Server Reporting Services (SSRS) and SQL Server Integration Services (SSIS). Our communications framework allows us to create and configure the content of any system generated communication based on business rules, workflow items and events that occur within the system and will support the ability to provide messaging in Multilanguage and multi-literate formats.
	Progressive Technology	Our solution uses a service-based architecture, different application layers, and a set of modern tools to implement a loosely coupled modular application. This approach enables us to leverage system configurability to support on-going program changes, new initiatives and facilitate interoperability and data sharing with partner systems. The use of a rules engine and configurable workflows enables system updates to be made with lower risk and cost. Our SOA-based design enables integration with the ESB while still allowing legacy interfaces to continue until they can be replaced.

	MPATH Standard	MAXIMUS Solution Alignment
Web Interface	Automate Manual Processes	Our solution combines a user-friendly Provider self-service web portal with configurable operational workflows and automated communications all under the umbrella of an integrated web platform. This functionality will increase accessibility for Providers and reduce the amount of paper applications and manual processing required. We will configure business rules to support Montana specific processing rules.
Federal Guideline Compliance	Administrative Simplification	The MAXIMUS solution's main purpose is to reduce the time and effort necessary for providers to enroll, maintain, and access information related to the Medicaid Program. Our approach and solution are directly aligned with the administrative simplification requirements in HIPAA and we have shown how our modular solution eliminates paper, increases processing performance, and reduces the overall effort in Provider Services business processes.
Federal Guideline Compliance	Mechanized Claims Processing and Information Retrieval Systems Final Rule	MAXIMUS fully understands the requirements for enhanced federal funding participation (FFP) for system development and operational efforts for Medicaid systems. We have strived to provide a solution that allows the State to obtain enhanced FFP while at the same time realizing the cost benefits of utilizing a vendor with a technology-driven solution using a set of industry standard COTS products. We believe our overall solution will not only provide the overall lowest cost of ownership, but will also provide a stable long-term platform with which to include additional Provider management capabilities.
Federal Guideline Compliance	Standards and Implementation Specifications for Health Information Technology Final Rule	We designed the MAXIMUS solution to meet data transport requirements included in 45 CFR part 170, subpart B. Our infrastructure platform contains data encryption services that protect data in transit and at rest. We use tools such as SFTP and site-to-site VPN to add a further layer of security as data is being moved between solution components. We developed our solution to be implemented in a modular fashion, providing security at various physical and system levels. We provide secure facilities for our staff and systems with controlled access, we safeguard our networks using a variety of high-technology products and firewalls and protect our systems and data using encryption technology and role-based security. We will work closely with the system integrator to develop secure transport mechanisms as the ESB integration is implemented.

	MPATH Standard	MAXIMUS Solution Alignment
Federal Guideline Compliance	HIPAA and HITECH	We built HIPAA security and privacy considerations into the fabric of the application. We have designed the system to support controlling access to data, role-based security access controls, and other items that safeguard the access of protected information. Our corporate security staff reviews our approach to security and privacy and provide feedback into how our policies can be strengthened. The application has gone through a NIST security assessment and our Amazon Web Services (AWS) cloud hosting approach meets all applicable state and federal requirements. We also adhere closely to the HITECH expansion of the HIPAA Security and Privacy requirements. We have implemented a comprehensive security approach that safeguards mission-critical and confidential data from alteration, loss, theft, destruction, and breach of confidentiality, and meets Federal and State guidelines for security, confidentiality, and auditing, including HIPAA and FISMA. We tailor our security approach for each of our Provider-facing projects based on the type of data that is being collected, stored, transferred, or acted on. Our staff is trained on the requirements and the procedures for reporting incidents are documented and agreed to with each of our clients.

MAXIMUS is mindful of each of the high-level requirements for the MPATH Program; we have aligned our solution and implementation plan directly with the State's envisioned results from the modernization project. MAXIMUS is committed to working with the State and each partner to implement data sharing and interoperability in a manner where enhanced federal funding participation is received and our module is certified according the CMS MECT guidelines.

3.5 Montana Healthcare Programs Overview

3.5 MONTANA HEALTHCARE PROGRAMS OVERVIEW

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

Table 3.5 Montana Healthcare Programs Member Groups

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

	between their countable income and the Medically Needy Income Level each month. The resource limit is $2000 for an individual, and $3000 for a couple or family.
Autism Services	This program provides intensive treatment services for Medicaid members up to age 21 with a diagnosis of autism spectrum disorder or related condition.
Montana Medicaid for Workers with Disabilities (MWD)	MWD allows certain individuals who meet Social Security's disability criteria to receive Medicaid benefits through a cost share. The cost share is based on a sliding scale according to an individual's income. MWD resource and income standards are significantly higher than many other Medicaid programs: $15,000 for an individual and $30,000 for a couple; while the countable income limit is 250% of the FPL.
Additional healthcare services	
Medicaid Expansion	On January 1, 2016, Montana expanded healthcare coverage to thousands of state residents through the Montana Health and Economic Livelihood Partnership (HELP) Act. Individuals who receive healthcare coverage through the HELP Act are either eligible for Standard Medicaid benefits or HELP Plan benefits. Help Plan benefits are administered through Blue Cross Blue Shield (BCBS) of Montana, a third-party administrator (TPA). Section 9 of the HELP Act includes provisions to provide health care services for individuals who are in the custody of the Department of Corrections or who are residents by commitment or otherwise residents of the following facilities. • Montana State Hospital • Montana Mental Health Nursing Care Center • Montana Chemical Dependency Center • Montana Developmental Center
Mental Health Services Plan (MHSP)	This program provides state funded benefits for individuals who have severe and disabling mental illness and meet income limits establish by the state but do not qualify for Standard Medicaid.
Emergency Alien Medical Coverage	This program provides limited benefits for emergency services such as labor and delivery. Other emergency services may be covered from the time treatment is first given for a condition until that same condition is no longer considered an emergency. These services must be determined an emergency by Medicaid department staff.
Medicare Savings Program (MSP)	MSP benefits may be provided to individuals who are low income Medicare beneficiaries. • Qualified Medicare Beneficiary (QMB) –Medicare premiums, co-payments and deductibles are covered for individuals who have QMB eligibility. • Specified Low-Income Medicare Beneficiary (SLMB) – Medicare premiums are covered for individuals who have SLMB eligibility. • Qualified Individuals (QI) – Part B premium payments are covered for individuals who have QI eligibility.
Montana Waiver Programs	Montana has a number of waiver programs that provide services to supplement existing Standard Medicaid benefits that include the following waivers: • Section 1115 waivers – 1115 Plan First – 1115 Health and Economic Livelihood Partnership (HELP) Demonstration – 1115 Basic Waiver for Additional Services and Populations • Section 1915 (b) waivers – 1915(b) Health and Economic Livelihood Partnership (HELP) – 1915(b) Passport to Health – 1915(b)(4) Montana Big Sky Waiver Case Management – 1915(b)(4) Montana Autism Evaluation Services • Section 1915 (c) waivers – 0208 HCBS Comprehensive Services Waiver for Individuals with Developmental Disabilities – 1915(c) Montana Big Sky – 1915(c) HCBS Severe Disabling Mental Illness (SDMI)

X MAXIMUS has read, understands, and will comply will each requirement in this section.

For 42 years, MAXIMUS has assisted state, federal, and local governments to provide critical health and human service programs and health information system technology to a diverse array of communities. We leverage our extensive experience and strong commitment to ethics to provide high quality services and solutions. With a passion for public service, our 18,000 employees are dedicated to providing innovative programs that improve the quality of life around the globe. Our health and human services solutions are designed to make a meaningful impact on people's lives and strengthen communities through state, federal, and local government partnerships. We collaborate with government agencies to develop cost-effective health and human service programs tailored to their communities' unique needs. At the same time, we offer governments the ability to implement programs rapidly with scalable operations and automated systems.

Through our experience and especially through our deep understanding of the Medicaid program itself, MAXIMUS is well prepared to deliver a Provider Services solution that meets the unique needs of States. Our solution is specifically designed to cater to the needs of the Provider community, allowing providers to enroll and maintain their data in a timely and accurate fashion, so that they are able to efficiently serve the needy population of the State. Our proposed staff for the project have reviewed the list of programs supported under the Montana Healthcare Programs and fully appreciate the diverse types of Providers that are required to support the critical services offered by Medicaid as well as appreciate the population and people that the programs support. As we mention throughout our proposal, we provide the State with a configurable solution specifically designed to support the State’s provider community and all stakeholders involved in the business processes that involve the provider community. Our configurable solution allows us to adapt to the specific business rules for each individual state and in each of our three past modular implementations we have been able to support multiple programs types and the specific differences in business rules between states.

In reviewing the list of programs supported under Montana Healthcare, we are able to readily see the different types of data, workflow, and users that may need to be involved in the enrollment of each respective provider type. We understand that on the surface, Medicaid Programs are similar in the types of programs but between states can have very different requirements for provider enrollment. For example, MAXIMUS has implemented our Provider Services module in three (3) different states and the business processes and business rules for the processing of waiver providers has been entirely different in each of these states. That being said, our solution has been able to accommodate the unique needs of each state when processing waiver enrollments, re-enrollments and data updates. *Exhibit 3.5-1: Waiver Provider Enrollment* illustrates the list of menu options a newly enrolling provider will see once they have established an account through the Provider Services web portal. This list will be tailored to the individual needs of the state and the unique enrollment requirements defined within each Medicaid Program. Our solution is designed to support any number of programs and the specific provider types that are allowed to deliver services to the specific populations under each program.

CONFIDENTIAL

The enrollment options shown in *Exhibit 3.5-1* illustrate the current configuration of our solution for the District of Columbia. In the District's implementation, a provider is required to select from each application type based on program and is required to be assigned a unique Medicaid ID for each application type submitted. In other state implementations, we allow the provider to enroll by selecting multiple program types during the enrollment process. Under this configuration, we allow (for example) a Dentist to be enrolled as fee-for-service (Standard Application), ordering/referring (Streamlined Application), and as a waiver provider (HCBS-Waiver) all under the same Medicaid ID. MAXIMUS will work with the Department during the DDI phase to understand the unique needs of Montana for configuring the provider workflows, data requirements, and enrollment process for each program. Our knowledgeable staff will support this process by offering lessons learned from other states and best practice processes we have developed from our experience in multiple states.

MAXIMUS highlights our expertise in the configuration and enrollment of waiver providers because in our experience, the business processes and workflow configurations for these types of providers typically require more time during the DDI phase as compared to other provider types. In addition, we have found that waiver providers are the most heavily affected by the ACA enrollment and screening requirements so we try to minimize the impact through an easy and intuitive enrollment and data update process. We have found that for waiver providers, other stakeholders are usually involved that can be outside the jurisdiction of the State's Medicaid agency. The types of supporting documentation and attachments that need to be submitted by waiver providers are also typically more complex than those of other provider types. For the Montana implementation, we will bring our expert staff and configurable solution to facilitate an implementation that meets any and all of the unique waiver enrollment requirements for

Montana waiver providers. We will also support all program and provider types included in the Medicaid Program.

3.5.1 Montana Healthcare Programs Benefits

3.5.1 Montana Healthcare Programs Benefits

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

Table 3.5.1 Example of Standard Medicaid Covered Services

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

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

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

MAXIMUS understands that the populations served by Medicaid often require a wide variety of services and support. In reviewing the list of services offered by Montana, we notice that in addition to meeting the federal guidelines for mandatory benefits, Montana has also chosen to cover other optional services. We have reviewed the list of services covered in RFP Table 3.5.1 and understand the different types of payment methodologies currently used by the State for the payment of Medicaid claims. We have also researched and are aware of the additional information contained in the 2017 DPHHS report to the Legislature. Based on our review of the current offered services, MAXIMUS is confident that we can bring a solution to the State that will capture and maintain all of the Provider data necessary to allow the State's MMIS to support the various types of payment methodologies currently in place, as well as for any methodologies that the State may opt to implement in the future.

Flexibility

CONFIDENTIAL

The MAXIMUS Provider Services solution captures various types of Provider characteristics for each Provider that enrolls through the system. This data includes Application Type(s), Provider Type, Entity Type (Individual, Organization, or Facility), Specialty(s), Taxonomy(s), Services (for waiver providers, if separate from specialties) and Category of Service (by Provider Type). We can also relate providers to the programs they support if necessary. The data requested and captured for each Provider is configurable and controlled through a combination of the system's flexible Workflow engine working in concert with the system's Business Rules engine. In this sub-section of our proposal, we provide some examples of the types of data the Provider Services module captures for Providers as it relates to the types of services a provider may be eligible to provide for eligible Montana Medicaid members and recipients. During DDI, we will work closely with the State to configure provider data requirements to meet the specific Program needs. In each of our three modular implementations, we have been able to accommodate all program and provider requirements specific to each state.

Category of Service

Our solution contains reference data for each Provider type that allows the system to automatically identify the Category of Service(s) that a provider is authorized to bill for based on the Provider type. *Exhibit 3.5.1-1: Category of Service* shows the Categories of Service that are assigned to an EPD Waiver provider that has completed their re-enrollment using the Provider Services module.

In the screenshot shown in *Exhibit 3.5.1-1*, you can see that the system has automatically assigned two Category of Services for the provider type (EPD Waiver). The system tracks the begin date and the end dates of each Category of Service authorized for the provider, and maintains a history of all Category of Services. Internal users (Enrollment Specialists) have the ability to end date Category of Services for the provider or add additional Category of Services for the provider during the application/re-enrollment review process. Once the Provider is approved in the system, the Category of Service data are sent to the MMIS as part of the MMIS interface and stored in the MMIS as needed to support claims processing for the Provider. MAXIMUS will leverage this design for the State if the State uses the concept of Category

CONFIDENTIAL

CONFIDENTIAL

of Service as part of their provider enrollment process to support the various types of payment methodologies in use by the State.

Waiver Services

In addition to Category of Service, our solution also allows waiver providers to identify the types of services that can be performed as part of their enrollment process. We discussed our experience in handling waiver provider enrollment in the introduction of *Section 3.5–Montana Healthcare Program Overview*. Authorization of such services varies from State to State. Currently, in our District of Columbia implementation, providers are 'pre-authorized' by District users (DDS Enrollment specialists) to perform a selected number of services under the waiver program. When the provider establishes an account and begins their enrollment process through the self-service web portal, the Provider is able to view from a pre-defined list of services and indicate their ability for providing such services. *Exhibit 3.5.1-2: Waiver Services*, provides an example of what a user might see when enrolling as an IDD waiver provider through the system. The screenshot shown is a snippet of the overall waiver services screen that the provider can see.

In the screenshot shown in *Exhibit 3.5.1-2*, the Provider is able to view the services that have been pre-approved by the waiver services specialist. The Provider is then able to select those that they intend to support and for each, provider additional supporting information as to their ability to support the service. All of this data is configurable based on each State's needs. For example, we can configure this process to allow the Provider to select any service and put the responsibility for approving each service on the Waiver services specialist.

Different states store their waiver services data in different ways on the MMIS. For example, in our Tennessee and Nebraska implementations, 'Services' are stored as a separate characteristic for the Provider (they are not Specialties, they are Services). In the District of Columbia, the Services are actually stored as additional Specialties for the Provider, as this is the manner in which the MMIS will

CONFIDENTIAL

CONFIDENTIAL

accept that data for purposes of Claims processing. Our solution is capable of supporting either method, and the enrollment and review workflows are configurable to accommodate whatever the unique business process may be for the State of Montana. This example illustrates some of the major differences we anticipate between states and the flexibility of our solution to handle two completely different configurations for the same types of services. Our experience in setting up provider requirements for different states will enable us to help each state determine the best approach to meet their Program requirements.

Streamlined Applications

Although the State has provided a comprehensive list of Healthcare Programs in the RFP, MAXIMUS understands that, based on the response to the RFP questions the enrollment requirements for Providers to enroll with Montana Healthcare Programs are similar for all providers aside from certain certifications, endorsements, and licenses required for some provider types. Ordering, referring, attending and prescribing providers are allowed to complete an abbreviated enrollment that excludes tax, banking, and ownership information from their enrollments. This approach aligns precisely with how we have our solution currently configured for our District of Columbia implementation.

Our solution allows Providers to submit ‘streamlined’ applications; which are configurable based on Department defined rules. Examples of streamlined applications include Providers submitting applications for purposes of receiving payment for emergency out-of-state claims or Providers submitting applications to be registered as ordering/referring only. *Exhibit 3.5.1-3: Application Types* provides an example of how our solution is configured to allow Providers to submit various types of applications.

Streamlined applications are typically abbreviated enrollments that do not require the Provider to submit a full enrollment profile as compared to what is required for a fee-for-service Provider (for example, we configure the system to not request W9 information for Streamlined applications). Our solution also allows types of applications to be flagged as expedited, meaning that these applications rise to the top of the worker queue once they have been submitted by the Provider. When the system determines that an application was submitted as ‘expedited’, the system invokes a business rule that places these applications

CONFIDENTIAL

in a priority status at the head of the work queue for expedited processing. When an Enrollment Specialist retrieves a Provider from the work queue, the expedited applications will be retrieved first.

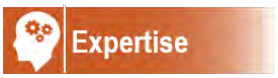
In reviewing all the services offered by Montana and the provider types that support each, MAXIMUS is confident our solution can be configured to support all of the requirements. As part of our implementation approach, we plan to gain a detailed knowledge of each program and help the State determine the best approach for each enrollment workflow.

3.6 Montana Healthcare Programs Enterprise

> 3.6 MONTANA HEALTHCARE PROGRAMS ENTERPRISE
>
> The Montana Healthcare Programs enterprise is comprised of multiple components and services that support activities related to provider enrollment and maintenance, population health management, care management, benefit management, claims adjudication, payments, reporting and other business processes necessary to administer Montana Healthcare Programs.

X MAXIMUS has read, understands, and will comply will each requirement in this section.

MAXIMUS understands that the Montana Healthcare Programs enterprise consists of a complex array of components and services all of which must seamlessly work together to support all of the business processes associated with the State's Medicaid enterprise. We believe that the solution we bring to Montana offers the best approach to meeting the State's requirements for a modular Provider Services solution. Our strength is based on our pinpointed focus on health and human services solutions. Since the passing of the Patient Protection and Affordable Care Act (ACA) in 2010, MAXIMUS has been involved in the implementation of this monumental policy. Since that time, we have focused on helping our clients achieve compliance with the Provider enrollment and screening requirements included in the ACA. In addition, with CMS pushing modularity as a key building block for new Medicaid support systems, our three modular Provider management implementation projects are unsurpassed in the Medicaid market. Our clients in Tennessee, Iowa, Massachusetts, Nebraska, and the District of Columbia are some of the first agencies to achieve compliance with these new requirements and this experience provides a strong basis for our Montana Provider Services implementation.



Our broad experience in supporting State Medicaid agency clients gives us a unique perspective for implementing our Provider Services module for the State. We not only will bring our production-proven, configurable Provider Services solution to the State, but also we will bring deep expertise and understanding in supporting the various ancillary activities related to all facets of the Medicaid enterprise. Our primary focus, of course, is on implementing a high quality, CMS compliant Provider Services solution for the State. However, we also have a firm understanding of the different types of interactions (both automated and manual) that must also be in place to support not only the provider business function, but other Medicaid/healthcare related components of the Medicaid enterprise.

In the sub-sections that follow, we highlight our understanding and approach for implementing our Provider Services solution for Montana, sensitive to the various components of the Montana Healthcare enterprise that will need to be factored in to the solution to meet the unique needs of the State.

3.6.1 Current MMIS Environment

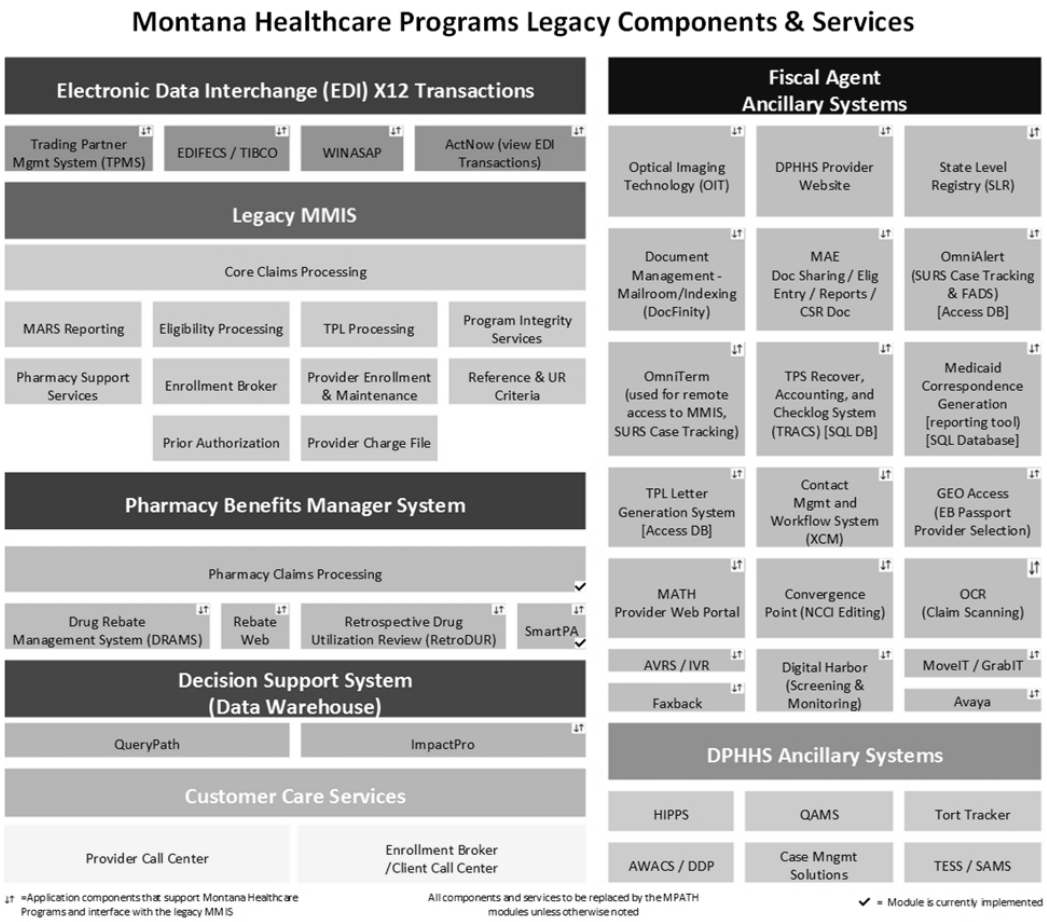
3.6.1 Current MMIS Environment

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

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

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

Figure 3.6.1 Montana Healthcare Programs Legacy Components and Services



MAXIMUS understands that aging, legacy systems significantly limit the State's ability to make software updates that would lead to more optimized, modern business processes. The State of Tennessee recognized this with their legacy MMIS several years ago and partnered with MAXIMUS implement a modular Provider Services component to begin an incremental modernization of their MMIS enterprise. MAXIMUS is the first company to develop and implement an independent Provider management solution outside of the traditional MMIS. We accomplished this project in partnership with the State of Tennessee

as they moved away from a traditional MMIS model to a model that more fully supported their managed care Medicaid Program.

As modularity ideas have advanced, MAXIMUS has developed a model to transition fiscal agent operations into standalone business services components governed by service level agreements and technology requirements. This approach benefits our clients by allowing the incremental modernization of systems and services to improve the quality of services delivered. It also enables clients to control how and when new services and supporting technology are delivered. The Provider community specifically benefits from having a customer-centric, intuitive, web-based solution that eliminates mounds of paper and encompasses a variety of communication methods that support the modern technology currently used by the larger Medicaid Provider population. Acquiring and retaining qualified providers is pivotal in supporting the mandates of the Medicaid Program. Our solutions eases the enrollment, revalidation and data update processes to make it easier for providers to enroll and maintain eligibility while minimizing the impacts for new enrollment and screening requirements.

MAXIMUS has reviewed the available information on the State's current environment as it relates to the business processes and systems currently in place to support the Montana Healthcare Programs enterprise. We understand that the State has a blend of newer/modern applications as well as aging legacy applications. We also understand that the new Provider Services module must not only replace and augment current MMIS functionality as it relates to the Provider enrollment function but also must provide seamless integration to other State systems (both modern and legacy). Our approach for integration with other State systems will involve the use of our solution's Open Interface Framework, Business Process (Workflow) Engine, and our Business Rules engine. We have closely examined all of the technical and functional requirements contained in Appendix F of the RFP and are confident in our ability to deliver all of the functionality (present and future) to the State. We will leverage existing, out-of-the-box functionality from our Provider Services implementations in other States and augment our existing capabilities where required to deliver all components required for MPATH.

MAXIMUS experience in supporting modular integration is unsurpassed in Medicaid. We are currently integrated with a variety of legacy MMIS and Medicaid Support systems. In Tennessee, our Provider Services module is implemented as a standalone system outside of the traditional MMIS provided by DXC (formally HP). Our solution is the system of record for provider data and we integrate with the legacy MMIS using web services. We also integrate with the state's EDIFECS subsystem using an enterprise services bus (ESB) to enable many of the self-service components the State has included in Option A. To support individual enrollments we have created a two-way an XML file transfer interface with CAQH, the state's CVO. In Nebraska, our Provider Services module integrates with two state supported legacy systems both based on COBOL, CICS and DB2. One houses the traditional MMIS providers and the other includes the waiver program providers. These are accomplished through two-way SFTP file transfer interfaces. In the District of Columbia, we interface with the Conduent legacy MMIS using a two-way SFTP flat file interface structure based on the legacy MMIS requirements.

After a review of the existing environment in Montana and the plans for new modular components, we are confident our solution contains the functions and configurability necessary to seamlessly integrated with partner systems now and in the future.

3.6.2 Legacy Components and Services

3.6.2 Legacy Components and Services

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

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

Component	Users
Legacy MMIS	425
Pharmacy Claims Processing and Management	120
Legacy DSS	225
DPHHS Ancillary Legacy Systems	1855
Fiscal Agent Ancillary Legacy Systems	550

MAXIMUS has reviewed the end-user statistics for the legacy systems currently in place in Montana. We understand our primary focus will be to implement the Provider Services module for Montana, which will generate a new set of statistics for end-users once the new module is implemented. Our solution is successfully implemented in three States, some of which are comparable in size to Montana (. We are confident in our ability to support any number of users through the Provider Services module, including the user community that may be required for other State implementations under the NASPO agreement. Our use of cloud-based hosting coupled with the architecture of our solution enables MAXIMUS to increase the size of the various environments, add additional servers to each tier and to scale the telecommunications as needed by the size of each State using our solution.

As the Data Integration module is implemented, the MAXIMUS Provider Services solution will interface with other MPATH modules to enable seamless interoperability with the MPATH Integration Platform to obtain Provider verification information and deliver updated, consolidated information regarding a Provider's enrollment in the Medicaid Program. Our solution enables the synchronization of Provider data across internal and external data processes to maintain data relationships and integrity. Our solution currently provides a variety of data exchange mechanisms including but not limited to:

- **Secure Web Service Calls** –Demonstrable capabilities to connect with systems like java, .NET, and native C++ SOAP client that are able to consume interoperable web services in a secure manner.
- **ESB Integration** – extensive data and process sharing using a variety of web service message integrations including XML and JSON supporting a variety of web services types including WSDL, WS-*, SOAP, REST, UDDI, and ODATA.
- **Trigger Tables** – When within a shared domain, MAXIMUS Provider Services solution can access or provide trigger tables with the request and response information to allow automated data transfers with older systems that do not use web services.
- **Secure File Transfer Protocol (FTP) and Batch Interfaces** – To cater to legacy mainframe systems and many other partner systems, MAXIMUS Provider Services solution contains a secure FTP site

coupled with a set of configurable batch interfaces that can automatically process inbound and outbound files using agreed upon file formats.

We understand that the interface with the MMIS is the most critical interface to be implemented as part of a Provider Services modular implementation. We have successfully implemented this interface using various mechanisms, including flat file transfer via SFTP on the legacy MMIS system. Under the MPATH incremental modernization approach, when the MMIS transitions to the modern system, and the ESB is implemented as part of the Systems Integration module, the MAXIMUS Provider Services MMIS Interface can quickly transition to the new data exchange format (web services). The MMIS Interface file definition is packaged with defined transactions using standard Provider data to exchange data with any State's MMIS. The MMIS Interface file definition includes transactions that allow for add new Provider, update Provider, terminate Provider, terminate with sanction reasons, add affiliate, and update affiliate. These transaction definitions are configurable and can be extended based on the need of the State. We are planning to work closely with the System Integrator to create specifications and ESB-based data integration transactions for all provider data requirements.

As the MPATH project evolves, the MAXIMUS Provider Services solution will continue to support all required file transfer protocols. However, we will continue to focus on supporting and implementing advanced interoperability functions and will augment other application interfaces using a standard catalog of web services via ESB.

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

> 3.6.2.1 Electronic Data Interchange (EDI) X12 Transaction Components/Services
>
> Trading Partner Management System
>
> The Trading Partner Management System (TPMS) is the system that is used to create and manage the types of EDI transactions that trading partners have enrolled to submit and receive.
>
> EDIFECS/TIBCO
>
> EDIFECS/TIBCO is the software used to verify the information contained in EDI transactions meet the necessary requirements.
>
> WINASAP
>
> WINASAP5010 is free billing software offered to providers enrolled with Montana Healthcare Programs to create, and submit X12 compliant EDI claims transactions.
>
> ActNow
>
> ActNow is software used by the customer care center to view and research EDI transactions.

MAXIMUS has reviewed and understands the infrastructure that is currently in place to support Electronic Data Interchange (EDI) X12 transaction processing. CAQH.org has introduced CORE requirements to promote interaction of healthcare trading partners and the exchange of healthcare-related information in a consistent, clear, and standardized manner and in compliance with applicable laws and regulations. CMS has adopted a variety of CORE operating rules to control how HIPAA transactions are used by entities covered by HIPAA. These new rules put in place requirements for accessibility, performance and structure and expand on the base X12 transaction and code set rules. Compliance with these requirements will be important as the self-service functions included in Option A are implemented.

MAXIMUS has a solid understanding of the CORE Operating Rules as offered by CAQH and mandated by the Affordable Care Act (ACA). MAXIMUS has implemented some of the high profile CORE related requirements into our Provider Services web portal, including:

- ACH/EFT functionality
- Ability for Providers to retrieve and view electronic remittance advice (eRAs)
- Enabling the remaining HIPAA transactions to be executed directly from the web portal

For example, the State of Tennessee is focused on making the provider web portal the single interaction point for all provider data. To make this possible, MAXIMUS is currently working on a major enhancement to include all the functions enabled through HIPAA transactions to be accessible directly from the provider web portal. We are completing this effort in an incremental fashion with eligibility verification (270/271) and claims status (276/277) first and claims entry next (837s). We have already implemented the 835 and online remittance advice functionality. We expect to have all of the functionality in production no later than September 2018 per the existing project schedule.

Being able to readily implement CORE requirements into our system demonstrates the flexibility and versatility of the modern, service oriented architecture of MAXIMUS Provider Services solution. To implement the ACH/EFT functionality for Tennessee, MAXIMUS worked with members of their Finance and Accounting department to make sure the EFT CORE requirements were properly addressed in the Provider Services web portal. This consisted of a thorough review of the CORE-required Maximum EFT Enrollment Data Set to make sure that the system captured all the required data elements for EFT. The system's flexibility to capture the required EFT data elements was only part of the implementation. MAXIMUS also implemented other functionality to fully incorporate the EFT requirements to meet the State's business model. This functionality included automated workflows for Accounting and Finance and updates to the MMIS interface to send vendor numbers across for enrolled providers.

In addition to the ACH/EFT CORE functionality, MAXIMUS has been tasked with moving functionality traditionally supported though EDI transactions to the provider portal. In the first increment of this work, we have implemented eRA functionality into the web portal. This allows authorized Providers to search for and view remittance advice on the web portal. This functionality also allows internal Medicaid users to search and view eRAs. To implement this functionality we again leveraged the flexible architecture our Provider Services solution to implement a data sharing interface with the State EDIFECS platform utilization the State's ESB. MAXIMUS developed an architecture consisting of web services messages to adhere to the CAQH-CORE guidelines. Our solution was built on existing standards and makes the electronic transactions more predictable and consistent, regardless of the technology.

MAXIMUS has implemented functionality on the self-service web portal to allow Providers and Trading Partners to submit a unique submitter number for each billing service that transmits HIPAA X12 transactions with the State for single or multiple providers. In Tennessee, we have also implemented the functionality to allow entities enrolling as trading partners with the State's healthcare programs to select the HIPAA X12 transactions they choose to submit and receive. We will bring these components to Montana as part of our Provider Services implementation and configure them, as needed, to meet any unique needs of Montana. Our solution uses data integration with the EDIFECS platform to support X12 transaction processing both in and out of the system. For our Montana implementation, we will work with the various module partners to implement the ability to create/edit, send, receive and process X12, NIEM standardized transactions and NCPDP D.0 transactions. We envision the web portal acting as the initiation point for requests and responses. As the new modules are implemented we will validate the

overall process and limit our transactions to our scope of work as described in the RFP questions and answers.

By continuing to expand our Provider Service's module SOA capabilities, we can help Montana respond more quickly and cost-effectively to changing business needs. By leveraging the SOA architecture and expanding the web service interface with EDIFECS, we are constructing well defined services that can be reused by both internal and external components. For providers to access 271 transactions, they can either login into the Provider Services web portal or consume a service exposed by the State. To identify and authorize the provider, we are in the process of building an authentication service which will support the various access methods. The resulting architecture, and our adherence to the CAQH-CORE guidelines, cause various parts of the system to behave the same way by using SOA irrespective of who is hosting them.

3.6.2.2 Pharmacy Benefits Management System Components/Services

> 3.6.2.2 Pharmacy Benefits Management System Components/Services
>
> FlexibleRx: FlexibleRx, the Pharmacy Claims Processing and Management module is an on-line, real time pharmacy claims adjudication system. Today, FlexibleRx receives member eligibility and provider information from the legacy MMIS. Adjudicated claims are sent to the MMIS for payment generation to providers. FlexibleRx was implemented December 2015 as the first legacy replacement module within the Montana Healthcare Programs enterprise and was certified by the Centers for Medicare and Medicaid Services (CMS) on February 15, 2017.
>
> Drug Rebate Analysis and Management System (DRAMS): The Drug Rebate Analysis and Management System (DRAMS) is an application which calculates and maintains records of rebate amounts paid for pharmacy claims to provide the necessary data for CMS for reporting on drug rebates.
>
> Rebate Web: Rebate Web is a web based application where drug rebate invoices and associated claim level detail are uploaded for manufacturer drug rebate management.
>
> Retrospective Drug Utilization Review: Retrospective Drug Utilization Review (RetroDUR) uses a member's drug utilization history to create a usage profile which is then used to help prevent instances of drug abuse, misuse, or fraud. This service is currently contracted to Mountain Pacific Quality Health.
>
> Smart PA: SmartPA is a web based service that interfaces with the pharmacy claims processing system (FlexibleRx) and provides prior authorization validation services during adjudication for pharmacy claims.

MAXIMUS has reviewed and understands the components that comprise the State's Pharmacy Benefits Management System. We also understand that it will be part of the scope of the Provider Service's module to make available the system functionality to enroll and screen all of the providers that deliver services to Montana Healthcare members, which includes pharmacies. The MAXIMUS Provider Services solution provides the functionality to enroll and screen pharmacy providers. We have implemented this in different ways depending on State requirements. Our solution is configurable to allow us to meet any of the unique requirements for Montana.

In our solution, pharmacies are placed into their own enrollment category (referred to simply as Pharmacy). *Exhibit 3.6.2.2-1: Dashboard* shows the active system dashboard from our District of Columbia implementation.

CONFIDENTIAL

As shown in *Exhibit 3.6.2.2-1*, our solution shows the status of all pharmacy providers in the system including the number of active providers and those that may be in an active workflow within the system. This gives DPHHS and other stakeholders a real-time view of the current providers in the system.

Our Provider Services module utilizes our existing enrollment and screening components for Pharmacies. During DDI, we will identify the specific enrollment and data update requirements for these providers and configure them to meet any unique requirements for MPATH. Pharmacy providers will be able to enroll, revalidate, and update their enrollment profiles through the system's web portal. Any unique data (and supporting documentation/attachments) required for pharmacies will be captured in the system, and sent to the MMIS as required. *Exhibit 3.6.2.2-2: Pharmacy Providers* gives an example of some of the unique data we capture for pharmacies in our District of Columbia implementation. Since pharmacies are treated the same as other provider types, we utilize the base functions in our system to support this provider population.

CONFIDENTIAL

CONFIDENTIAL

Our solution will assign the appropriate Risk Level to pharmacy providers and also facilitate the required screening for the pharmacy based on the Risk Level. Once the pharmacy enrollment is completed, we will send the provider data to the MMIS through the MMIS interface. This will allow the State's FlexibleRx PBM to utilize the correct provider information from the legacy MMIS as it currently works. Once the Data Integration module is implemented, the FlexibleRx system will have the ability to receive pharmacy provider data directly using web services messages through the ESB. Adjudicated claims will continue to be sent from FlexibleRx to the MMIS for payment generation to providers.

Efficiency

MAXIMUS strives to streamline the enrollment process for all Provider types. We listen to our clients and take steps to optimize the process and reduce data entry burdens on Providers and internal staff, when possible. Our experience allows us to offer and share best in class services across our customer base. As an example, MAXIMUS implemented a streamlined enrollment process for large pharmacy providers. Large pharmacy providers (also referred to as 'Chain Pharmacies') typically have multiple locations with unique NPIs. To decrease the administrative burden of manually enrolling several locations online that potentially have duplicate information, we created and implemented a file submission enrollment process for pharmacy providers. Using this process, large pharmacy providers are able to submit their enrollments (and updates) by providing a file that contains the minimum required data elements for a single service location with a unique NPI. As a part of this implementation, MAXIMUS provided documentation to the providers, accessible via the web portal, to direct them to the new process. The documentation provides the steps the provider needs to take to complete their enrollment using this streamlined method. The file submission method is optional. All pharmacies continue to have the ability to enroll and update their provider records through the online portal. MAXIMUS may bring forth solutions from our other projects to determine if the state might benefit from the use of these components.

CONFIDENTIAL

3.6.2.3 Decision Support System Components/Services

3.6.2.3 Decision Support System Components/Services

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

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

MAXIMUS has reviewed and understands the system components that are currently in place for the Decision Support systems in Montana. Based on our understanding of the initial scope of the project as it relates to integration with the State DSS, our Provider Service solution is capable of providing an extract of Agency defined data to the Agency's data warehouse, at a minimum on a weekly basis. We provide this extract as part of the scope of our Option B Provider Services, as specified in the RFP. In each of our current implementations, we provide these types of data extracts in various formats and to various internal and external entities, including external data warehouses.

MAXIMUS leverages existing extracts and file definitions from our previous implementations and tailors them to meet the unique requirements for Montana. In Nebraska, we interact with a data warehouse that is supported by an external vendor. In that implementation we have agreed to the fields that will be included and transfer the file on a predefined schedule using our SFTP site. In Montana, we will work with the State to determine how to transmit the data if the System Integration module is not in operation. Once that is in place, we will use ESB integrations to move the data to the Enterprise Data Warehouse.

The provider enrollment process in our solution enforces edits and requires a clean application to be submitted by the provider prior to initiating the screening steps in both the new enrollment and re-enrollment workflows. Using our configurable workflow engine in concert with our rules engine, the system captures accurate and complete information for each provider. Our data model, specifically designed for Provider management, results in an accurate and de-duplicated list of active providers within the system. As a result, the data extracts we produce as it relates to Provider data are accurate and represent the complete and accurate enrollment profile (and history) for each provider maintained in the system.

An example of one of the file extracts we produce on a weekly basis is our MCO Extract file (Provider Directory) that we generate each week and place on an SFTP server for our customer in Tennessee. MCOs are able to retrieve the files from the SFTP site and consume the files in whatever method they choose. The set of files produced for the MCOs could easily be imported into the State's data warehouse. We would customize the file layout to meet any unique needs for the State's data warehouse.

MAXIMUS produced a user guide for the MCOs for their retrieval and use of the files. This guide is published on the SFTP site and is also published in the Learning section of the Provider Services web portal. *Exhibit 3.6.2.3-1: Provider Directory User Guide* provides a snippet of some of the documentation that is included in the guide.

MAXIMUS

3. YYYYMMDD-TennCare-MCOProvider.txt

This file contains all of the active providers in PDMS; once the provider record is terminated it will remain on the file for 30 days after the date the provider was terminated. A provider can be an individual or a non-individual (a group, entity, facility, or a non-medical service provider). If the "Base Medicaid Id" is blank for a provider, check the MCOLocation file, use the PartyID or NPI as the key and a location should exist with a "Medicaid Id".

Standard date format: YYYY-MM-DD

Note: ***Medicaid IDs for individual and non-individual locations are in the MCOLocation file; Base Medicaid IDs displayed in this file are only for individual providers with previous or current group affiliations.***

3.1. File Layout

Column Name	Data type	Max Length	Description
PartyID	int	10	Provider PDMS ID – system assigned ID
Name	varchar	255	Provider Name (First and Last Name or Organization Name)
NPI	varchar	10	National Provider Identifier
DBA	varchar	100	Provider DBA Name
Gender	char	1	Provider Gender
BirthDate	date	10	Provider Birth Date
ProviderTypeID	int	10	Provider Type – system assigned ID
ProviderTypeAbbreviation	varchar	4	Provider Type Abbreviation
ProviderTypeName	varchar	255	Provider Type Name
ProviderCategoryTypeID	int	10	Provider Category – system assigned ID
ProviderCategoryTypeName	varchar	80	Provider Category Name
CAQHID	varchar	80	CAQH assigned ID
BaseMedicaidID	varchar	80	*Medicaid ID assigned to individual providers with group affiliations
TaxID	char	9	Provider's Tax ID (populated for non-individual providers)
SSN	char	9	Individual SSN (populated for individual providers)
CredentialAddress1	varchar	100	Credentialing Address Line 1
CredentialAddress2	varchar	100	Credentialing Address Line 2
CredentialCity	varchar	50	Credentialing Address City
CredentialCounty	varchar	50	Credentialing Address County

Exhibit 3.6.2.3-1: Provider Directory User Guide (MCO File Extract). *In our Tennessee Provider Services implementation, we produce a weekly extract file that is posted to the State's SFTP server. We produce full documentation and user guides for all of file extracts.*

The files submitted as part of the MCO Extract file give the receive agency the ability to import the complete enrollment profile for each provider in the system, including ownership data and group/member affiliations. We will leverage this process and file definition for Montana to produce the required extracts for the State's data warehouse.

3.6.2.4 Customer Care Services

3.6.2.4 Customer Care Services

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

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

Call Center

MAXIMUS understands that the Provider Call Center services are currently contracted by DPHHS through the Fiscal Agent contract. MAXIMUS is prepared to deliver these same services as an integrated component of our Provider Services module if Montana decides to include Option B services under this procurement. We feel strongly that we are uniquely qualified to provide such services. With a proven integrated system and service solution that meets ACA and the CMS requirements and experience in operating similar provider screening and enrollment projects in five other jurisdictions, MAXIMUS has unparalleled credentials to deliver Provider services in Montana, including Call Center support to assist providers with inquires related to Provider enrollment and screening.

Through our strong national presence and Provider operations in multiple jurisdictions, we currently manage Provider data and enrollment services for more than 200,000 Medicaid providers. We will leverage this expertise, relying on best practices and lessons learned to deliver high quality end-to-end customized Call Center, Provider enrollment, and screening services that strive not just to meet, but exceed performance expectations.

Enrollment Broker/Member Call Center

MAXIMUS understands the current infrastructure for Montana as it relates to the enrollment broker/member call center business function. We understand that provider data is critical to enable these functions and we will provide accurate and timely data as needed by these modules. With 19 Medicaid managed care enrollment broker projects, we understand that Provider management is not isolated from other services based around Medicaid, but is highly integrated with the larger Medicaid and health care environments. MAXIMUS leverages best practices and lessons learned from our Medicaid Provider experience and from our wide array of health services projects (including Enrollment Broker, Health Insurance Exchange, and eligibility support).

MAXIMUS is currently working with multiple states, forming new ideas for how Provider data should be structured and made available outside of the traditional MMIS to avoid built-in constraints that impact data sharing and advanced business processes. Our solution designed to be sensitive to the needs of provider management as it relates to the enrollment broker function in each State. We support sharing provider data across all Medicaid partner systems so that members understand where they can receive the services they need without having to look through multiple data sources with varying degrees of accuracy.

3.6.2.5 Fiscal Agent Ancillary Systems

3.6.2.5 Fiscal Agent Ancillary Systems

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MAXIMUS has been providing member and provider services to Medicaid agencies for 19 years. Our support model has always required the implementation of services and systems that work alongside the MMIS so we are intimately familiar with how these systems work and the data integrations that are required. We have reviewed the available documentation from the RFP relating to the State Fiscal Agent's existing ancillary systems. Obviously, the primary existing system that will be immediately impacted by implementing the new Provider Services module will be the provider management functions contained in the legacy MMIS. However, based on our experience, we also understand that there could be challenges (and potentially new integration points) between the Provider module and the Fiscal Agent's ancillary systems. We appreciate the State providing this information in the RFP to help give us an

understanding of where we must be aware of differences as we compare the MPATH requirements for the Provider Services module to existing Fiscal Agent systems.

Modularity

We believe it is important to reference our experience as it directly relates to our ability as the State's vendor to not only be aware of the potential impacts to existing systems but also to have processes and software in place to deal with them. All of our implementations have specifically been Medicaid Provider Service ***modular*** implementations, not monolithic MMIS replacements. Through the course of implementing these systems, we understand the importance of factoring all systems under the State Medicaid enterprise umbrella and that all systems must work in concert to maintain existing service levels as well as to provide for the incremental modernization of the enterprise as a whole.

In this sub-section of our proposal, we have provided a brief summary for each of the Fiscal Agent ancillary systems that may be impacted in some way by the Provider Services implementation. We will confirm these assumptions during the Requirements Validation phase of the project. In *Exhibit 3.6.2.5-1: Fiscal Agent Ancillary Systems*, we provide a description of the potential impact to each system, demonstrating our understanding of the State's existing environment.

Fiscal Agent System	MAXIMUS Considerations for Provider Services Implementation
Montana Access to Health Web Portal	The provider enrollment functionality on the MATH Web Portal will be replaced with the new enrollment functionality in the MAXIMUS Provider Services module. Also, MAXIMUS is proposing to provide Option A functionality and services in our proposal. As a result, much (if not all) of the self-service functions in the MATH Web portal will be replaced by the new functionality provided in the Provider Services module if the State chooses to implement Option A along with the base system.
AVR/IVR	MAXIMUS is proposing Option B Services in our proposal. If the State opts to procure these services, the provider enrollment related self-service options available under the current AVR/IVR will be replaced with the new scripts provided by MAXIMUS. Even if the State does not opt to procure our Option B Services, there may still be in impact to the current AVR/IVR as the Provider Services system will now be the system of record for Provider data.
FaxBack	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to Faxback as a result of the Provider Services implementation.
Avaya	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to Avaya as a result of the Provider Services implementation.
Digital Harbor	MAXIMUS Provider Services solution provides full ACA-compliant automated screening for providers, including monthly database checks. Even if the State does not procure our Option B services, the current Fiscal Agent will use the MAXIMUS Provider Services system for all provider enrollment activities including screening. As a result, the Digital Harbor tool will no longer be needed.
Optimal Imaging Technology	MAXIMUS will convert provider related images from this repository into the new Provider Services document repository. We will rely on the Fiscal Agent to provide us with a document index file and an image file to load the images into the new document repository. We performed such a conversion in our District of Columbia implementation, receiving the index file and images from the Conduent image repository.

Fiscal Agent System	MAXIMUS Considerations for Provider Services Implementation
Optical Character Recognition	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to OCR as a result of the Provider Services implementation. In addition, we anticipate a large deduction in paper provider applications once the online portal is implemented which could enable the state to eliminate this function for providers.
DPHHS Provider Website	The MAXIMUS Provider Services web portal could replace the need to house much of the provider related documentation on the current DPHHS Provider Website. We could also implement access to our application on this site and continue to utilize it. We will work with DPHHS during the DDI phase to determine exactly what will be stored on the new Provider Services web portal, versus what may need to remain on the DPHHS Provider Website. Our portal provides links and sections to allow self-service viewing and retrieval of all types of documentation, with an emphasis on provider and provider enrollment.
DocFinity	Based on our understanding of the requirements in the RFP, we anticipate replacing this product with our OnBase solution which is an integrated component of our Provider Services module. However, given the timeframe for implementation of the modules that will replace the current legacy MMIS, we anticipate this system will continue to function for some amount of time and we may need to create an interface to exchange provider documents. We expect to determine the exact requirements during system design.
Montana ACS Extranet	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to the Montana ACS Extranet as a result of the Provider Services implementation. However, Provider Services related files and reports produced by MAXIMUS that need to be viewed and consumed by DPHHS will be housed on a separate repository.
OmniAlert	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to the OmniAlert as a result of the Provider Services implementation. Provider data from the Provider Services module will be pushed to the MMIS as part of the MMIS interface. Any provider related data required for OmniAlert can continue to be retrieved from the MMIS.
OmniTerm	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to the OmniTerm as a result of the Provider Services implementation.
Third Party Recovery and Checklog System	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to the Third Party Recovery and Checklog System as a result of the Provider Services implementation. Provider data used by the system will either come from the MMIS or once the System Integration module is implemented could be shared through an ESB integration directly from the Provider Services Solution.
Medicaid Correspondence Generation Tool	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to the Medicaid Correspondence Generation Tool as a result of the initial Provider Services implementation. However, we do expect that provider enrollment and revalidation correspondence would begin to be come directly from the Provider Services solution so it is likely that some correspondence would be eliminated from this system.
Third Party Liability Letter Generation Tool	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to the Third Party Liability Letter Generation Tool as a result of the Provider Services implementation.

Fiscal Agent System	MAXIMUS Considerations for Provider Services Implementation
State Level Registry	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to the State Level Registry as a result of the Provider Services implementation.
Conduent Case Management	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to the Conduent Case Management tool as a result of the Provider Services implementation.
GEO Access	We do need to consider that provider data will be captured in the new Provider Services module. Our solution captures GEO coordinates as a part of USPS address validation for each Provider service location. MAXIMUS is unsure as to how the GEO Access system captures the coordinates for a Provider. We may need to consider that the coordinates be passed to the MMIS as part of the MMIS interface.
MoveIT/GrabIT	MAXIMUS also uses the MoveIT/Grab IT for provide secure file processing, storage and transfer. In our District of Columbia implementation, we use MoveIT//GrabIT for the secure file transfer of the conversion files, conversion image files, and MMIS interface files (both send and receive) with Conduent. Decisions on how the file transfer will work with Conduent for the Montana implementation will be collaboratively discussed and decided during the DDI phase of the project.
Convergence Point	Based on our understanding of the requirements in the RFP, we do not anticipate there would be any impact to Convergence Point as a result of the Provider Services implementation.

Exhibit 3.6.2.5-1: Fiscal Agent Ancillary Systems. *The MAXIMUS Provider Services Module accounts for system or data integration with ancillary systems that may still be used by the legacy MMIS.*

3.6.2.6 DPHHS Ancillary Systems

3.6.2.6 DPHHS Ancillary Systems

Health Insurance Premium Payment System

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

Quality Assurance Management System (QAMS)

QAMS is used to track trends, medication errors, and reporting critical incidents.

Tort Tracker

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

Agency Wide Accounting Client System (Developmental Disabilities Services)

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

Case Management Solutions

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

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

Therap-This system is used for incident reporting.

The Eligibility Screening System

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

Substance Abuse Management System

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

Web Infrastructure for Treatment Services

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

MAXIMUS has reviewed the available documentation from the RFP relating to the DPHHS existing ancillary systems. Based on the comparison of the RFP requirements to the DPHHS existing systems, our initial observation is that there would be no impact to these systems as a result of the new Provider Services module implementation. The existing systems appear to be more Member focused rather than Provider focused. However, we will need to confirm this assumption during the DDI phase of the project.

In our experience, State's typically have separate systems in place to track data and information related to Waiver and/or State-specific programs. For example, in our Nebraska Provider Services implementation, the State actually stores and maintains their Waiver providers on a system separate from their MMIS (Waiver providers were actually stored in their Eligibility system). This required us to create a separate interface to send Waiver provider data to a system separate from the MMIS. There was no existing interface between the Waiver system and the State's MMIS, so our Provider Services solution needed to provide sophisticated conversion, transformation and load routines to merge provider data to prevent duplicate providers from being stored in the new Providers Services database. As a result of this need, our conversion load routines, which are reusable components and services within our SaaS solution, contain sophisticated algorithms to blend and merge provider data from potentially disparate systems.

In addition to the data requirements being different for Waiver providers, we have also experienced that each State has radically different business processes for enrolling waiver providers. We have found that administration of the waiver programs vary from state to state and consequently have strived to design the process to be as flexible as possible. As a result, the MAXIMUS Provider Services solution contains configurable enrollment process and automated screening functionality for these Providers, many of which are categorized as moderate or high risk.

The reengineered Waiver business processes that typically result from our Provider Services implementations, which provide full electronic enrollment for Providers, sometimes result in the removal of existing State systems. The required documentation and attachments that are required for Waiver provider enrollment are now stored and viewable within the Provider Services solution whereas previously they were not. During the DDI phase of the project, MAXIMUS will confirm the Departments requirements as they relate to Montana waiver and State-specific programs and configure our solution as required to meet the data collection, workflow, and business rules needed for the State's programs. This will determine the impact on any of the Waiver related ancillary systems in place for DPHHS. MAXIMUS will also examine other non-waiver related DPHHS ancillary systems during DDI to determine if there will be any impact to those systems as a result of the new Provider Services implementation.

3.7 Future MPATH Environment

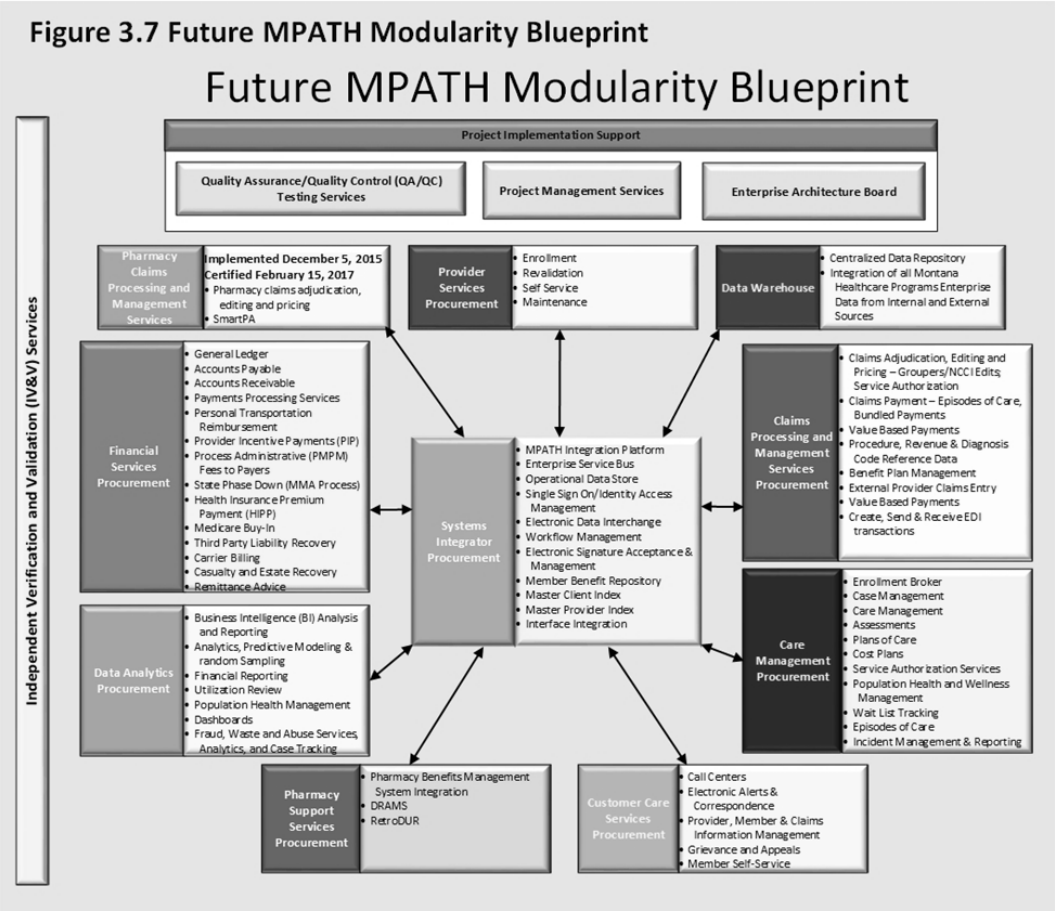
3.7 FUTURE MPATH ENVIRONMENT

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

DPHHS will contract with multiple vendors who will each provide a discrete set of components and/or services to support the MPATH modules and components. Each contractor will be responsible to operate and maintain its provided solution and will

work with the Systems Integration Services Contractor to integrate the solution with rest of the MPATH Integration Platform. Figure 3.7 below illustrates a high-level view of the to-be future MPATH Modularity Blueprint Environment.

Figure 3.7 Future MPATH Modularity Blueprint



X MAXIMUS has read, understands, and will comply will each requirement in this section.

The Department has recognized that the limitations of the legacy Medicaid Management Information System and the current service delivery organization require innovative ideas that will enable the Medicaid Program to evolve as new requirements are defined. The MPATH initiative was specifically designed to create the technical and operational environment for improving current Medicaid services while lowering costs. To support the State of Montana in this endeavor, MAXIMUS offers a comprehensive technology-enabled Provider Services module that is designed to become a component of a new service delivery solution that allows the State to overcome current system and organizational constraints, fully align with the Medicaid Information Technology Architecture, and meet the Seven Standards and Conditions for enhanced Federal Funding Participation.

MAXIMUS understands the current limitations facing Montana and has determined that flexibility in solution delivery is critical if we are able to support the modular structure envisioned by the MPATH project. We have already implemented solutions that help bridge the gap between new requirements and existing legacy systems and organizations. We do not believe "one-off" solutions make sense given the time and resources required to procure and implement them. Therefore, we have focused on developing a Provider Services solution that uses a combination of automated system functions that feature web service

enabled data collection, data sharing through interoperability, automated business edits and workflow, which are coupled with provider management services to support the full range of provider requirements specified in the MPATH RFP. Ultimately, we see our solution working as a component of the overall MPATH implementation in a seamless manner sharing data through the ESB to partner modules.

Our solution is configured to seamlessly exchange data with legacy systems, next generation systems and other web portals. Our solution's Open Interface Framework provides us with the capability to expose various functions of the system in different modes. This will enable Java based clients, .Net clients and other clients to easily consume and exchange data with the Provider Services module web platform. By exposing our solution's interfaces as services, we can enable these loosely coupled units of functionality to be used by trading partners and other software. Our Provider Services solution is built on the latest Microsoft technologies so we can create highly interoperable services and expose endpoints that can be consumed by both legacy and next generation systems.

As the future MPATH environment evolves, we will leverage the existing SOA capabilities of our solution to help the State respond more quickly and more cost-effectively to changing business needs. The expanded SOA architecture will include well-defined services that can be reused in both internal and external components. Apart from exposing the services needed by the state infrastructure, the MAXIMUS Provider Services solution is already capable of consuming the services exposed by the state or other partners. Thus, a provider coming to the web portal can easily get to the right functionality with the help of our intuitive user interface.

The use of a modular approach to replacing the various components of the legacy MMIS environment brings upon the need for extensive planning, coordination and partners who understand and agree with the approach. MAXIMUS is focused on supporting our customers in changing the Medicaid Program so there is more focus on service delivery and enabling technology that simplifies many of the administrative functions. With a proven record of three modular implementations, MAXIMUS has proven that we not only understand how to implement a modular solution, we support data integration and system interoperability through mechanisms that support SOA and legacy installations. Based on our experience, we fully expect to have to provide some data integration outside of the ESB and our flexible solution will enable the Provider Services module to be implemented ahead of the other MPATH modules and then integrate using the ESB as new modules are implemented.

3.8 Stakeholders and Governance

3.8 STAKEHOLDERS AND GOVERNANCE

X MAXIMUS has read, understands, and will comply will each requirement in this section.

MAXIMUS has reviewed the inventory of stakeholders that will be involved in the MPATH project, and understands that there will be governing stakeholders as well as stakeholders that are directly impacted by the project. MAXIMUS appreciates that the State has considered and listed all stakeholders involved in the project especially when we consider how additional modules will be added as the MPATH project evolves. From a project governance perspective, reviewing the stakeholder list reassures us that the people, process, and technology we have in place, which we are proposing based on our extensive experience in implementing modular Provider Services solutions, is the right mix to promote the success of the MPATH project. From a project management perspective, the

stakeholder list will shape our Communications Plan, which will be a critical vehicle in support of our approach to meet Montana's vision, objectives, and goals. From a system implementation perspective, the list of stakeholders helps us to visualize the correlation of system users (both internal and external) to the existing user roles we bring with our Provider Services SaaS solution. Our executive management staff along with the onsite project manager will work collaboratively with the State and other module vendors to promote partnership and communication across the MPATH project.

We build a partnership with the State, beginning with the DDI phase of the contract and continuing throughout the entire project operations lifecycle, based on best practices of shared commitment and transparency of our operations. This partnership approach has proven to be successful in developing strong working relationships with our state government clients to manage and oversee our operations in Tennessee, Nebraska and the District of Columbia. In the sub-sections that follow, we highlight our understanding and approach for promoting the success of the MPATH project as it relates to the involvement and engagement of all project stakeholders.

3.8.1 Governing Stakeholders

3.8.1 Governing Stakeholders

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

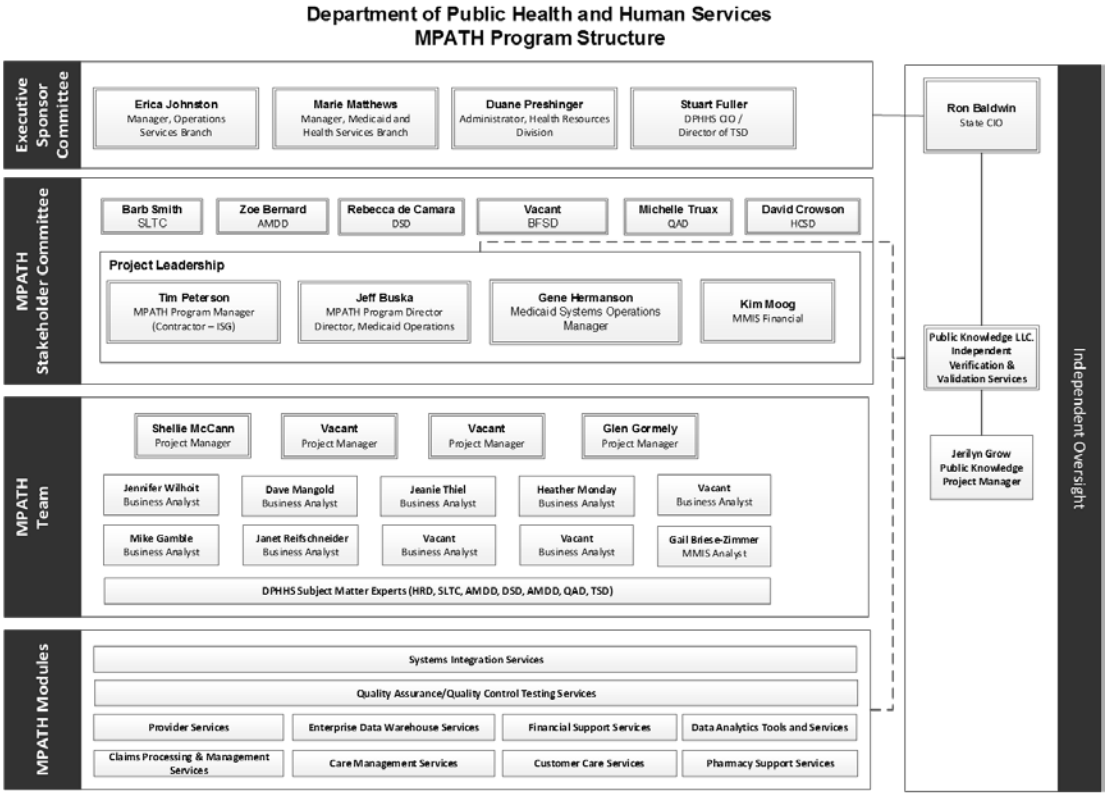
Center for Medicare and Medicaid Services (CMS): CMS is the government entity responsible for authorizing enhanced federal funding for the design, development and installation or enhancement of a state's MMIS. The Mechanized Claims Processing and Information Retrieval Systems (90/10) Final Rule, effective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

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

1. The Medicaid and Health Services Branch of DPHHS is responsible for contractual administration and Fiscal Agent management responsibilities.
2. The Human and Community Services Division (HCSD) is responsible for Member eligibility determinations.
3. The Business and Financial Services Division (BFSD) is responsible for the accounting and financial functions of Montana Healthcare Programs.
4. The Health Resources Division (HRD) is responsible for overseeing and managing the Acute, Physician and Hospital programs. The care management, Healthy Montana Kids (HMK) and Montana Health and Economic Livelihood Partnership (HELP) programs are also located in this Division.
5. The Senior and Long-Term Care Division (SLTC) is responsible for overseeing and managing the Nursing Facility Services and Home and Community Based Services programs.
6. The Addictive and Mental Disorders Division (AMDD) is responsible for overseeing and managing the adult mental health, behavioral health, home and community services, and chemical dependency programs. The State funded MHSP is also located in this Division.
7. The Quality Assurance Division (QAD) is responsible for all activities related to Program Integrity and third-party liability programs.
8. The Disability Services Division (DSD) does not currently reimburse providers through the MMIS system. However, the DSD will be utilizing the new systems and services procured via the MMIS Replacement Program. This division is responsible for overseeing the Developmental Disability, HCBS waiver and the Children's Mental Health program.

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

Table 3.8.1 MPATH Program Structure



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

MPATH Stakeholder Committee: The MPATH Stakeholder Committee is made up of the division administrators from each DPHHS division and the MPATH Program leadership. The division administrators advise the MPATH Program Leadership on business requirements, program rules and policies. The Division administrators also ensure subject matter experts are available to MPATH DDI Team as necessary to provide detailed insight into specific processes or procedures.

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

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

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

> Project Governance Team: For each MPATH module there will be a project governance team comprised of the Medicaid Systems Operations Manager, the Program Manager, and the module specific Project Manager. The project governance team will meet regularly with the Contractor to review project status, scope, schedule, issues, risks, and quality and will make recommendations to the DPHHS Stakeholder Committee and the Executive Sponsor Committee. The project governance team will also be responsible for approving project deliverables and change requests.
>
> Project Manager: For each MPATH module, a Project Manager will be designated by the Medicaid Systems Operations Manager to work with the Contractor's project manager to coordinate DPHHS activities related to the project. The Project Manager will be responsible for day-to-day contract administration and ensuring compliance with the contract, monitoring scope, schedules, issues, risks and quality.
>
> Lead Business Analyst: For each MPATH module, a lead business analyst will be designated by the Medicaid Systems Operations Manager and Program Manager to work with the Contractors to participate in requirements validation, solution review sessions and other project meetings. The Lead Business Analyst will be responsible for research and provide timely responses to Contractor inquiries and requests, completing deliverable reviews and conducting parallel and user acceptance testing.
>
> Independent Validation and Verification (IV&V) Contractor: The State's IV&V Contractor, Public Knowledge LLC., is responsible for assessing project management methodologies and project execution and validates conformance of the product and project to RFP requirements and to the contract. The IV&V Contractor further assists the MPATH Program Management Office in monitoring project schedule, scope, quality, risk and completing MECT milestone reviews and Certification activities for each project.

The list of roles and committees provided in the RFP for the MPATH governing stakeholders is comprehensive and it is clear the Department has put a great deal of thought into the planning effort for the MPATH project. All of the governing stakeholders will play key roles on the project throughout all phases of the Providers Services module DDI and this involvement will extend into the operations phase.

MAXIMUS has reviewed the MPATH high-level timeline as provided in the RFP. While our obvious focus will be on the initial implementation of the Provider Services module for the State, we also recognize that there will several projects in motion before, during, and after the Provider Services implementation. Of particular importance will be the parallel efforts involved with the Provider Services module and the Systems Integration module implementation. We understand, for example, that the initial interface with the MMIS will require a flat file SFTP file exchange due to the limitations of the current legacy MMIS and also due to the initial absence of any consumable web services within the State's Enterprise Service Bus (ESB). As a result, it will be critically important that project status and communication channels are open and transparent between all parties involved in the design and implementation of the interface. This will include many of the governing stakeholders but also must include the State's System Integration Services vendor, the State's Fiscal Agent, and the State's IV&V vendor. There are also functions within the Provider Services module that may have to be delayed until other modules or specifications for particular products have been completed. MAXIMUS will work closely with DPHHS and the other module partners to understand the dependencies between projects and clearly communicate items that must be jointly agreed upon.

An understanding of the stakeholders involved in the entire MPATH project is critical to understanding and directing the appropriate channels of communication. Through implementing our modular solution in several States, we have recent, practical experience in knowing the importance of stakeholder involvement throughout all phases of the project with an emphasis on establishing (and documenting) system boundaries and responsibilities between multiple vendors. In *Exhibit 3.8.1-1: MPATH Governing Stakeholders* we document our understanding and identify how our approach will support Montana's vision, objectives, and goals for the MPATH program.

MPATH Stakeholder	MAXIMUS Considerations for Provider Services Implementation
CMS	MAXIMUS and DPHHS will work with CMS to make sure our solution, approach, and services comply with all regulations and are certifiable to meet all the federal reporting requirements necessary to secure CMS authorization of enhanced federal funding. Certification efforts of the MAXIMUS Provider Services solution are well underway in Nebraska and the District of Columbia. As a result, our team has current experience with the new modular implementation procedures. MAXIMUS will integrate certification activities into our DDI approach and provide appropriate documentation and support during the various review that must occur as part of the DDI effort. We will also draft certification plans and checklist responses, and prepare the evidence and artifacts required for the CMS Certification Final Review (R3). Please refer to *Section 3.10.3–Certification* for further details on our CMS related experience in modular implementations.
DPHHS	MAXIMUS recognizes that DPHHS is responsible for the administration of Montana Healthcare Programs and for the administration and oversight of the MPATH modules and components. MAXIMUS will work with all stakeholders and subject matter experts within each division of the agency as needed throughout the project. We will provide regular open and transparent communications and our Helena-based Project Manager will regularly meet with DPHHS staff throughout the implementation effort and throughout the entire project.
Medicaid and Health Services Branch of DPHHS	We anticipate needing to work with this branch of DPHHS as it relates to contract management of our services under the MPATH procurement. We also anticipate working closely with stakeholders from this branch to understand how our system will impact current fiscal agent operations and to meet state level requirements for our system functions.
Human and Community Services Division (HCSD)	Based on the defined role for this division, we would not anticipate frequent communication or involvement, but we will need to determine the extent to which stakeholders and potential users within this division are concerned with Provider enrollment. We plan to fully engage these stakeholders to understand the level of involvement necessary.
Business and Financial Services Division (BFSD)	We would anticipate stakeholders from this division providing input into the financial related workflows within the Provider Services solution including collection of ACH/EFT data and handling of application fees that may be collected as part of the enrollment process. Depending on how DPHHS wants the financial related workflows configured for the Provider Services solution, we will likely need to configure system roles that will oversee and manage these workflows. For example, in our Tennessee provider implementation, there are 2 separate user roles defined in the State's accounting division for the review and approval of ACH/EFT information submitted by Providers and interfaces with external systems to support EFT enrollment.
Health Resources Division (HRD)	MAXIMUS will work with staff from this division during the DDI phase of the project to define the specific requirements for the providers supporting these programs. We understand that program policy may be directed at a more central level, but interaction and communication with staff from this division will be helpful to confirm we understand the programs.

MPATH Stakeholder	MAXIMUS Considerations for Provider Services Implementation
Senior and Long Term Care Division (SLTC)	MAXIMUS assumes we will be required to work with subject matter experts from this division during the DDI phase of the project. MAXIMUS will rely on DPHHS to make us aware of any needed involvement from SLTC. Based on our experience, data and workflow requirements for Nursing Facilities and HCBS providers will require input from this division, and in some states, we have created specific user roles SLTC staff to support various aspects of provider enrollment and precertification of services. For example, in our District of Columbia Provider Services configuration, we created an LTC Reviewer role that is involved in the final approval of EPD Waiver and ADHP 1915(i) Providers. In Nebraska, LTC staff refers eligibility waiver providers for enrollment.
Addictive and Mental Disorders Division (AMDD)	As with the SLTC staff, MAXIMUS assumes we will be required to work with staff from this division during the DDI phase of the project. We anticipate gaining valuable program understanding and provider enrollment and screening rules for the providers supporting these services.
Quality Assurance Division (QAD)	We assume that subject matter experts within this division will need to participate during the DDI phase of the project. In all 3 of our implementations, users from this Division participate in several workflows within the application, some examples include: ▪ New Enrollment: Refer to State – potential adverse action during screening ▪ New Enrollment: Refer to State - Approve retroactive Effective Date request for Provider ▪ New Enrollment/Revalidation: Refer to State - Review hardship Waiver Request for Application Fee ▪ New Enrollment/Revalidation: Refer to State – Provider Appeal ▪ New Enrollment/Revalidation: Refer to State – Disenroll Provider MAXIMUS will work with subject matter experts from this Division and the State's Lead Business Analyst to confirm the user roles required for this Division and the steps where they will need to be involved in system workflows. We also anticipate working with this Division to set the initial risk levels for providers and making updates to providers that have been moved into a higher risk level according to CMS requirements.
Disability Services Division (DSD)	We assume that subject matter experts within this division will need to participate during the DDI phase of the project in developing enrollment, revalidation, and update workflows relating to the pre-approval and final approval for providers offering services under the State's DD and HCBS Waiver program. MAXIMUS will work with subject matter experts from this Division and the State's Lead Business Analyst to confirm the user roles required for this Division and the steps where they will need to be involved in system workflows.
Executive Sponsor Committee:	MAXIMUS will strive to establish a collaborative working relationship and partnership with this important committee at the onset of the project. Participation of this committee on the Provider Services MPATH module will be critically important in making timely business and technical decisions regarding the Provider Service's module integration with the Medicaid Enterprise. MAXIMUS structures our project status reports to provide an accurate summary of the project as well as documenting risks and issues. This committee will have a vested interest in reviewing our status reports and it will be important that timely actions are taken by this committee when required. MAXIMUS proposes that our Contract Manager participate on this Sponsor Committee so that we have visibility into the overall project and can make timely decisions in conjunction with the overall plans.

MPATH Stakeholder	MAXIMUS Considerations for Provider Services Implementation
MPATH Stakeholder Committee	Active and engaged participation of all DPHHS Division administrators will be critically important to a successful implementation of the Provider Services module. During the requirements validation and design phases of the DDI, MAXIMUS will rely on the leadership of these administrators to provide guidance to the MPATH DDI team for policy decisions and business requirements. It will also be important for the Division administrators to allocate and provide the required subject matter experts to the project, as needed during the DDI phase. We propose that our Project Manager participate in this committee so that we can keep project issues visible to all project stakeholders. We also think that this committee can assess how best to modify business processes to reduce project risk and simplify testing by using the flexibility of our workflow and rules engines
Program Director	We anticipate that our Contract Manager will have a direct communication channel to the State's Program Director and will meet regularly. Questions and issues relating the contract will need to be discussed periodically throughout the project and our Contract Manager will be available in person as required. However, given that our Project Manager is onsite, we would also propose a direct communication channel to the State's Program Director. We will establish these protocols as a part of the project Communication Plan and Issue Resolution Plan and implement the process that works best for the project.
Program Manager	We anticipate daily interaction with the State's Program Manager as we configure and implement our solution. We expect the Program Manager will take more of a hands-on role as it relates to potential scope, schedule, issues, risks, and quality concerns on the project. The MAXIMUS Project Manager should have a direct line of communication to the Program Manager and meet in person as required but no less than weekly. We will document these procedures as a part of our overall Project Management Plan for the project. Based on our experience in implementing modular Provider solutions, we believe that a close working relationship between the State and MAXIMUS Project Manager lead to open communication and teamwork and allow the project to work through minor scope changes and project related issues. We prefer to keep the project moving and avoid an over-engineered change management process that consumes the valuable time of both State and MAXIMUS staff. Our approach is more agile and iterative, and our flexible system allows us to adapt to change more easily than a rigid COTS solution. There will be times however where scope issues, risks, and issues merit the attention of the Program Manager. Our approach promotes building an open, transparent, and trusting relationship with our State colleagues and we intend to bring that approach to the MPATH project to swiftly and collaboratively resolve potential project issues.
Medicaid Systems Operations Manager	Our management team's interaction with Medicaid Systems Operations Manager will need to be discussed and documented in our Communications Plan. In other States, the State staff member that facilitates and coordinates the meetings required between MAXIMUS and the State Fiscal Agent for purposes of designing, testing, and implementing the MMIS Interface and Conversion processes is a key resource. We know that the MMIS Interface and MMIS Conversion process are the heavy-lift in Provider Services modular implementations. It will be critically important to the project that key technical and business members knowledgeable of the State's legacy MMIS are present and engaged throughout all phases of the DDI. In addition, since the fiscal agent staff will be using our Provider Services module to support the provider community, it is important they actively participate in the design of the workflows. We look forward to working with the Medicaid Systems Operations Manager, regardless of this staff member's responsibilities on the project.

MPATH Stakeholder	MAXIMUS Considerations for Provider Services Implementation
MPATH Program Management Office	MAXIMUS is meticulous about tracking the progress of the project. All project staff are require to report progress against their individual assignments on a weekly basis so completion percentages can be applied to the project plan task and an accurate assessment of the project completion can be reported against the planned progress to date. Our Project Status Reports contain an Executive Summary listing the highlights and discussion items for the week. The remainder of the status report provides the detailed data that supports the summary and dashboard assessments. We anticipate that our weekly status reports will be sent to the State's PMO. We are confident that the detail contained in our status reports will provide the PMO (and all DPHHS stakeholders) with a solid understanding of the status of the project and alert the PMO to potential issues that may require recommendations to the DPHHS Stakeholder Committee and the Executive Sponsor Committee.
Project Governance Team	MAXIMUS anticipates having frequent communication and interactions with the Project Governance Team. This team's focus will be on the Provider Services module, which is the scope of our work under the procurement. Please refer to our narrative earlier in this section to see a description of our approach for dealing with the individual members that comprise this team. We would expect that members of this team would be present at our weekly status meetings and would be engaged in any of the detailed discussions that would occur during those status meetings. We also understand that this team will be responsible for the approval of project deliverables and change requests. We fully anticipate our Project Manager and Lead Business Analyst will work closely with members of this team on project items. We are pleased that the State has required the use of the Deliverable Expectation Documents (DEDs) as part of the MPATH project. MAXIMUS follows this approach in our Provider Services implementations. Creation of the DED helps clarify the deliverable requirements from the RFP and lays a blueprint for creation and ultimate acceptance of the deliverable.
Project Manager	The MAXIMUS Project Manager will be responsible for the execution of our implementation plan. We expect frequent interaction with the Provider Services module Project Manager throughout all phases of the DDI. Our Project Manager will be proactive in her communications with the MPATH Project manager and will be available to be onsite as necessary. Our PMP Certified Project Manager brings to the project recent and relevant experience in implementing Medicaid systems, and specifically modular Provider Services systems. As a result, our Project Manager is well aware of project governance issues that merit attention and aware of business related issues that require attention. We look forward to working with the individual that the State assigns to this all important role on the project.

MPATH Stakeholder	MAXIMUS Considerations for Provider Services Implementation
Lead Business Analyst	The Lead Business Analyst from DPHHS will play a vital role on the project. We will rely on this resource to be knowledgeable of the existing business processes in place for the program as well as to be knowledgeable of the existing data needs for Provider Enrollment. We expect that the Lead Business Analyst at times will need to draw on other subject matter experts within the Medicaid agency to provide responses and decisions to design related questions that surface during the requirements validation and solution review sessions. We envision a project model where the MAXIMUS Lead Business Analyst works closely with the DPHHS Lead Business Analyst to transfer knowledge to support the design, testing, and implementation of the system. In our experience, this role is one of the most critical roles on the project. Keeping the project schedule on track requires timely decisions and active engagement by the Lead Business Analyst. Our approach to design/configuration is agile, iterative, and interactive. During design sessions, we provide live demonstrations of our solution to the project stakeholders in the context of the business area being discussed. This helps the Lead Business Analyst gain a visual understanding of how the system will support the required business functions. We have found that using this approach promotes quicker and more practical decisions on potential changes to workflow or data collection requirements as it relates to provider enrollment. The early visualization of the system also will prepare the Lead Business Analyst for her responsibilities during the parallel and user acceptance testing phases of the project.
Independent Validation and Verification (IV&V) Contractor	MAXIMUS understands the importance that the IV&V contractor will bring to the project. We are confident that our proven project management and software development methodologies, combined with quality control procedures we have in place for our deliverables will result in little or no concerns raised by the IV&V vendor during the MPATH project. We will work closely with the IV&V vendor to educate them on all aspects of our approach and provide them adequate status information throughout the project. Certification efforts of the MAXIMUS Provider Services solution are well underway in Nebraska and the District of Columbia, and we have been required to work closely with the IV&V vendors for these customers to prepare certification materials and support CMS visits including the CMS Certification Final Review (R3). We have learned from other certification efforts that even with the new federal guidance in the 2.2 checklist, there can still be significant difference of opinion among the State, the IV&V vendor and MAXIMUS as to the true requirements of individual items. Establishing a baseline understanding at the beginning of the project will save significant time and effort during the process. To reduce this potential risk, the MAXIMUS Certification Manager will take steps to establish these baseline understandings with DPHHS and the IV&V contractor early in the project. Regular checkpoints throughout the project will help confirm these understandings.

Exhibit 3.8.1-1: MPATH Governing Stakeholders. *Based on our experience, we demonstrate an understanding of the multiple types of governing stakeholders involved in modular implementations and the key factors MAXIMUS considers important to limit risk and promote project success.*

3.8.2 Impacted Stakeholders

3.8.2 Impacted Stakeholders

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

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

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

The strength of the MAXIMUS Provider Services core solution is the self-service options we offer through the web portal specifically for providers along with the paperless process and the speed at which applications, revalidations and data updates are processed. In each of our implementations, we have seen extensive gains in the speed of the entire enrollment and screening process and have received very positive feedback from the end users or our system.

Provider Testimonial
MAXIMUS DC Provider Services Implementation

"For the past 9 months, MedStar Provider Enrollment Staff have been utilizing the DC Provider Data Management System. As a user of the system, our enrollment staff is extremely satisfied with the PDMS system and automated processing of our providers applications. As one of the biggest groups in DC with more than two thousand providers moving away from paper application packages the new process has been helpful and cost effective. (No more paying for FedEx shipping or USPS Certified Mail, constant traceable communication of additional information requests, etc.).

Although the DC Government Rule required an application processing time of 30 to 45 business days, MAXIMUS Project Manager and Operations Staff worked diligently to ensure efficient processing of our providers applications, many within 5 to 10 business days cutting the regular application processing time by more than 20 days. "

- Ottilia Kufcsak, Manager Provider Enrollment and Contracts
  MedStar Physicians' Billing Services

We have provided a detailed narrative on the existing capabilities as it relates to provider enrollment, revalidation, and update in *Sections 3.10.10–Enrollment*, *3.10.1–Maintenance*, and *3.10.12–Self Service Portal*. As part of the Option A services proposing, we will also offer self-service functionality to allow Providers (and Trading Partners) a variety of other self-service options including claims submission, warrant inquiry, and remittance advice inquiry. These self-service functions provide additional capabilities to make it easier for providers to perform Medicaid Services.

While we closely focus on the provider community, Medicaid members also directly benefit from the new Provider Services model. During the data conversion effort, we will identify and work with the Department to correct problem data, identify data anomalies, and deliver correct and complete provider data. Our address verification software will not only provide correct addresses, it will also populate geo-codes so that provider locations can be mapped to help members find them. Accurate provider data is critical for the enrollment broker to correctly assign members to PCPs and potentially MCO plans. We also make provider data accessible to MCOs directly so they can validate providers are eligible to perform services and eliminate duplicate providers in their systems. Finally, accurate provider data can be made available directly to members through a Provider Directory. We are able to provide access to real-time provider data to help members find the services they need from providers that are in close proximity to residence.

Exhibit 3.8.2-1: MPATH Impacted Stakeholders summarizes our understanding and highlights our approach for the impacts that our solution will have on the Montana provider and member user community.

MPATH Stakeholder	MAXIMUS Considerations for Provider Services Implementation
Members	The implementation of the MAXIMUS Provider Services solution for the State will directly contribute toward the Department's goal of improving outcomes for Montana Healthcare Program members by making accurate real-time provider data available to members and to the systems that assign members to providers. The sophisticated and efficient self-service provider enrollment process in our solution significantly reduces the time it takes for providers to enroll. The system functions and edits deliver accurate and validated provider data. Our solution also brings extensive screening capabilities that prevent potentially unsafe or fraudulent providers from becoming eligible service providers to eligible State Medicaid recipients. The public search capabilities that are packaged within our solution allow members and authorized reps to easily locate active providers in geographic regions of the State by using a GIS search, providing full details of the Provider and giving directions to the Provider's servicing location. Throughout *Section 3.10.10–Enrollment*, *Section 3.10.11–Maintenance*, and *Section 3.10.12–Self Service Portal* we provide detailed narrative and examples of how our solution will directly benefit the State's Member community.
Providers	The MAXIMUS Provider Services solution is an ACA-compliant system that supports all of the Provider enrollment and screening functions required by federal regulations (42 CFR 455 Subpart E). It offers Providers an intuitive, easy-to-use web portal for submitting new applications, re-enrollments and revalidations electronically. The system is designed to prevent ineligible Providers from enrolling and/or remaining enrolled in the State's Medicaid program. The production-proven, configurable business processes built into our solution will maximize efficiencies for Providers as well as Department staff users. As part of the Option A services we also offer self-service functionality to allow Providers (and Trading Partners) a variety of other self-service options including claims submission, warrant inquiry, and remittance advice inquiry. The core functionally we bring with our base Providers Services solution, combined with the additional features we offer with Option A will directly contribute toward Providers receiving timely and accurate reimbursements, and to receive accurate and timely responses to inquiries via the self-service web portal. Please refer to *Section 3.10.10–Enrollment*, *Section 3.10.11–Maintenance*, and *Section 3.10.12–Self Service Portal* for a detailed narrative and examples of how our solution will directly benefit the State's Provider community.

Exhibit 3.8.2-1: MPATH Impacted Stakeholders. *Our solution will benefit both the Member and Provider community for the State, leveraging the robust and production-proven system and services we bring with our core Provider Services module as well as the functionality we provide with Option A.*

3.9 High Level Scope of Work

MAXIMUS offers a comprehensive SaaS Provider Services solution that has been deployed successfully in three states as a standalone module in the Medicaid enterprise. MAXIMUS uses a project management-based methodology to control how we will design, develop, and implement our Provider Services Solution. We understand the importance of replacing the provider service functions currently supported by the legacy MMIS and finding the right approach that completes the project requirements in a timeframe that is acceptable as well as achievable. Our solution provides the advanced technology and service delivery capabilities necessary to meet the State's vision for the MPATH project while aligning with the MITA and meeting the Seven Standards and Conditions for enhanced federal funding participation. We have developed a proven implementation model accompanied by a process-based project approach that includes risk mitigation, lessons learned, and a highly skilled team that has completed similar efforts using our system as the base solution.

3.9 HIGH LEVEL SCOPE OF WORK

In the past, DDI efforts for the Medicaid Enterprise have been governed largely by the functionality that the MMIS contained. These engagements followed standard software development methodologies, often reviewing the same requirements every time an MMIS was bid. This traditional approach severely limited innovation by vendors, limited the state's ability to implement new business processes, and impacted Members and Providers because the systems received were focused on satisfying the business needs within Medicaid rather than on a specific business needs of the providers and members. The policies within the MITA and the Seven Standards and Conditions for Enhanced Funding equip states with a standardized model to review their strategic goals and objectives, and target business capabilities that will enable the transformation of their Medicaid enterprises into a nationwide network of integrated systems. The standardized model will support interoperability, shared standards, rapid response to changes in program and technology, timely and accurate data, performance measurements, and coordination of health care outcomes within the Medicaid community.

MAXIMUS understands the scope of work for the Provider Services module revolves around the replacement and modernization of the provider enrollment and management functionality provided by the legacy MMIS and the Montana Access to Health (MATH) Web Portal. This MPATH initiative sets the stage for an entire slate of new modules that will change how Medicaid services are provided and how the Medicaid Program supports the member and provider communities. The Provider Services module must support the functional requirements for provider management, and provide the advanced technology and data sharing capabilities that will enable seamless integration across the entire MPATH platform.

The MAXIMUS solution's technical architecture is driven by configurable workflows and business rules that support the enrollment, screening and update requirements from ACA; it also drives electronic communication with Providers. We developed our solution to integrate seamlessly with both legacy environments as well as modern platforms utilizing web services and SOA messaging via an Enterprise Service Bus (ESB).

Throughout our proposal, MAXIMUS describes how we use formal processes and procedures to create an operational and technology solution to support the Department. We meet the ACA Provider screening and enrollment requirements and provide improved self-service by configuring and deploying our Provider Services Module for MPATH. We are committed to supporting the Department's objectives for this project and are confident that our solution:

- Increases automation and communication between agencies to access data timely and appropriately, removing the need for the volumes of paper that currently move between sites
- Achieves full compliance with 42 CFR Part 455 Subpart E
- Satisfies all elements of both the MITA 3.0 Provider Data Management Business Process and the elements of the MITA 3.0 Eligibility and Enrollment Management Business Process
- Enables seamless integration with the other MPATH platform modules
- Provides an online Provider directory with an enhanced user experience to allow easy access to real-time Provider information
- Includes the provider self-service options specified in Option A
- Includes the full range of business operations services included in Option B

MAXIMUS understands that flexibility in solution delivery is critical. Our flexible SaaS solution, which is production proven and certifiable, meets the majority of the State's needs through configuration rather than customization. Our solution uses a flexible workflow engine that integrates with the Corticon Business Rules Engine, and uses a SOA capable, Open Interface Framework to enable reuse and configuration.

While our proposal addresses the business and technical requirements in the RFP specifically for Montana, MAXIMUS understands this procurement will support a multi-state cooperative procurement initiative through NASPO ValuePoint. Having implemented our modular solution in three states, we focus on providing a solution that is quickly adaptable to the different business rules required by state-specific Medicaid Programs. We are prepared to assist all of the NASPO ValuePoint states in implementing our system and operational solution.

3.9.1 Solution

> The Provider Services solution will replace and modernize provider enrollment and management functionality provided by the legacy MMIS and the Montana Access to Health (MATH) Web Portal.

The MAXIMUS Provider Services solution will replace and modernize the provider enrollment and management functionality that is currently supported by the legacy MMIS and MPATH Web Portal. We have designed our solution to make the enrollment and data update process simple to maximize Provider use of the web portal and eliminate the need for paper processing. The solution’s web portal functionality includes targeted data entry workflows based on business rules, validation of field input, user validation, an electronic signature, and a record of the application receipt date. We enable document upload directly to our content management solution, automatically linking the document with the appropriate provider record. The flexible workflow engine allows us to configure and optimize the business processes required for the entire Provider enrollment and screening process, including the involvement of Department staff within the workflow, as needed. By configuring our business processes to match the Department’s requirements, we are confident in our solution’s ability to fully modernize and replace the Department’s current provider enrollment and management functionality provided by the legacy MMIS and MPATH Web Portal.

3.9.2 Meeting 'To-Be' Vision

The Provider Services solution will meet Montana's "to be" vision, for the Provider Eligibility and Enrollment, Provider Management, as well as other applicable MITA business areas, detailed in the MITA 3.0 State Self-Assessment found in the Procurement Library.

Modern System Design

MAXIMUS will configure our Provider Services solution for the Department to meet Montana's "to be" vision for the Provider Eligibility and Provider Management functions. We provide Montana and Participating States with a modern solution aligned with the applicable MITA business areas, as referenced in the State's MITA 3.0 State Self-Assessment. We built our solution on the guiding principles of MITA, and equipped it to support all of the provider management functions within the Medicaid enterprise. Our solution uses modern day technologies; addresses security needs to facilitate confidentiality, availability, and integrity; enables support for data integration and interoperability; and our system methodology uses agile principles based on industry standards. The combination of our flexible technical architecture and reliable product implementation methodology brings Montana a fully compliant Provider Services Solution aligned with the goals and objectives of MITA.

The architecture of our solution was developed to adhere to MITA principles by incorporating an industry standard business rules engine, Progress Corticon, to enable the management of business rules outside the application. MAXIMUS recognizes the need for separation of business rules from other parts of the application code. Our solution has workflow rules, document/notice generation rules, reference table rules, document upload rules, screening categories, Provider type rules, risk level setting policy rules and MMIS interface preprocessing/validation rules. These rules can be changed quickly to align with the business process priorities set by the State. Our application is configured specifically to support the full range of provider business processes and we will configure the system to meet the business process requirements of the State.

The technical foundation for our system is based on a mixture of industry standard COTS products including Microsoft SQL Server as the database engine. The system uses the .NET platform as the main architectural building block for the application. .NET includes a large library of development tools, plug-in and functional components and is designed to be flexible to support multiple programming languages and third-party tools. To bring further openness to our system, we have coupled the .NET platform with a number of third-party Open Source toolkits that provide additional functionality to the application. This combination of products enables MAXIMUS to bring a cost effective solution to Montana. Our Provider Services Solution has been architected to specifically support the MITA 3.0 Goals as shown in *Exhibit 3.9.2-1: MAXIMUS Provider Services Solution Alignment with MITA Goals*.

MITA Objective	How the MAXIMUS Provider Services Solution Supports the MITA Objective
Develop ***seamless and integrated systems*** that effectively communicate, achieving common Medicaid goals through interoperability and standards	▪ Uses the MAXIMUS developed Open Interfaces Framework ▪ Uses industry standards for data exchange and promotes a web services based framework that supports ESB integration ▪ Service-based framework designed with web services ▪ Specifically designed to support the Provider Management business processes

MITA Objective	How the MAXIMUS Provider Services Solution Supports the MITA Objective
Promote an environment that supports ***flexibility, adaptability, and rapid response*** to changes in programs and technology	▪ Architectural foundation is based on the MITA maturity model ▪ Business processes optimized and flexible ▪ Standardized business model focused on streamlining administration of the program ▪ Data-driven framework for flexible business rules and configuration ▪ Flexible solution promotes lower cost of ownership and reduces operations costs
Promote an ***enterprise view*** that supports enabling technologies aligned with Medicaid business processes and technologies	▪ Supports multi-channel intake of provider enrollments, revalidations and date updates, including via web portal, paper (imaging), and phone ▪ Leverages enabling technologies in an open framework ▪ Specifically designed to support the MITA 3.0 Provider Management business processes ▪ Specifically designed to integrate with existing Medicaid enterprise systems: local, state, and federal
Provide ***data that is timely, accurate, usable, and easily accessible*** to support analysis and decision making for health care management and program administration	▪ Data is accessible by all authorized stakeholders and information consumers via the web ▪ Real time dashboards provide the operations and Medicaid staff with a common, consistent view of all provider data ▪ Supports decision making for the operations management and decision support for state policy makers ▪ Solution is highly flexible and can be implemented in other states with minimal configuration ▪ Provider web portal provides self-service features for providers and allows professional, modern interaction between providers, the State, and MAXIMUS
Provide ***performance measurement*** for accountability and planning	▪ Our solution provides for the accurate and timely processing of provider applications and revalidations using a modern framework, including automated workflow. ▪ Business processes were designed first – followed by the technology implementation. This approach results in optimized business processes. ▪ Dashboards and reports provide user community with up-to-date status of the program to assist the users in determining the performance of the program and what steps should be taken to improve program performance.

Exhibit 3.9.2-1: The MAXIMUS Provider Services Solution Alignment with MITA Goals. *We have designed our solution to meet the stated MITA Goals.*

From a business standpoint, we felt the unique nature of the Provider Screening and Enrollment process necessitated that the system be built to be as configurable and flexible as possible to support the needs of each state as they implemented the program. Our Cloud-hosted solution provides us with the flexibility to support a variety of programs, scaled based on size and requirements, without needing to make a large investment in technology. Our solution will provide Montana and other participating states with a robust, production-proven, high performance, high availability environment allowing providers, operations staff, and Medicaid staff to access the application through the Internet using a multitude of web browsers. Our Provider Services Solution is specifically designed to support each of the MITA 3.0 provider-related business processes in a highly automated fashion.

3.9.3 Supporting a Web-based Self-Service Tool

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

The MAXIMUS Provider Services Solution is built on a web platform to equip providers with self-service tools to enable rapid online application entry and submission, online revalidation and real-time data updates. Our web-based user interface, web portal, and enhanced electronic messaging tools give providers a full slate of technology functions that enable enrollment and data updates to occur without the need for paper and without the need for any additional support outside of system access. Our solution is configurable and supports a dynamic, intuitive enrollment process that is driven by the identified provider role, risk level, provider type, and provider classification.

All of our Provider Service Solution rules are configured to consume multiple parameters such as application type, Provider category type, Provider type, enrollment type (new, update, re-enrollment) to give maximum control to the policy expert and to enable the implementation for any state. The rules engine factors the various parameters and depending on the context of the application, and returns the appropriate results. One of the notable requirement changes in one of our system implementations was to factor Provider specialties, in addition to the Provider types, when determining the risk level for a waiver Provider. We were able to quickly modify the rules to include specialty as a Risk level parameter for the waiver Providers.

We routinely configure the system based on specific enrollment, revalidation, and updated requirements based on provider type, specialty, and provider role. We have implemented a wide array of application types and support expedited enrollments for Ordering, Referring, and Prescribing providers as well as providers that have supported Medicaid members out of state. We have found from our existing modular implementations that the configurations and business rules for different providers are among the most complex to define between states. The flexibility of our solution coupled with the expertise of our project staff will enable us to support any number of provider type configurations.

Since our initial implementation of the web portal in Tennessee, we have continued to augment and improve the user interface based on feedback from our customers as well as the Provider community themselves. From our first implementation, Providers immediately began to gravitate to the web portal to submit their electronic applications and revalidations. We have seen with all of our projects that providers have been asking for self-service functions and the Provider community has been extremely satisfied with the time savings they have achieved in getting a Medicaid application submitted and approved. What once took several weeks to complete, now took only a matter of days and in some cases hours to complete. We took great care in designing the user interface to make sure that we did not 'over engineer' the site, making sure that the site would be simple, straightforward, and intuitive for providers to use.

Underneath the intuitive and easy to use web portal, our solution yields a technical platform for managing workflows that support assigning, routing, and monitoring tasks while giving supervisors the ability to prioritize, delegate, or reroute tasks as needed. Our solution automates all Provider management functions including the ability to:

- Enroll Providers and conduct periodic reactivation/revalidation activities electronically via a web portal
- Standardize and improve the data collection process through automated business edits and task-based workflows
- Screen Providers against verification databases, track the status of required Provider site visits and other outreach activities, and
- Monitor the payment of application fees as applicable.

Please refer to *Section 3.10.10–Enrollment*, *Section 3.10.11–Maintenance*, and *Section 3.10.12–Self-Service Portal* for further details regarding how our proposed solution will meet the Provider self-service web portal requirements for the implementation of the Provider Services module in Montana.

3.9.4 Support Provider Maintenance Activities

> In addition, the Provider Services module must also support provider maintenance activities for external and internal users that are founded on business process driven workflow automation principles.

The MAXIMUS Provider Services solution is designed to handle multiple updates from Providers, track the age of Provider data, and notify Providers of upcoming events and actions, including when they must revalidate their Provider information. The system will be configured according to current DPHHS policy to alert Providers and Department users when high-risk Providers are due for their three-year revalidation and when all other Providers are due for their five-year revalidation. We are able to configure the system to send automated reminders at varying intervals so that providers know when they must revalidate and are reminded as their due date approaches. The system is also configured to require the collection of application fees during the revalidation process, per CMS and DPHHS policy. Revalidation will include the same screening elements as appropriate for the same Provider type performing an initial enrollment but the process is reduced because we provide current data for the provider to validate rather than requiring new data entry.

Our solution also contains a configurable License Monitoring workflow. The License Monitoring workflow runs each night and sends notifications to Providers (email or paper depending on the Provider's enrollment profile) notifying them that a License is expiring. In the current configuration, Providers receive a notification at 60 days and again at 30 days, reminding them to return to the web portal to provide a new expiration date of their renewed license. If the Provider does not take the action to renew their license and the license expires, the system is configured to auto-terminate the Provider for failure to renew the license. Optionally, the system can be configured to refer these Providers to the Department for further review prior to taking the action to terminate the Provider.

The MAXIMUS Providers Services solution contains an Update Workflow, which allows existing Providers to use the web portal to make direct updates to specific types of data within their enrollment profile. Providers must not be due yet for Revalidation to be placed into the Update Workflow. In the current configuration, all updates submitted by a Provider are subjected to internal review. This however, can be configured in the system to only require a review of certain types of data that the Provider may update.

Please refer to *Section 3.10.10–Enrollment* and *Section 3.10.12–Self-Service Portal* for further details on the configurable workflows and provider maintenance functions offered as a part of our Provider Services solution.

3.9.5 Collecting Information

> The web-based application will collect required information to support decisions regarding approval or denial of a provider's enrollment request. The online application will accept the electronic attachment of supporting documentation and collect required electronic signatures.

The MAXIMUS Provider Services solution is a web-based application that facilitates the streamlined collection of all required information to support decisions regarding approval or denial of a provider's enrollment application. Our configurable solution is based on provider roles and provider characteristics, and requests only the information required for a particular enrollment type. We configure the data requirements for Providers based on program, application type and/or provider type and specialty. Our automated workflow guides the provider through the application process, validates data entry, and helps providers complete all necessary data entry and validation sections. Our online, wizard-based enrollment process also requests and accepts electronic attachments of supporting documentation and automatically uploads the records to our document repository. Once we have confirmed that all data necessary for the application has been collected and is correct, we display the agreements to the Provider for their review along with contract compliance information then collect their electronic signatures, as specified by the Department.

Please refer to *Section 3.10.10–Enrollment* and *Section 3.10.12–Self-Service Portal* for further details on the configurable workflows and data collection functions offered as a part of our Provider Services solution.

3.9.6 Leveraging Automated Workflow

> The solution would leverage integrated automated workflow so that data and documentation are routed to appropriate unit responsible for decisions on provider enrollment applications.

The MAXIMUS Provider Services solution's business process framework is referred to as the Business Process Engine. The Business Process Engine automatically executes the appropriate business process model based on the inputs from the business rules engine. Our solution provides a role-based interface for process definition that leads the user through the steps of defining the workflow associated with a business process. The user can choose a trigger for the workflow that will initiate the workflow. The trigger can be a scheduled event or an action. Authorized users are able to define tasks for the workflow, which can be either manual user driven tasks or automatic system tasks. The tasks can be parameterized, allowing the user to select these parameters from a predefined list of values. Users are also able to select roles for the tasks, which identifies which user role should be performing the task.

Our solution is packaged with several pre-defined user roles and workflows. We will configure these roles based upon DPHHS requirements. When the workflow tasks are defined, the worker role that will complete that task, is also identified. For example, any type of adverse action task will always be assigned to the state administrator role (which may be the State's Program Integrity staff) while provider review and screening tasks are assigned to the operator role (the Enrollment Specialist). Our flexible Business Process Engine will enable us to collaborate with the Department during the DDI phase to configure the

system so that data and documentation are routed to the appropriate unit responsible for making decisions throughout each step of the provider enrollment process.

Based on the knowledge we have gained from our past project, we are able to help the State understand best practices and, in some cases, the pitfalls of specific configurations. We will make available the wide array of workflow routing and approval configurations we have implemented as a starting point for Montana. Please refer to *Section 3.10.1.9–Workflow* for further details on the technical components and features of our Business Process Engine. Please refer to *Section 3.10.10–Enrollment* and *Section 3.10.12–Self-Service Portal* for further details on how we leverage the Business Process Engine to provide the functionality and workflows that are necessary to support a Provider Services modular implementation.

3.9.7 Updating/Revalidating Information

> In addition, providers may complete periodic updates and revalidation of their enrollment information via the self-service web portal.

A key functional component of our solution is the ability for providers to complete data updates and to complete revalidation activities directly from the portal. Please refer to *Section 3.9.4–Support Provider Maintenance Activities* earlier in this Section for a summary of our solution's capabilities for allowing provider self-service revalidation and update. Please refer to *Section 3.10.10–Enrollment* and *Section 3.10.12–Self Service Portal* for further details on the configurable workflows and provider maintenance functions offered as a part of our Provider Services solution.

3.9.8 Adhering to Federal and State Standards and Regulations

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

MAXIMUS Provider Services solution is packaged with a built-in and robust security mechanism that complies with federal architecture guidelines and standards (including NIST) and incorporates the appropriate evolving national standards including HIPAA privacy and security requirements. To control security across the multiple application tiers and numerous data interface components, our solution contains a variety of security layers to protect the application and its data.

HIPAA security and privacy compliance is a core component of our solution for the DPHHS. As a major state and federal vendor, MAXIMUS is required to comply with HIPAA across the majority of our health and human services projects. MAXIMUS designed all aspects of our solution to meet Medicaid requirements for interoperability, data exchange, security, and confidentiality. The solution addresses federal architecture guidelines and standards and incorporates the appropriate national standards including HIPAA privacy and security requirements and technological guidelines as defined by the Health Information for Economic and Clinical Health (HITECH) Act. Our security and privacy practices allow us to:

- Reinforce the ability to safeguard people, assets, and information through well-integrated, standard policies and processes
- Strengthen protection while improving system responsiveness
- Develop and implement action plans to build awareness of and enforce compliance with standards and protocols

Access control and associated policies, procedures, initiatives, security assessments, and technical security controls are based on compliance with the HIPAA Security and Privacy Rule and associated security control framework.

Our solution's web portal complies with state and federal accessibility standards, guidelines related to electronic information resources. The solution currently deployed in the Tennessee, Nebraska and District of Columbia is in full American Disability Act (ADA) Section 508 compliance, including accounting for the various forms of colorblindness. Checking for 508 compliance is embedded in the development process of the web portal, thus making it compliant for any new features that are introduced.

The MAXIMUS Provider Services solution is an ACA-compliant system that supports all of the Provider enrollment and screening functions required by federal regulations (42 CFR 455 Subpart E). The system is designed to prevent ineligible Providers from enrolling and/or remaining enrolled in the State's Medicaid program. Included in our ACA-compliant solution are automated screening and data matching functions with SSDMF, NPPES, LEIE, and EPLS. We also support the security requirements documented in trading partner agreements as specified in 45 CFR 162.915.

MAXIMUS has also reviewed the requirements for data retention based on business need. We are able to support a variety of retention requirements including those cited in 45 CFR 164.316 and Administrative Rule 37.85.414. We understand the Department may require a longer retention period on an exception basis to support ongoing business needs (e.g., TPL recovery and drug rebate). We will work closely with the Department on defining and implementing these requirements.

As required in our proposal, MAXIMUS has responded on how we meet all security standards, federal and state requirements and all laws, rules, and regulations (such as HIPAA and the ACA). Please refer to all subsections in *Section 3.10– Detailed Scope of Work* for detailed responses on all standards and compliance-based requirements.

3.9.9 Providing Optional Functionality

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

Additional Provider Services Option A

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

Additional Provider Services Option B

- Conduct Provider Site Visits
- Include Reference Documentation
- Provide Technical Help Desk Support
- Provider Services Call Center
- Staffing
- Collect and Enter State Auditor's Office Financial Information
- Provider Services Call Center Management System
- Integrated Voice Response System/Automated Voice Response System

Option A Services

The MAXIMUS Provider Portal is designed and built around what a Provider needs. Our web-enabled solution is easy to use and intuitive with functionality to alert providers via different communication mechanisms to initiate provider actions. In addition to this, we developed the web portal on a technology platform that is SOA-based, includes an open interface framework, and supports an ESB communications and technology backbone to support modern functions including mobile technology. This makes our solution the one stop solution for all provider needs.

In Tennessee, our client continues to move provider related functionality out of the MMIS and into our online provider portal. Recently, we implemented the ability for providers to obtain their remittance advice and 835 transactions online directly from the portal. We enabled this functionality using SOA-based messaging enabled by the MMIS ESB connecting our solution to the state's EDIFECS platform. We are currently in the process of enabling the remaining HIPAA transactions directly from the web portal through this same type of integration. These new functions provide the basis for our solution for the functions included in Option A and will be yet another aspect of our solution that is production-proven.

Please refer to *Section 3.10.13–Option A Provider Services* for further details on our approach for implementing the required Option A functionality for the MPATH project.

Option B Services

MAXIMUS excels at providing operational services in the Medicaid Market. In the Provider Services area, we currently provide full provider enrollment, screening, and management functions for four states all meeting the new ACA requirements. We have a proven model of implementing our Provider Services solution in conjunction with the full slate of business operations requirements included in Option B. Our current projects include call center services, IVR and call routing technology, enrollment and screening services, and customer service centers. Through our strong national presence and Provider operations in multiple jurisdictions, we currently manage Provider data and enrollment services for more than 200,000 Medicaid Providers. We will leverage this expertise, relying on best practices and lessons learned to deliver high quality end-to-end customized Provider enrollment and screening services that strive not just to meet, but exceed performance expectations.

Building on our more than nineteen years of experience serving Medicaid Providers, MAXIMUS is fully prepared to assist the State of Montana's efforts to implement and maintain enhanced Medicaid Provider screening and enrollment requirements mandated by the Affordable Care Act (ACA). Please refer to *Section 3.10.14–Option B Provider Services* for further details on our approach for implementing the required Option B services and support for the MPATH project.

3.9.10 Providing a Seamless End-User Experience

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

As the State of Montana prepares to meet the enhanced Medicaid Provider screening and enrollment requirements mandated by the Affordable Care Act, MAXIMUS offers a service delivery solution that is realistic, attainable, and appropriate for meeting all operational requirements. This solution combines our production proven Provider Services system module, our experience operating Provider services projects in several states, and our business processes for conducting Provider outreach, screening and enrollment, reactivation and revalidation, site visits, and other mandated activities.

MAXIMUS is uniquely qualified to provide both the system and automation functions required by the RFP (including the Option A functionality) and to provide the operational services under Option B. We are currently the only vendor to have a production-proven solution that contains every component required in the Montana RFP. In Tennessee, we operate the system only including the functions required in Option A. In Nebraska and the District of Columbia, we have coupled our proven Provider Services module with the full array of services included in Option B.

Regardless of what options each state requests, MAXIMUS can show a history of successfully completed projects. As a result, MAXIMUS can bring its experience and best practices to support the specific requirements of the State. In *Section 3.10–Detailed Scope of Work* of our proposal, MAXIMUS provides a detailed explanation of our proposed solution, which supports all business and application activities and requirements described in the RFP. We will demonstrate our clear understanding of the scope of work required for the Provider Services module by providing detailed descriptions and concrete examples of how we will meet each requirement within the proposed solution.

3.10 Detailed Scope of Work

3.10 DETAILED SCOPE OF WORK

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

MAXIMUS has conducted a detailed review and analysis of all RFP requirements. In addition to the main RFP sections, we have also reviewed each of the attachments included in the RFP. We understand that unless otherwise noted as Option A or Option B requirements, Attachment F requirements are mandatory and are included in our Base system solution.

We understand that these requirements can only be changed through written approval of DPHHS and MAXIMUS. To address each requirement in the scope of work, we have provided a summary of our approach followed by a response to each individual requirement. MAXIMUS is also proposing to support Option A and Option B and our solution and response to those requirements are addressed in response to sections 3.10.13 and 3.10.14. Attachment F contains our response for each requirement along with notes, where applicable.

3.10.1 Technical and Information Architecture Requirements

3.10.1 Technical and Information Architecture Requirements

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

The MAXIMUS Provider Services solution platform is built on a flexible design with a focus on user experience, ability to integrate, and configurability. This is achieved by taking advantage of a combination of mature technologies and a system architecture built to change and adapt. The MAXIMUS Provider Services solution uses Progress Corticon Business Rules engine and MicroStrategy to support business intelligence in a loosely coupled manner supported by a Business Process (Workflow) engine built on the .NET framework. To provide interoperability with other systems, the MAXIMUS Provider Services solution exposes well-defined service components based on open standards and is able to support data exchanges in any manner that a trading partner prefers. Our solution takes advantage of the open standard to efficiently integrate with disparate systems and we have successfully integrated with all required trading partners in the three modular implementations of our Provider Services solution.

The MAXIMUS Provider Services solution includes a consolidated data repository that allows authorized users to store, retrieve, and report on all data generated by processes and activities. The data repository will house all data and information produced during the provider application, enrollment, certification, and licensing processes, and maintenance activities, as well as all related data generated by multiple State agencies and Trading Partners. The data repository is updated in real-time as providers make updates, enrollment staff makes decisions, screening processes run, and workflows are executed. Depending on the specific requirements of each state, we may integrate a reporting platform into our overall solution with real-time connectivity to the main data store that is the system of record for provider data.

MAXIMUS uses MITA principles and standards for application development and maintenance. The technical foundation for our solution is based on a mixture of industry standard COTS products, including Microsoft SQL Server as the database engine. We have standardized our development platform using .NET; all software utilized is compatible with this platform. Our integrated development environment (IDE) uses Visual Studio with MSDN and includes access to all Microsoft software for development and test environments. The .NET framework includes a large library of development tools, plugins and functional components, and is designed to be flexible to support multiple programming languages and third-party tools. To bring further openness to our system, we have coupled the .NET platform with a number of third-party open source toolkits, which add additional functionality to the application. We also integrate third-party COTS products to support functions such as the rules engine and correspondence management. This combination of products enables MAXIMUS to bring a cost effective solution that minimizes risk.

To control security across the application tiers and data interface components, our solution contains a variety of security layers to protect the application and its data. The security scheme was architected to meet interoperability, data exchange, security, and confidentiality requirements defined by CMS. It addresses federal architecture guidelines and standards (including NIST) and incorporates the appropriate evolving national standards including HIPAA privacy and security requirements. User access to the solution is based upon security roles. Security roles are based on business function and necessary access to information. Security roles will control what data users can view, update, or report on. See our response to 3.10.1.2.1 for more details on our security architecture.

Underneath the intuitive and easy to use web portal, is a technical framework and platform for managing workflows that supports assigning, routing, and monitoring tasks and gives supervisors the ability to prioritize, delegate, and/or reroute tasks as needed. Our solution automates all Provider management functions including the ability to enroll Providers and conduct periodic reactivation/revalidation activities electronically via a web portal. Our solution provides extensive support functions designed to improve program performance including:

- Standardized and improved data collection processes through automated business and data edits controlled by task-based workflows,
- Interfaces with all approved trading partners to enable system interoperability across different platforms,
- Automated communications with providers throughout the enrollment, revalidation or update processes both electronically via email and on paper as required by provide preference to prompt action or provide reminders of activities,
- Screening of Providers against verification databases,
- Integration with partner systems including MCOs and the legacy MMIS or other Medicaid modules,
- Tracking the status of required Provider site visits, criminal background checks and other outreach activities, and
- Monitoring the payment of application fees as applicable.

Our provider services solution is integrated with the Corticon rules engine that controls how business functions are configured to support the State’s current and future needs. Our Solution has a number of

integration points including MMIS, Credentialing Verification Organizations (CVO) and the departments administering Waiver programs. We have successfully implemented interfaces with the Council for Affordable Quality Healthcare (CAQH) for all providers in Tennessee. Our solution also has a set of data exchange interfaces with the State, Federal and third party data sources including Managed Care Organizations (MCOs).

At the core of the analytics and reporting framework is an integrated business intelligence platform supported by MicroStrategy. The business intelligence suite provides authorized users with powerful reporting capabilities within the solution including the ability to create reports against audit data, perform scans against program data and trace activities that have occurred throughout the enrollment process. The basis for the reporting functions is the database structures that store all information about the enrollment and screening process and a uniquely defined reporting layer that makes standard and ad hoc reports easy to create and maintain. Our solution will use a combination of standard reports, dashboard reporting and online data to support the administration of the program. These reporting processes provide operational and management users with all required information about the overall enrollment status across the program as well as more detailed status by Provider type, business flow and even individual Providers. The output of all reporting functions can be made available online and allow creation in various formats including Microsoft Word, Excel, and Adobe PDF. Reports can be pulled as required or included in a schedule for running at a prescribed time.

While our solution meets all CMS-requirements for Provider enrollment and screening, we understand that the actual implementation of the regulations can vary from state to state to support differences in operational structure, differences in data collection requirements, differences in Provider populations, and differences in support systems. Our approach is to configure our solution to provide the functionality required by Montana by conducting project activities focused on reviewing the base configuration and determining if changes are required to meet contract requirements. Concurrently with this process, we will configure third party products to support some of the enhanced requirements including correspondence management and chat functionality. To complete this scope of work, MAXIMUS utilizes a formal software application development methodology that we use to manage all transition activities and after go-live to manage system maintenance and enhancement actions. *Section 3.10.2.1–Project Management* and *Section 3.10.2.2–Software Development Methodology* contains the details of our Integrated Project Delivery approach including explaining our methodology for completing all application development and maintenance activities.

Technical Architecture

The Montana DPHHS is supported by a number of Providers who perform both fee for service work as well as provide services for Managed Care Organizations (MCOs). Numerous systems have been implemented that contain Provider screening and enrollment functions as well as management of the associated Provider data. The disparity of systems and data collected coupled with the lack of fluidity of data movement has become especially problematic as states are asked to meet Federal and State requirements to cover new groups of individuals, verify their Provider networks are adequate to support their members, and enable members to find the best Provider for their individual situation. In addition, the lack of a central repository of current and accurate information on Providers makes it harder to avoid and detect fraudulent activities or to identify Providers who do not meet Medicaid Program requirements.

To combat these issues as well as to change how Providers interact with the Medicaid Program, MAXIMUS has developed a Provider Services application architecture driven by the business functions required to support Provider management including the enrollment and screening requirements from ACA. Our modular architecture is designed using a service oriented model with a variety of technical components to enable ease of use by offering web-based functionality to both Providers and internal users. We utilize role-based access; enable the secure storage, transport, and use of data adhering to HIPAA and NIST requirements; incorporate advanced tools that enable data sharing from a variety of sources using an open interface platform; and provide all data in a robust repository supported by a business intelligence software suite. The following table identifies the main architectural aspects of our solution, identifies the business problems solved by our architecture, and describes the benefits to DPHHS of each component.

	Business Problem	Benefits to the DPHHS
Web Interface	▪ Manual paper-based application receipt and processing. ▪ Access using desktop applications. ▪ Availability of functionality to all system users in an agnostic manner.	Our Provider Services solution couples a user-friendly Provider self-service web portal with operational workflows, automated communications, and advanced functionality all contained within an integrated web platform accessible via a web browser. This functionality will increase accessibility for Providers and reduce the amount of paper applications and manual processing required. The processing time of applications is vastly reduced allowing Providers the ability to enroll faster with less effort and constraints.
Modern System Design	▪ Lack of integration between business rules and workflow. ▪ Inability to scale and configure business applications to support new initiatives. ▪ Inability to share data using modern technology.	Our solution uses a service-based architecture, different application layers, and a set of modern tools to implement a loosely coupled modular application. This approach enables us to leverage system configurability to support on-going program changes and facilitate interoperability and data sharing with partner systems. The use of a rules engine and configurable workflows enables system updates to be made at lower risk and cost.

	Business Problem	Benefits to the DPHHS
Interoperability	▪ Support systems cannot efficiently or effectively share information ▪ Lack of real-time data to make decisions or include in business processes ▪ Time required to obtain and process data from partners	Legacy systems make it difficult to support system interoperability and data integration with other systems. Our Open Interface Framework will provide DPHHS with existing interface functionality "out-of-the-box," with the ability to easily configure any unique interfaces required for the Project. Our experience with connecting Provider Services Solution to legacy MMIS applications and modern systems allows us to cross-reference the data in our system to the key values needed by our trading partners. Our data integration approach allows us to receive and use screening source data as part of our screening methodology. This will lead to better Provider data and less fraud. With the introduction of service-oriented data exchanges, our solution enables seamless connectivity between the Provider Services solution and data partners including the MMIS for data integrity and real-time decision-making.
Data Storage	▪ Inability to store all Provider data in a single repository ▪ Lack of data query and reporting across all Provider data and business functions	The MAXIMUS Provider Services solution includes a consolidated data repository that houses all data and information produced during the Provider application, enrollment, certification, and licensing processes; the maintenance activities, as well as all related data generated by multiple State agencies and Trading Partners. MAXIMUS Provider Services solution has integrated business intelligence tool that will enable authorized users to access standard and ad hoc reporting across all data contained in the solution.
Flexibility	▪ Rigid business rules and workflows reduce productivity or program updates ▪ Inability of Providers to review their existing data leading to inaccurate information	The MAXIMUS Provider Services solution is based on a series of configurable business rules and workflows that move Provider applications through the enrollment, screening, and decision-making processes. These items are configurable and can be changed quickly and efficiently to align with Program needs. The flexibility in business rule and workflow definition aligns the system with program requirements, enables immediate support of new, and allows continual implementation of process. Based on our experience, we have found that Providers want the ability to review and update their information in real-time. Legacy MMIS systems do not facilitate the ability for Providers to review their information leading to inaccurate and outdated data. In addition, we have found that revalidation requirements are a key method of delivering accurate and updated Provider data. We are able to present Providers with their current data at any time so they can make changes leading to cleaner and more accurate Provider information and an easier and more effective revalidation process.

CONFIDENTIAL

	Business Problem	Benefits to the DPHHS
CMS 7 Compliant	▪ Compliant with CMS 7 Standards and Conditions for Enhanced Funding including interfacing with future MMIS implementations	Our solution follows the guiding principles of MITA 3.0 and is compliant with the CMS 7 Standards and Conditions for Enhanced Funding. We have proven our system can be implemented outside of traditional MMIS implementations in a modular fashion while acting as a functional conduit to support data integration and interoperability between legacy systems and Medicaid data partners. Our SOA and web services design allows for flexibility in interface technology, which enables the quick integration with any new MMIS implementations.

Application Tiers

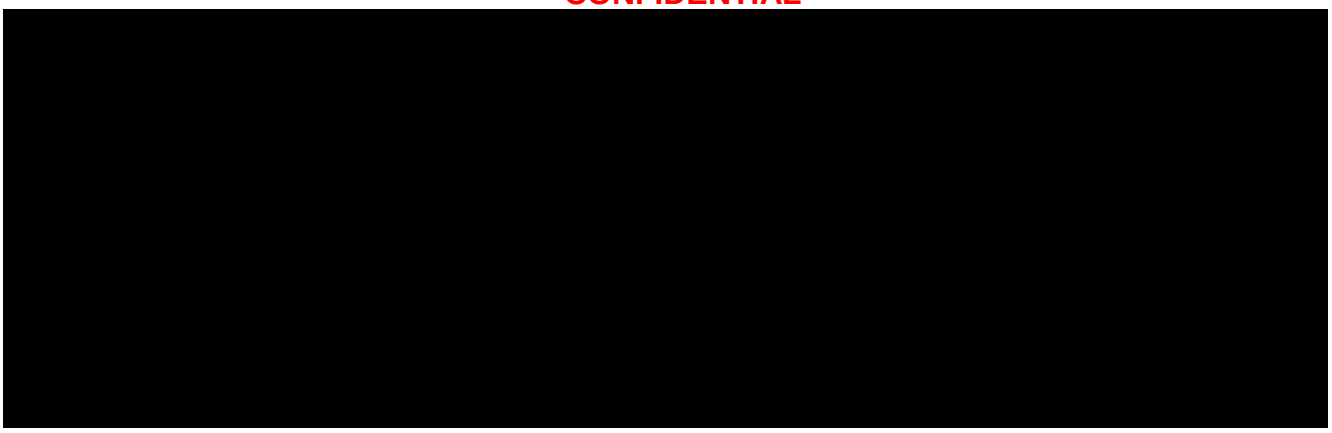
The MAXIMUS Provider Services solution business architecture is designed to deliver performance, scalability, and cost-effectiveness. Because our solution was specifically developed to operate outside of the traditional MMIS environment, we understand the need for the system to be configurable and flexible. The result is a fully functioning system built to use industry standard development and open source tools.

Our application website is built in ASP.NET, a widely used and highly scalable application framework. Our application uses caching wherever necessary for improved performance. MAXIMUS performs load testing as new features are introduced to verify system performance is not degraded. To bring further openness to our system, we have coupled the .NET platform with a number of third-party open source toolkits that add functionality and performance to the application. We use JQuery and AngularJS light-weight javascript frameworks to help make the website responsive. We also use BootStrap to make the website user friendly and to provide a consistent look and feel. These different frameworks allow the website to be browser agonistic. We use Content Delivery Networks for any web frameworks to allow all users in different locations to be served with faster page load times.

The MAXIMUS Provider Services solution is designed as a fully web-based application supported by an n-tier design that separates logical application components into processing layers and tiers, each of which contain specific functionality to manage various aspects of the Provider Services solution.

CONFIDENTIAL

CONFIDENTIAL



Together, the various tiers and layers of the application bring the set of business processes required to support Provider management activities. We have developed these business functions as separate functional components and applied them in a business layer that is accessible from the presentation layer, data layer and communication layer. Each of the business functions work independently while connecting to the other components of the system. The solution contains business workflows enabled through business service orchestrations. Work queues are created dynamically based on outstanding work items, the type of processing, and the user role. The workflows guide the users — both Providers and internal operations staff — through the tasks and activities necessary to complete required processes for completing applications, reviewing and screening Provider data, and receiving payments. We use business service orchestration to enable these workflows, and include external communication processes to allow automated reminders, notices and other documentation to flow electronically to Providers based on their actions in the system and the associated status of those actions. *Exhibit 3.1.10-1: MAXIMUS Provider Services Solution Application Architecture* provides a graphical depiction of the MAXIMUS Provider Services solution and the overall business architecture.

CONFIDENTIAL

System Configuration

The MAXIMUS Provider Services solution was implemented originally in Tennessee in 2011. Since that time, MAXIMUS has continued to upgrade the platform as we have implemented the system for different customers and made internal improvements and investments. Our solution core is flexible, adaptable, and stays in alignment with current technology products and trends. We began the initial projects using configurable reference tables, configuration files, and configurable execution parameters. This approach enabled MAXIMUS to provide a low-cost solution to our customers who were focused on value while meeting all of the MITA and CMS 0053even Standards and conditions.

With the advent of some of the new technology standards and the desire of states to acquire COTS products to support configuration and application extensibility, MAXIMUS began using a mixture of custom-built frameworks and COTS products. The solution includes a Business Process (workflow) engine to support provider services functions, a Business Rules engine hosted in Progress Corticon, an Enterprise Content Management (ECM) system based on Hyland OnBase and a Business Intelligence Software supported by MicroStrategy. These different products work in a loosely coupled manner to provide flexibility and extensibility to the Provider Services solution. While building the system architecture, we have taken into account future trends such as increasing network bandwidth and availability, increasing use of mobile devices, and continued improvement in hardware performance. In addition to these products, MAXIMUS is also implementing an external Correspondence Management platform supported by the Quadient Inspire ™ Platform. To support our client's desire for price flexibility, we can include or remove application extensions in scope and price. In this proposal, we have included all the products that support RFP requirements.

Business Process (Workflow) Engine

Our solution has a business process framework, which we refer to as the Business Process Engine, which enables execution and modification of process workflows. The Business Process Engine enables high-performance flexibility, and extensibility to the solution. The Business Process Engine has a process repository, a server-based process execution engine, monitoring, reporting and analytics. The Business Process Engine automatically executes the appropriate business process based on the inputs from the business rules engine. In addition, we are able to add steps in the workflow processes to enable communications with providers, provider reminders to providers and internal users, data integration processes and, when necessary, to pause a workflow until data or action triggers the continuation. The flexibility of our workflow engine enables our solution to be configured to support any state program regardless of size.

System Configurability

The MAXIMUS Provider Services solution architecture adheres to MITA principles by incorporating an industry standard business rules engine - Progress Corticon. The Rules engine enables business rules to be managed outside the application. MAXIMUS recognizes the need for separation of business rules from other parts of the application code and our architecture delivers this separation. Our solution has a variety of rules including workflow rules, document/notice generation rules, reference table rules, document upload rules, screening categories, Provider type rules, risk level setting policy rules and MMIS interface preprocessing/validation rules. These rules can be quickly changed within the rules engine as needed. The expanded features of the Corticon product enable what-if testing and supports testing of changes before they are implemented.

All of the rules in our Provider Services solution are configured to consume multiple parameters such as application type, Provider category type, Provider type, enrollment type (new, update, re-enrollment) to give maximum control to the policy expert. The rules engine factors the various parameters and, depending the context of the application, returns the appropriate results. One of the notable requirement changes in one of our implementations was to factor Provider specialties, in addition to the Provider types, when determining the risk level for a Waiver Provider. We were able to quickly modify the rules to include specialty as a Risk level parameter for the waiver Providers.

Information Architecture

The MAXIMUS Provider Services solution is packaged with an analytics and reporting platform. For reporting and analytics, we use two COTS products: Microsoft SQL Server Reporting Services (SSRS) and MicroStrategy. These two applications serve closely related purposes and play a very important role in Provider application processing. Our solution has system dashboards, standard reports, custom reports, ad hoc reports, and analytics.

Our solution is packaged with over 50 on-demand reports that provide detailed insights into application processing. All the reports in the system can be exported into several formats, including Excel, Word, PDF, and CSV. The reports are configured to have standard features such as totals, parameters that are used to execute the query and the date and time in which the query is executed. Our system reports use SSRS for real time data. All the reports are point in time reports and allow for several filtering parameters.

MicroStategy supports business intelligence and provides the analytics platform for state-approved staff to conduct analysis. Our solution is packaged with a variety of standard analytic reports. Based on our experience in different states, we know that most of the analytic reporting needs to be developed as we understand the specific needs of the State and the operations team involved.

Section 3.10.15–Reporting provides a detailed description of our reporting and analytics solution.

SOA and Shared Services

MAXIMUS Provider Services solution is a modular and flexible SOA-based solution supported by our Open Interface Framework that exposes application programming interfaces (API) to support data integration. In addition to delivering performance, scalability and cost effectiveness, the MAXIMUS approach to business architecture allows us to create SOA based services for a wide variety of application scenarios including provider data, business process information, business rule information, and authentication and authorization information. This allowed us to create shared services with other systems depending on the level and kind of integration needed. Our solution uses a service-based architecture, different application layers, and a set of modern tools to implement a loosely coupled modular application. Our solution has built in standardized service contracts to allow other applications to consume them.

The MAXIMUS Provider Services solution services are abstracted from implementation. This allows implementation to change but will keep the service contract and the clients that are using the contract from changing. Due to our extensible SOA principles, different components such as the user interface use the same services that are exposed to outside entities allowing for changes in implementation to occur seamlessly across system components and other systems that use our services. MAXIMUS creates SOA

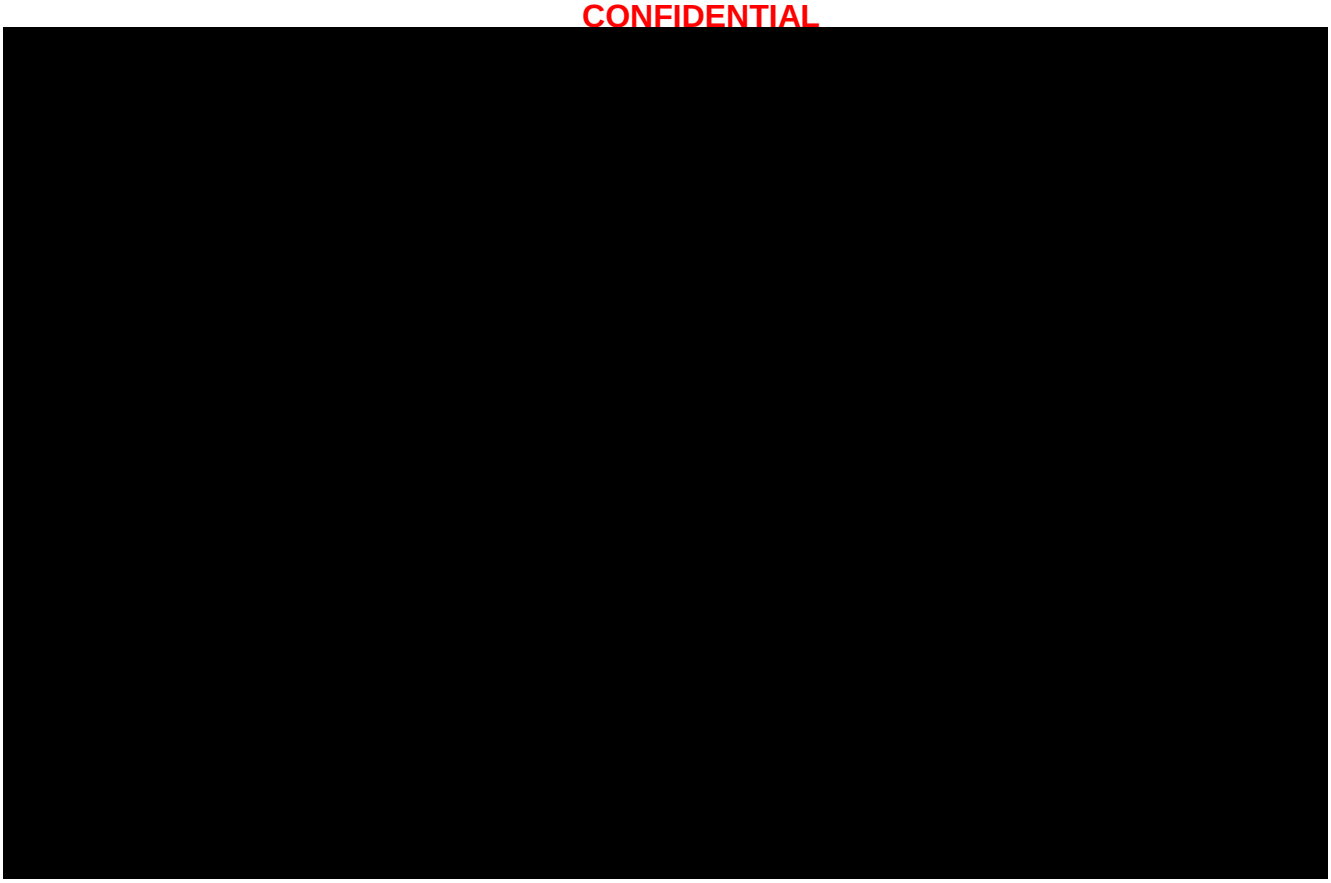
services as domain driven and use case based so they are relevant to the existing business processes and recognized by the user as a meaningful service.

The MAXIMUS Provider Services solution has a web services registry that documents the web services available, the service end points and the mechanism in which the services can be consumed. The Provider Services Solution web services registry is re-built automatically when a new service is added or when an existing service is modified. Our web service registry documentation is automatically published along with web service enabling the clients to consume the new services with ease. Our web service registry and the documentation can be made accessible to any third party.

MAXIMUS has delivered a SOA solution architecture that has integrated successfully with disparate applications that are running in their own platform specific environment because of SOA standards that we have introduced. The MAXIMUS Provider Services solution can be the single gateway for providers to get Medicaid enrolled, check patient eligibility, claim submission and claim statuses as well. This is becoming a reality in our Tennessee implementation as our provider services solution is the gateway for all provider specific functions. Also, because of our SOA model, our solution is able to act as the authentication provider for services that are exposed by other vendors.

By using Open Interface Framework, a core module of our SaaS offering, MAXIMUS will customize the existing MMIS and other interfaces as necessary to meet any unique requirements of the State. As a part of our Tennessee, Nebraska and District of Columbia implementations and our nineteen enrollment broker projects, we have implemented a variety of MMIS interfaces using both web services and flat files, and currently have automated interfaces with eight of the required verification data sources in Nebraska, Tennessee, and District of Columbia. As part of our solution, MAXIMUS will configure an interface with the existing MMIS and enable new interfaces with other State approved trading partners as required. Additionally, we will include all required verification databases in the solution and automate the interface method that is available. *Exhibit 3.10.1-2: MAXIMUS Provider Services Solution Interface Processing Approach* illustrates the external systems with which our solution will integrate and the flexibility we have in implementation options. The integration capabilities are further discussed in *Section 3.10.1.4– Integration.*

CONFIDENTIAL



3.10.1.1 Compliance

> 3.10.1.1 Compliance
>
> This section addresses compliance with state and federal statutes, policy, mandates as well as industry standards required for the Contractor's Scope of work. Offerors must describe how their solutions and operational approach meet each of the Compliance requirements detailed in Attachment F, Requirements Matrix.

Medicaid systems are governed by a variety of federal guidelines that define business processes, data requirements, technical standards, security and privacy considerations, and other operational performance metrics. CMS is continually looking at system and business process requirements within the Medicaid Program and making changes and improvements to key governing documentation such as the certification checklist, the MITA framework standards and items related to security and privacy. We understand that CMS has issued new standards and conditions that states must meet for Medicaid technology investments to be eligible for enhanced federal financial participation (FFP) and has updated the processes for how Medicaid systems are defined and certified.

For over six years, MAXIMUS has supported modular Medicaid Provider-facing solutions designed to operate outside of the MMIS. Our proposed project team members are already familiar with, and are experts in, existing documentation and federal requirements that govern the current and future designs of the modular MMIS implementation projects. We understand CMS' desire to use systems based on open standards and the need to look at what other states are doing to determine if components or technical artifacts can help our team build a better solution. We understand the broad array of technical requirements under which our solution must operate and be in compliance.

CONFIDENTIAL

MAXIMUS staff proactively monitor HHS, CMS and other applicable regulations that could potentially affect our provider services implementations. Additionally, MAXIMUS participates in "Community of Practice" and other national calls used by CMS to provide guidance and insight into the various programs. We understand the constantly changing landscape of Medicaid and are poised to respond quickly but thoughtfully to potential impacts on the system. These plans cannot be done in a vacuum and all approaches to implement changes must be done in collaboration with the State and its partners, particularly where changes affect an interface file. Following the established change management process as detailed in the change management plan is the vehicle for securing approval of any required changes.

Our solution is designed to follow the guiding principles of MITA 3.0 and is compliant with the CMS Seven Standards and Conditions for Enhanced Funding. We have proven our system can be implemented outside of traditional MMIS implementations while acting as a functional conduit to support data integration and interoperability between legacy systems and Medicaid data partners. Our Service Oriented Architecture and web services design allow for flexibility in interface technology, which will enable the quick implementation with any new MMIS systems.

We have created system security plans (SSPs) that adhere to recognized best practices including the latest version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series related to cyber security and have performed risk assessments that meet the NIST 800-30 requirements. We completed external penetration testing and, as a regular process, scan our software before any UAT or production release. As a regular component of our application development approach, MAXIMUS engages our corporate Office of Information Services (OIS) Security and Audit Team to secure our systems, infrastructure, and operational sites that conform to federal standards.

Our solution contains a variety of functions that address each of the Compliance requirements included in Attachment F. We closely protect data and develop automated mechanisms to purge and secure data when projects end. We will conduct project assessment and audits to validate we are adequately protecting all provider data and that we meet all requirements for securing protected information. Our staff is trained to never release information directly and any requests will be forwarded to our security office and the DPHHS for assessment.

MAXIMUS is committed to compliance with relevant federal and state statutory and regulatory requirements and takes civil rights and any complaints related to civil rights very seriously. As such, MAXIMUS established the corporate Compliance Program to promote ethical and lawful conduct, and compliance with applicable laws and regulations. We train all staff on our internal processes and procedures. This program applies to all MAXIMUS employees and its contractors and is mandatory for all employees annually. Complaints from both employees as well as the non-employees can be made to the MAXIMUS Ethics Hotline. The company investigates all complaints, writes findings reports, and takes appropriate follow-up. For this project, we will supplement this procedure to also report Civil Rights complaints no more than ten (10) calendar days after a complaint is received.

As a vendor providing Medicaid services for over 19 years, MAXIMUS has implemented corporate security, privacy and technology standards that govern how we implement, manage and maintain systems and data associated with all of our customer projects. MAXIMUS OIS and our Privacy Officer have implemented mandatory procedures for reporting issues or possible breaches in security of privacy and we will tailor each process to align with the specific service level agreements in the RFP and with state requirements. We are confident our solution adequately managers all of the Compliance requirements in

the RFP. During the DDI, we will assess each requirement to validate our implementation process keeps these items visible through ongoing compliance.

3.10.1.1.1 Compliance Requirements

The following table includes Attachment F–Compliance Requirements and our summarized response to each requirement.

ID	Compliance Requirement	MAXIMUS Summarized Response
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.	We develop a Turnover Plan at the end of the contract period in accordance with the State's timetable. Our Plan includes the transfer of all data and the destruction of information in our custody according to approved retainage plans. When transferred, the records and data are in a format agreed upon by the State.
CMP03	The Contractor shall notify the State in writing within five (5) business days following initial detection of suspected fraud or abuse and provide supporting documentation.	MAXIMUS shares the State's desire to combat fraud and abuse. Our solution is designed to maximize provider use of the web portal, minimize the potential for fraud and abuse, and achieve full compliance with all provider screening and enrollment regulations contained in 42 CFR Part 455 Subpart E. MAXIMUS workers may be notified of suspected fraud or abuse through automated interfaces with OIG, SAM and EPLS. If a positive result is returned, the system is updated with the result for a worker to review. If validated, these matches are moved through the solution workflow to the State queue for review where State employees can review the information and all supporting documentation. The application will appear in the State worker's queue and the State will be notified immediately through an email generated from the solution. If we have initial detection of fraud or abuse outside the system, we will notify the State in writing within five business days and will provide supporting documentation.
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.	MAXIMUS uses principles and MITA standards for all application development and maintenance. Our solution follows the guiding principles of MITA 3.0 and is compliant with the CMS 7 Standards and Conditions for Enhanced Funding. MAXIMUS will retain all data (including PII) as directed by DPHHS, understanding the data retention requirements might be longer for some data.
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).	Data is retained using methods that are compliant with current federal and State laws and regulations, including 45 CFR 164.316 and Administrative Rule 37.85.14. MAXIMUS will retain all data (including PII) as directed by DPHHS, understanding the data retention requirements might be longer for some data.
CMP06	The Contractor shall have written policies governing access to, and duplication and dissemination of all individual or entity information.	MAXIMUS defines specific roles for staff and the associated access to system data. During Project Initiation, we define processes and procedures that define how data must be handled. In system projects, we only share data with defined data partners using secure transport processes. Generally, our staff is not allowed to duplicate or disseminate any information what so ever. To support these processes, MAXIMUS has a comprehensive corporate training program that focuses on security and privacy and the potential for data breach. Every MAXIMUS employee is required to attend this HIPAA training at the time of hiring and annually thereafter. This training incorporates the MAXIMUS policy governing access to, duplication and dissemination of individual or entity information. In addition to Code of Conduct and Ethics Training, MAXIMUS includes a section on responsibilities and the need to maintain confidentiality of all data entrusted to MAXIMUS. Employees are required to pass a test that demonstrates their understanding of their responsibilities. Training dates and test scores are maintained in each employee's MAXIMUS University transcript.

ID	Compliance Requirement	MAXIMUS Summarized Response
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.	The MAXIMUS Provider Services solution web portal (which includes the Online Provider Directory) complies with State and Federal accessibility standards, guidelines related to electronic information resources. The solution currently deployed in the Tennessee, Nebraska, and District of Columbia is in full American Disability Act (ADA) Section 508 compliance, including accounting for the various forms of colorblindness. Checking for 508 compliance is embedded in the development process of the web portal, thus making it compliant for any new features that are introduced. During the DDI process, our training materials and any new functions will meet these requirements.
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.	MAXIMUS is knowledgeable of existing Federal statutes, rules, policies, and standards and has taken care to develop our solution in full compliance with these mandates. Similarly, we are familiar with the Montana Code Annotated, as well as the Administrative Rules of Montana (ARM) Title 37. Because we closely monitor and participate in CMS policy discussions, we are aware of upcoming changes to existing rules and regulations that may impact the scope of work. Our team will remain vigilant in detecting changes to existing rules and assessing any impacts to our system based on new updates.
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.	The MAXIMUS Provider Services solution is packaged with a built-in, robust security mechanism that complies with federal architecture guidelines and standards (including NIST) and incorporates the appropriate evolving national standards including HIPAA privacy and security requirements. As part of past project we have completed SSPs that adhere to recognized best practices including the latest version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series related to cyber security and have performed risk assessments that meet the NIST 800-30 requirements. Our corporate security officer will oversee compliance with all security standards.
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.	The MAXIMUS Provider Services solution supports architecture that adheres to MITA principles including the CMS Standards and Conditions and is designed to move Montana Medicaid to the next MITA maturity level. Our business team participates on several industry calls and boards, and we will align our solution with the required maturity for each process.
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.	The MAXIMUS Provider Services solution meets the Industry Standards Condition. All aspects of the MAXIMUS Provider Services solution meet Medicaid requirements for interoperability, data exchange, security, and confidentiality. It addresses federal architecture guidelines and standards and incorporates the appropriate national standards including HIPAA privacy and security requirements and technological guidelines as defined by the Health Information for Economic and Clinical Health (HITECH) Act. Access control and associated policies, procedures, initiatives, security assessments, and technical security controls are based on compliance with the HIPAA Security and Privacy Rule and associated security control framework. During the implementation project, we will work closely with the State to maintain the right focus on how we implement the various business processes.

ID	Compliance Requirement	MAXIMUS Summarized Response
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.	The MAXIMUS Provider Services solution meets the Leverage Condition in that it is available for re-use in other states as a transfer system. We expect to bring our system with the District of Columbia configuring as a starting point for Montana. However, we are already planning to implement specific configuration for Tennessee and Nebraska to support specific items. In addition, our solution is flexible to meet the unique requirements of Montana. Montana will be able to leverage much of the existing system with minimal customization.
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.	The MAXIMUS Provider Services solution meets the Business Results Condition in that it effectively and efficiently screens, enrolls, and communicates with providers. Our solution uses highly automated processes to accept and route applications according to pre-defined business needs. Notices to providers are sent by email. We incorporate automated messages, notices, and correspondence based on workflow items. The web chat feature further supports communications. Providers can return to the portal to check the status of their applications and receive email notifications if anything is missing that prevents the application from being processed.
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.	The MAXIMUS Provider Services solution meets the Interoperability Condition in its demonstrated ability to interface with multiple state's MMIS systems. Our solution's Open Interface Framework allows us to import external Provider data from any source, including State MCOs and Credentialing agencies. Regardless of the source of the Provider's data, our solution contains a normalized data model that allows us to present Provider information to end users and stakeholders in a consistent, straightforward manner. We currently support a wide variety of data integrations including web services using an ESB, XML format using flat files, SFTP flat file exchanges and where we share a common domain, trigger tables to initiate data sharing.
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.	We have proven our system can be implemented outside of traditional MMIS implementations in a modular fashion while acting as a functional conduit to support data integration and interoperability between legacy systems and Medicaid data partners. The MAXIMUS Provider Services solution meets the Modularity standard in that the architectural foundation is based on the MITA maturity model and we utilize open standards to support data exchange with any partner. The business processes are optimized and flexible and standard business models focus on streamlining administration of the program. The data driven framework supports flexible business rules and configuration. Our SOA and web services API design allows for flexibility in interface technology, which enables the quick integration with any new MMIS implementations. The MAXIMUS Provider Services solution has a business rules engine and workflows based on business rules that move Provider applications through the enrollment, screening and decision-making processes. Our business rules engine rules are machine and human readable and thus are configurable so they can be changed quickly and efficiently to align with Program needs. The flexibility in business rule and workflow definition aligns the system with program requirements, enables new initiatives to be supported immediately, and allows process improvements to be continually implemented.
CMP17	The Contractor must provide the Department with compliance assurances for the Contractor scope of work.	MAXIMUS provides full assurance and pledges to maintain compliance with federal and state statutory, regulatory, policy guidance and all applicable standards relative to the scope of work within this contract.

ID	Compliance Requirement	MAXIMUS Summarized Response
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.	HIPAA security and privacy compliance is a core component of our approach for Montana. As a major state and federal vendor, MAXIMUS is required to comply with HIPAA across the majority of our health and human services projects. MAXIMUS designed all aspects of our solution to meet Medicaid requirements for interoperability, data exchange, security, and confidentiality. We are also fully compliant with Administrative Simplification and have automated most processes to eliminate the need for paper and shortened processing times.
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.	MAXIMUS and our subcontractor, Microassist, agree to enter into a Business Associate Agreement (BAA) prior to the initiation of work. The BAA is subject to HIPAA, HITECH and corresponding regulations. MAXIMUS understands the responsibility for security and privacy compliance and employ the requisite policies and procedures required to prevent unlawful access by any person who may have access to the entire database. We currently have similar agreements in place with all three customers using our solution.
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.	We specifically address the security and privacy requirement for PHI and PII in our SSP. To support the extensive data integration functionality contained in our solution we have developed and implemented security controls that meet HIPAA and NIST standards. In addition, we implement corporate policies for handling protected information and reporting potential breach. We have designated security and privacy officials for this project and a defined process for reporting any issues to the State. Even data not specifically identified as PII or PHI is treated as privileged communications and will meet the terms and conditions specified in the RFP, BAA, and Contract.
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.	Only those employees with a specific need-to-know are granted access to personal information. Information is disclosed only to parties who are legally entitled to that information and as a rule we do not permit project staff to disclose any information. In the event a business need arises requiring information disclosure, we will disclose only after obtaining prior written consent from the State.
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.	The MAXIMUS Provider Services solution is packaged with a built-in, robust security mechanism that complies with federal architecture guidelines and standards (including NIST) and incorporates the appropriate evolving national standards including HIPAA privacy and security requirements. To control security across the multiple application tiers and numerous data interface components, our solution contains a variety of security layers to protect the application and its data.
CMP23	The Contractor's data management approach and operational policies shall meet HIPAA, HITECH, ARRA and other federal and State privacy and security requirements.	Data management, access control and associated operational policies, procedures, initiatives, security assessments, and technical security controls are based on compliance with the HIPAA Security and Privacy Rule, HITECH and ARRA, as well as associated security control framework. Access to MAXIMUS applications, data, and computer resources is managed through user account IDs and passwords that are unique to each user, as well as user privilege restriction mechanisms.

ID	Compliance Requirement	MAXIMUS Summarized Response
CMP24	"The Contractor's solution shall be compatible with multiple standard browsers in accordance to the State's IT Standards which can be found in the Procurement Library. The solution shall allow access from standard browsers without requiring specialized plug-ins or applets to function.	The website is hosted on the IIS web server and is accessible via standard web browsers. We use JQuery and AngularJS light-weight javascript frameworks to help make the website responsive. We also use BootStrap to make the website user friendly and to provide a consistent look and feel. These frameworks allow the website to be browser agonistic. We follow a methodical and high impact approach to cross browser testing and high-risk browser testing for browsers that are used by 95 percent of the United States Chrome, IE, Safari, Firefox, and Opera.
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.	Our solution contains document upload functions that do not require the receipt of paper. Providers and internal users upload documents directly in the system which them automatically propagates the document to our OnBase document repository. Under the base services, we do not envision receiving any paper as part of the application maintenance; however, during project initiation, we will create a process to deliver complete compliance with the retainage schedule and identify the potential areas where this might occur. Our solution does enable providers to submit paper documents.
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.	The MAXIMUS Provider Services solution contains an automated and complete electronic audit trail(s) of all changes made in the Provider Enrollment Master File and tables, including identifying the date and timestamp and user or process responsible for the update. It is a consolidated repository consisting of data from the solution workflow engine, rules engine and reporting framework that contains sophisticated auditing capabilities that track every change made to system data. The application will use access/audit logs at web, application, and database servers for auditing purposes consistent with GAAP and GAAS procedures and practices.
CMP27	The Contractor will ensure that all technologies implemented are in compliance with any End User Licensing Agreements or other licensing arrangements.	Implementation of our solution is done in full compliance with any End User Licensing Agreements or other licensing arrangements. This is a corporate standard for which our compliance team confirms we meet.
CMP29	The Contractor shall comply with Affordable Care Act Section 1104 Administrative Simplification, and Section 1561 Health IT Enrollment Standards and Protocols.	The MAXIMUS Provider Services solution is compliant with the applicable recommendations of Section 1561, including verification interfaces, business rules, and privacy and security. Our solution is compliant with the Administrative Simplification provisions and operating rules of Section 1104 of the ACA.
CMP30	The Contractor's solution shall ensure that all data necessary for legal requirements is retained.	After implementation of each module, seven (7) years of electronically imaged documents and data will be kept in that module. After seven (7) years, the data will be purged (deleted) from that module. All active records (active providers, 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.
CMP32	The Contractor shall provide a mechanism to purge source documents in accordance with HIPAA security provisions and State requirements.	Adhering to State and federal HIPAA information security standards, the MAXIMUS Provider Services solution is capable of purging all State data from our solution and backups when the State has confirmed in writing the receipt and usability of all data. Our solution has features to make documents obsolete to confirm to document retention policies and is integrated into our ECM component. Our solution's ECM component also has Records Management module to support the special access control, disposition, and retention needs for declared records throughout their entire life cycle.

3.10.1.2 Security

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.

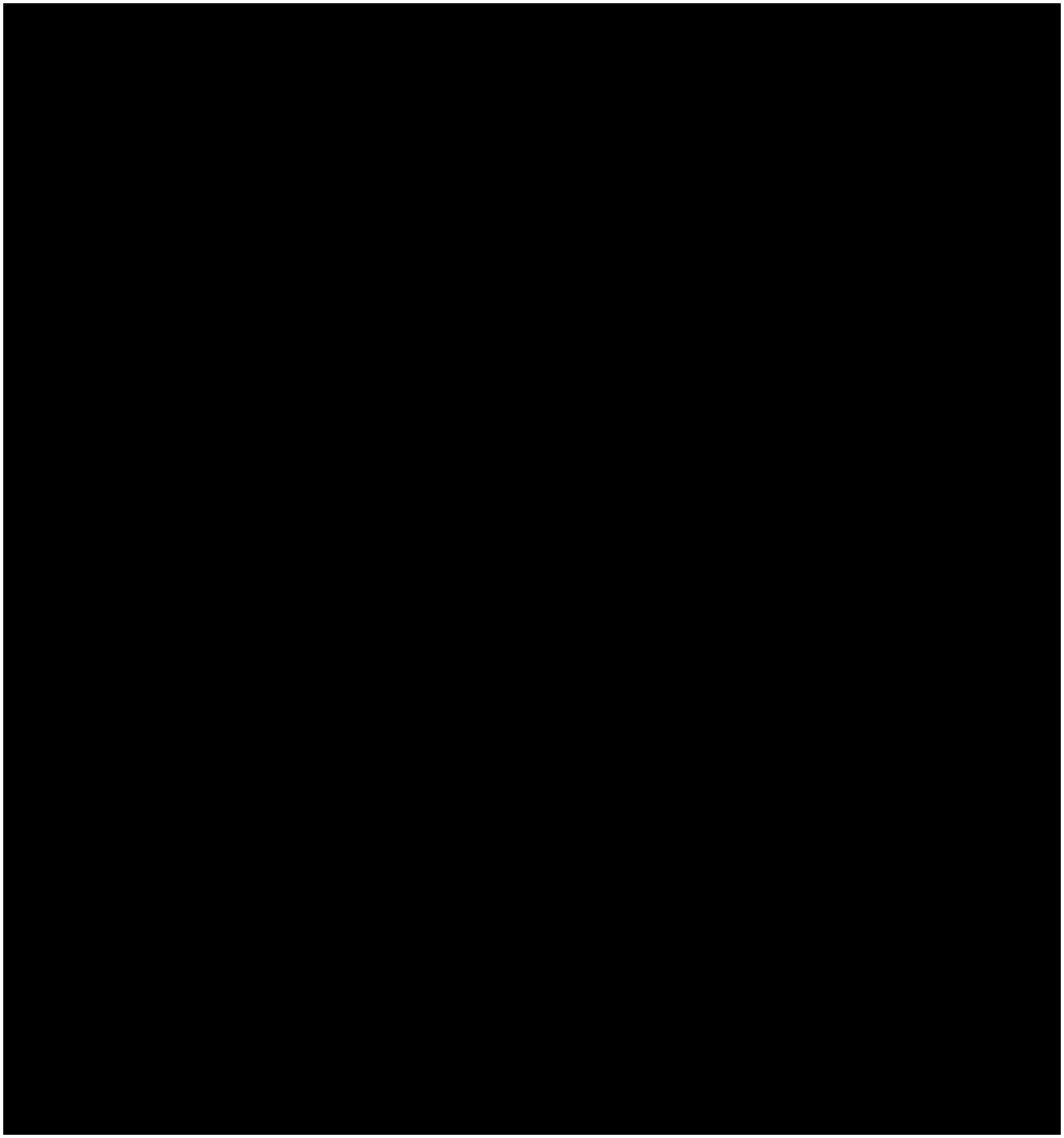
MAXIMUS understands the need to secure system data with no loss of confidentiality, integrity, or availability occurs. Security is treated as an integrated component of our solution and covers the application, hosting environments and our operations call and support centers. MAXIMUS has a corporate Office of Information Security (OIS) who's responsible for our projects meeting applicable security standards. For projects like the Provider Services module implementation, they are actively engaged beginning with proposal development and continues throughout the implementation and operations aspects of the project. Our integrated security approach takes into account security at each solution component. Due to the strict security requirements for this project and the specific audit and service level requirements, we have assigned a full-time security analyst to support this project and coordinate security activities with the various teams that will be integrating components of the solution.

We explain the different components of our solution in the sections below.

3.10.1.2.1 Security Architecture

The MAXIMUS Provider Services solution is packaged with a built-in, robust security mechanism that complies with federal architecture guidelines and standards (including NIST) and incorporates the appropriate evolving national standards including HIPAA privacy and security requirements. To control security across the multiple application tiers and numerous data interface components, our solution contains a variety of security layers to protect the application and its data. *Exhibit 3.10.1.2-1: MAXIMUS Provider Services Solution Security Architecture* demonstrates the system's high-level security architecture and addresses key areas of potential vulnerability. This architecture provides a framework in which MAXIMUS can work with DPHHS to verify our solution meets the applicable security policies and standards.

CONFIDENTIAL



Maintenance of user accounts, particularly disabling the accounts of terminated employees, is a key strategy to prevent possible data or systems access by unauthorized individuals. Our corporate Human Capital department issues a list of employee separations daily. This list is distributed to appropriate personnel responsible for disabling user accounts on various email, systems, file servers, network equipment, building access, data center access, and other applicable access control lists.

From a project perspective, the MAXIMUS Help Desk staff will be assigned the responsibility for terminating providers or operations staff. We will work with DPHHS to create a process and policy for providing this information between the teams in an efficient manner so no security issues are encountered.

CONFIDENTIAL

CONFIDENTIAL

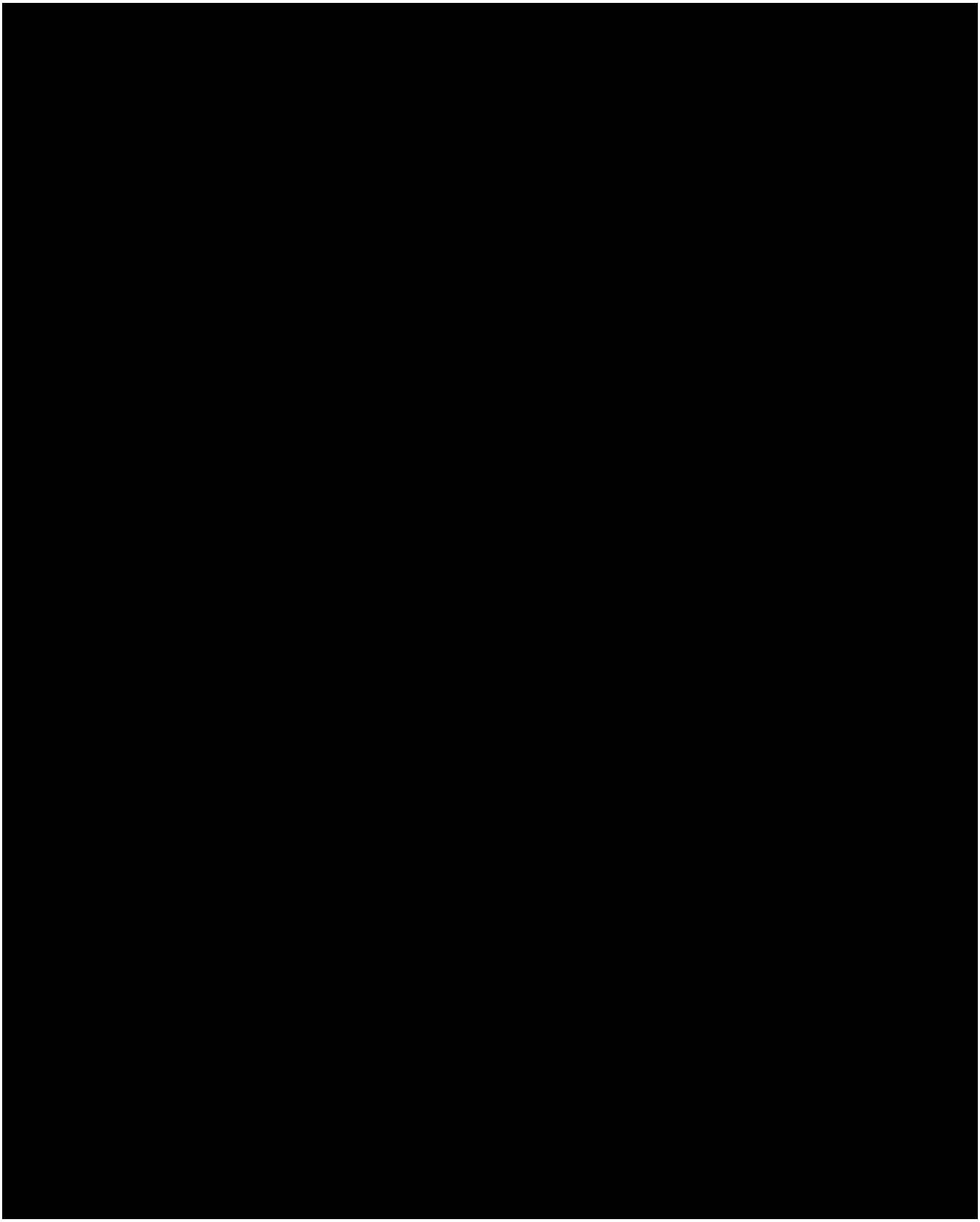
Requests for new user IDs and changed privileges must be in writing and approved by the user's manager before a systems administrator fulfills these requests. Other key user-based security measures include the following procedures:

- Users are instructed to choose complex passwords. So that a compromised password is not misused on a long-term basis, passwords must be changed at least every 90 days or at more frequent intervals for certain systems or per specific contract requirements
- User accounts are automatically locked and disabled after three unsuccessful login attempts, requiring a systems administrator to review the account and unlock it or reset the password, as appropriate

When users log on to our systems, they receive a visual reminder in the form of a "splash screen" or banner page, which reminds them of authorized use policies governing their access. We will work with DPHHS to place an appropriate security policy on the Provider Services solution login page.

CONFIDENTIAL

CONFIDENTIAL



CONFIDENTIAL

CONFIDENTIAL

[redacted]

3.10.1.2.2User Access Security

MAXIMUS is aware of the DPHHS's role-based security requirements. Our flexible role-based security modules can accommodate different types of configuration for teams and partner access to the system. MAXIMUS developed our solution with direct connections to the MMIS and data validation sources to support enrollment and screening. To support the extensive data integration functionality contained in the MAXIMUS solution and meet MMIS security and privacy guidelines, MAXIMUS designed the system to include specific security requirements included in the federal regulations and to meet industry standards and best practices.

Because the application includes an externally facing Internet component, we engaged our Corporate Enterprise Security and Risk Management group to help define the specific security requirements. We also continually conduct internal vulnerability assessments of the application. In our Tennessee installation, we conduct full third-party vulnerability and penetration tests of the application on a yearly basis, correct any identified defects, and add them to lessons learned.

To access the MAXIMUS Provider Services solution a user must have a valid use account with a unique ID. Providers are able to sign up for a user account using online functionality that requires specific data validation. The email address is also verified as part of this process. Providers are able to complete applications and revalidations or update their information. However, they are not able to see any internal information about their record.

Internal users are assigned an account with an associated role. Our flexible role-based security model accommodates different types of configuration for teams and partner access to the system. Our solution comes with pre-defined roles. For example, the operator role can review and screen the application while the site-operator can only perform site visits. In addition to that, our solution provides the ability to grant authorization through role-based security (create, delete, modify and view) access to user interfaces, reports, data elements/field level, menu items, etc. Our solution allows authorized users to create groups and roles and provide access to the groups. Tasks in the workflow can be associated to a group or role and they are automatically assigned to the respective group as the application moves through the workflow. *Exhibit 3.10.1.2-3: MAXIMUS Provider Services Solution User Management* shows an administrative function that enables a system administrator role to control what aspects of an application a user can view.

CONFIDENTIAL

CONFIDENTIAL

All user account passwords are stored as hash values to prevent compromise. User passwords have a configurable expiration time. Password strength is configured to force the users to select strong passwords that are more complex. User access to the MAXIMUS Provider Services solution system is based upon security roles. Security roles are based on business function and necessary access to information. Individual Providers can only access their own information, while operations staff has broader access to information based on their position requirements. An administrator role is also available with broader access across multiple functional areas, including security administration. MAXIMUS will verify the roles needed for State authorized staff and Providers during the onset of the Project.

Our solution also provides single sign-on capabilities. This is done in our Tennessee implementation by providing authentication capabilities to services hosted by State-approved trading partners who provide CAQH CORE services to Providers. In addition to accessing CAQH CORE requirements available through the web portal, the Provider systems consumes CAQH CORE services using the Authentication

CONFIDENTIAL

web service hosted in our solution. The solution also has the necessary infrastructure and capabilities to be a consumer of Kerberos, LDAP authentication, SAML and other SSO technologies.

MAXIMUS provides different environments for integration/system testing, training and user acceptance testing (UAT). We will work with DPHHS to define the user access to these environments. The MAXIMUS Provider Services solution has a user administration module that allows administrators to search for users based on name, NPI, Medicaid Id and user role. The MAXIMUS Provider Services solution allows the administrator to activate, de-activate, add, reset user password, and to verify security questions to reset a user's password. The MAXIMUS solution can provide state authorized users the functionality to perform such activities in various environments as needed.

Our solution's audit trail information includes information such as date and time of operation, type of operation (Insert, Update, and Delete), and user ID along with the affected data elements. This auditing model tracks all user activity and stores all of the details in the audit tables.

3.10.1.2.3System Security Plan

As a leading government contractor operating health and human services projects, MAXIMUS has a strong understanding of information security requirements and associated privacy and confidentiality laws and regulations. We have a comprehensive approach to security for each of our contracts and a long history of understanding the implementation of security policies covering physical, system, and personnel security protocols. Through the many contracts we operate for both federal and state government agencies, we have deep experience complying with applicable standards, policies, laws, and regulations. Our best practices incorporate adequate security in the information systems we provide for our clients.

Our solution will be hosted in the Amazon AWS cloud. We manage numerous systems and applications within the cloud that handle sensitive and confidential records for health and human services endeavors including Personal Identification Information (PII) and Personal Health Information (PHI). Because we interact with these protected data, we have implemented a comprehensive security approach that safeguards mission-critical and confidential data from alteration, loss, theft, destruction, and breach of confidentiality, and meets federal and state guidelines for security, confidentiality, and auditing, including HIPAA and FISMA. The security approach of each of our Provider-facing projects is customized based on the type of data that is being collected, stored, transferred, or acted on.

The MAXIMUS Office of Information Services (OIS) Security and Audit Team is responsible for data security. This group's role includes system security administration, security assessments, and reviews to safeguard corporate data assets. The Team continuously evaluates and assesses our capabilities and requirements to secure client data entrusted to MAXIMUS.

As a part of the implementation of our Provider Services Solution, MAXIMUS will complete a System Security Plan (SSP). We use the National Institute of Science and Technology (NIST) methodology for developing Security Plans, as detailed in NIST SP 800-53 Rev 4 Guide for Developing Security Plans for Information Technology Systems. Our Information Security Policy, maintained by our corporate OIS Security and Audit Team, defines the requirements pertaining to physical and information security, as well as authorized use. We have an extensive program that includes employee training, continuing education, specific situational alerts, and auditing to completely maintain all appropriate security

protocols. Our application, hosting, and operations components will meet the security requirements defined in our plan, and we will provide annual audits and updates as necessary.

3.10.1.2.4HIPAA Security and Privacy Compliance

HIPAA security and privacy compliance is a core component of our approach for the DPHHS. As a major state and federal vendor, MAXIMUS is required to comply with HIPAA across the majority of our health and human services projects. MAXIMUS designed all aspects of our solution to meet Medicaid requirements for interoperability, data exchange, security, and confidentiality. Our solution addresses federal architecture guidelines and standards and incorporates the appropriate national standards including HIPAA privacy and security requirements and technological guidelines as defined by the Health Information for Economic and Clinical Health (HITECH) Act. Our security and privacy practices allow us to:

- Reinforce the ability to safeguard people, assets, and information through well-integrated, standard policies and processes
- Strengthen protection while improving system responsiveness
- Develop and implement action plans to confirm awareness of and compliance with standards and protocols

Access control and associated policies, procedures, initiatives, security assessments, and technical security controls are based on compliance with the HIPAA Security and Privacy Rule and associated security control framework shown in *Exhibit 3.10.1.2-4: MAXIMUS Security Control Framework.*

Security Control Framework—Health Insurance Portability and Accountability Act (HIPAA)	
Security Management Process	Implement policies and procedures to prevent, detect, contain, and correct security violations. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (PHI) held by the covered entity.
Assigned Security Responsibility	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity
Workforce Security	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information (ePHI), as specified in the associated HIPAA Security Rule, and to prevent those workforce members who should not have access to PHI from obtaining access
Information Access Management	Implement policies and procedures for authorizing access to PHI that are consistent with the applicable requirements of the HIPAA Security Rule
Security Awareness	Implement security awareness and training programs for all members of the workforce (including management)
Security Incident	Implement policies and procedures to address security incidents. Develop and deploy an incident response team or other reasonable and appropriate response mechanism. Incorporate post-incident analysis into updates and revisions
Contingent Plan	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain PHI

Security Control Framework—Health Insurance Portability and Accountability Act (HIPAA)	
Evaluation	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under the HIPAA Security Rule and subsequently in response to environmental or operational changes affecting the security of PHI that establishes the extent to which an entity's security policies and procedures meet the requirements of the HIPAA Security Rule
Business Associate Contracts and Other Arrangements	A covered entity, in accordance with Section 164.306 of the HIPAA Security Rule, may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Section 164.314(a) of the HIPAA Security Rule, that the business associate will appropriately safeguard the information
Facility Access Controls	Implement policies, procedures, and technical controls to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed
Workstation Use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access PHI
Device and Media Control	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility
Workstation Security	Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users
Access Control	Implement technical policies and procedures for electronic information systems that maintain PHI information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a) of the HIPAA Security Rule
Audit Control	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI
Integrity	Implement policies and procedures to protect PHI from improper alteration or destruction
Person or Entity Authentication	Implement procedures to verify that a person or entity seeking access to PHI is who they claim to be
Transmission Security	Implement technical security measures to guard against unauthorized access to PHI that is being transmitted over an electronic communications network

Exhibit 3.10.1.2-4: MAXIMUS Security Control Framework. *The HIPAA security framework specifically focused on the safeguarding of electronic protected health information (ePHI).*

The MAXIMUS Security Control Framework formalizes the processes and procedures to be followed to secure protected information. It covers all access aspects of the project and implements repeatable processes that are followed on all of our health and human services projects. It also aligns with our corporate security standards, and is supported by the MAXIMUS Office of Information Services (OIS) Security and Audit Team, which implements, follows, and audits appropriate policies for compliance.

We enlist protective measures and safeguards to confirm that data and other related information, including data residing in our systems and work sites remain secure, highly confidential, and in compliance with federal HIPAA requirements and any other applicable state or federal laws or regulations. Specifically, we will capitalize on three main principles regarding data confidentiality and HIPAA compliance:

- Secure data in transport

- Secure access to data
- Secure data in storage

MAXIMUS secures data in storage and limits access to our sites through a combination of sound electronic and physical security measures. We employ strong electronic protections at our corporate data center, all company offices, and customer support centers. Badge access requirements are mandatory, electronic access controls are in place, and multiple levels of access are present to control who has access to information and to limit the access based on job assignment and role. We bring a history of successful Medicaid operations, all of which meet HIPAA security requirements.

MAXIMUS acknowledges our responsibility to execute the required agreements upon contract award:

- HITECH Business Associate Agreement
- HITECH Scope of Work
- Trading Partner Agreement
- Ownership/Controlling Interest and Conviction Disclosure form

3.10.1.2.5 Security Auditing

MAXIMUS currently manages numerous systems and applications that handle sensitive and confidential records for health and human services endeavors including Personal Identification Information (PII) and Personal Health Information (PHI). Because we interact with these protected data, we have implemented a comprehensive security approach that safeguards mission-critical and confidential data from alteration, loss, theft, destruction, and breach of confidentiality, and meets Federal and State guidelines for security, confidentiality, and auditing, including HIPAA and FISMA. Each of our Provider-facing projects fall under our security approaches that are customized based on the type of data that is being collected, stored, transferred, or acted on.

The MAXIMUS Office of Information Services (OIS) Security and Audit Team is responsible for data security. This group's role includes not only system security administration, but also security assessments and reviews to verify and validate the safeguarding of corporate data assets. The Team continuously evaluates and assesses our capabilities and requirements to safeguard the security of client data entrusted to MAXIMUS and works directly with project teams to identify, report and investigate security incidents. In the event of a security incident, we will immediately report incidents upon discovery, including breaches, to State-designated personnel. Our team will conduct a full investigation and submit a root cause analysis and Corrective Action Plan to the State within five (5) business days of the incident. We will be available to meet and confer with the State as requested.

In addition to regular responsibilities, the MAXIMUS OIS team will also coordinate the service organization control (SOC) 1 Type II audit that will be completed annually. In addition to this audit, MAXIMUS will also complete a Security Audit Report with results to the Department by the 30th (thirtieth) of September each year. The Security Audit Report will include a NIST 800-53 rev 4 assessment at a "moderate" system risk control level. All deficiencies identified in the report will be corrected within forty calendar days of the submission.

CONFIDENTIAL

3.10.1.2.6 Security Requirements

The following table includes Attachment F Security Requirements, our summarized response to each requirement, and the section(s) in our proposal in which we provide our detailed response.

ID	Security Requirement	MAXIMUS Summarized Response
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.	Our solution contains security at various physical and system levels. We provide secure facilities for our staff and systems with controlled access, we safeguard our networks using a variety of high-technology products and firewalls and protect our systems and data using encryption technology and role-based security. To access the MAXIMUS Provider Services solution a user must have a valid user account with a unique ID. Each log in ID is tied to a specific role and that governs what data can be accessed. To begin any sessions, the user ID and permissions for the role must be validated. Functions that are not available to a role cannot be executed and data set access can be controlled based on authentication.
SEC02	The Contractor shall ensure that any data being transmitted or transported either physically or electronically will be encrypted.	[redacted]
SEC03	The Contractor shall ensure that any unneeded hardware, software, and licenses have been decommissioned.	MAXIMUS is proposing to host our environments on the AWS Cloud. We are utilizing an approach that only engages the environments necessary. However, our decommissioning policy is defined by our IT Infrastructure / Security team. AWS provides various options for decommissioning such as those detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization").
SEC04	The Contractor shall protect all government data from loss or unauthorized disclosure.	To control security across the multiple application tiers and numerous data interface components, our solution contains a variety of security layers to protect the application and its data. The security contained in our solution was architected by a joint team of government and commercial healthcare professionals to meet interoperability, data exchange, security, and confidentiality requirements defined by CMS. See the *Section 3.10.1.2.3– System Architecture*.
SEC05	The Contractor's solution shall streamline electronic transactions by incorporating electronic and digital signatures compliant with HIPAA and other State and federal statutes.	Our solution has an electronic signature function, compliant with HIPAA and other State and federal statutes that providers utilize before they submit their applications or data changes. While we do not anticipate using it for this project, our solution's ECM component has an integration with DocuSign for electronic and digital signatures.
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]

CONFIDENTIAL

CONFIDENTIAL

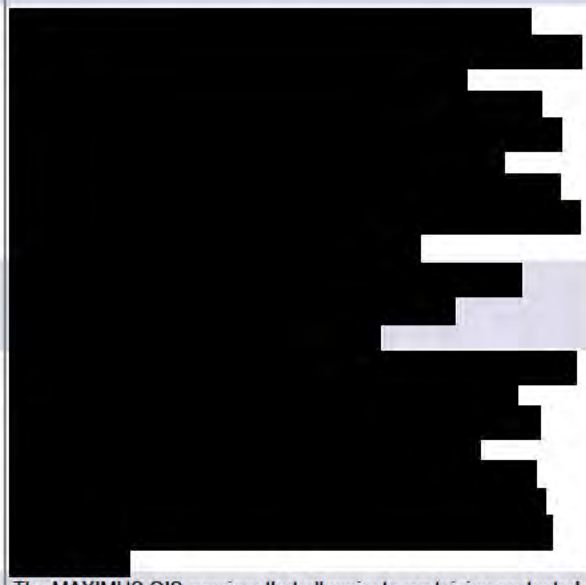
ID	Security Requirement	MAXIMUS Summarized Response
SEC07	The Contractor's solution shall automatically maintain an audit trail of users, including database administrators, who pass through or view a record, regardless of whether data is changed.	[redacted]
SEC08	The Contractor's solution shall have security audit trail reporting capabilities (e.g. security, level, locale, IP address, user ID, before and after changes).	
SEC09	The Contractor's solution shall ensure the audit trail that cannot be modified.	
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.	MAXIMUS designed all aspects of our solution to meet Medicaid requirements for interoperability, data exchange, security, and confidentiality. Our solution addresses federal architecture and guidelines and standards, including but not limited to auditing standards and incorporates the appropriate national standards including HIPAA privacy and security requirements and technological guidelines as defined by the Health Information for Economic and Clinical Health (HITECH) Act. For additional information, see *Section 3.10.1.2.4–HIPAA Security and Privacy Compliance*.
SEC11	The Contractor shall perform risk assessments per the Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach NIST SP 800-53 Rev 4. Risk assessments shall be completed on an annual basis and when additions or changes to functionality impact the security framework, architecture or when a new vulnerability exists.	As part of the development of our SSP, MAXIMUS will perform risk assessments that meet the NIST SP 800-53 Rev 4 requirements. As a standard component of our application development approach, MAXIMUS engages our Office of Information Services (OIS) Security and Audit Team to secure our systems, infrastructure, and operational sites. As described in *Section 3.10.1.2.3–System Security Plan*, we use the National Institute of Science and Technology (NIST) methodology for developing Security Plans, as detailed in NIST Special Publication 800-53 Rev 4, Guide for Developing Security Plans for Information Technology Systems.
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.	Our modular architecture is designed using a service oriented model with a variety of technical components to enable ease of use by bringing web-based functionality to both Providers and internal users utilizing role-based access; enabling the secure storage, transport, and use of data adhering to HIPAA and NIST compliant identification, authentication and accounting. During DDI we will create a System Security Plan that will detail the controls our system utilizes and how they meet NIST standards.

CONFIDENTIAL

ID	Security Requirement	MAXIMUS Summarized Response
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.	The MAXIMUS Provider Services solution contains security at various physical and system levels. We provide secure facilities for our staff and systems with controlled access, we safeguard our networks using a variety of high-technology products and firewalls and protect our systems and data using encryption technology and role-based security. MAXIMUS secures data in storage and limits access to our sites through a combination of sound electronic and physical security measures. We employ strong electronic protections at our corporate data center, all company offices, and customer support centers. Badge access requirements are mandatory, electronic access controls are in place, and multiple levels of access are present to control who has access to information and to limit the access based on job assignment and role. We bring a history of successful Medicaid operations, all of which meet HIPAA security requirements.
SEC04	The Contractor shall protect all government data from loss or unauthorized disclosure.	To control security across the multiple application tiers and numerous data interface components, our solution contains a variety of security layers to protect the application and its data. [redacted] The security contained in our system was architected by a joint team of government and commercial healthcare professionals to meet interoperability, data exchange, security, and confidentiality requirements defined by CMS.
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.	We conduct full third-party vulnerability and penetration tests of the application on a yearly basis, correct identified defects, and add them to lessons learned. We also provide Test Report results to our clients and work with them on a plan to address the vulnerabilities. MAXIMUS will perform a penetration test six months prior to go give and annually or when major system changes have occurred. We will utilize an industry standard third party to conduct the testing.
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.	Our solution provides a high availability infrastructure designed to meet the uptime as well as disaster recovery requirements. Our solution is architected in compliance with HIPAA and is deployed on AWS infrastructure. To meet the hosting requirements, our solution has a high availability redundant primary site supported by a high availability replicated disaster recovery site that mirrors the configuration of the primary site. We use different AWS zones so a disaster does not impact both sites, and use the same security scheme and configurations across the environments.
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.	The MAXIMUS OIS has developed and maintains detailed security and privacy procedures for all component of system and physical security. Every employee in the company must adhere to these standards. The Montana Provider Services Solution project has a full time security resource assigned to confirm we cover each aspect of security required for the project and that all project staff and company personnel follow the processes and procedures.
SEC18	The Contractor shall maintain adequate technical support/staffing to provide 24x7x365 coverage.	The MAXIMUS IT support team is available 24x7x365 to maintain adequate technical support/staffing to provide coverage. We use a mixture of automated tools and support staff to monitor our environments and make adjusts as required.

ID	Security Requirement	MAXIMUS Summarized Response
SEC19	The Contractor's data encryption solution shall meet Federal Information Processing Standard (FIPS) 140-2 and at a minimum use AES 128 encryption.	Our solution contains security at various physical and system levels. We provide secure facilities for our staff and systems with controlled access, we safeguard our networks using a variety of high-technology products and firewalls and protect our systems and data using encryption technology and role-based security to meet federal and state guidelines for security including Federal Information Processing Standard (FIPS) 140-2. We use highest level of encryption (AES 256); see *Exhibit 3.10.1.3-2: Technical Specifications for Hardware and Software.*
SEC20	The Contractor shall ensure that all data, regardless of its location, is encrypted at rest.	The underlying application data is encrypted at rest using Transparent Data Encryption (TDE). We use SQL Server 2016 Enterprise edition to support this function.
SEC21	The Contractor's transmission security shall use TLS 1.2, SHA 2 with a minimum of a 2048 bit key.	Our solution uses industry standard HASH algorithm SHA-2 with and 2048bit (min) RSA hash using TLS 1.2 for transmission.
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."	As part of the development of our SSP, MAXIMUS will perform risk assessments that meet the NIST SP 800-53 Rev 4 requirements. As a standard component of our application development approach, MAXIMUS engages our Office of Information Services (OIS) Security and Audit Team to secure our systems, infrastructure, and operational sites. As described in *Section 3.10.1.2.3–System Security Plan*, we use the National Institute of Science and Technology (NIST) methodology for developing Security Plans, as detailed in NIST Special Publication 800-53 Rev 4, Guide for Developing Security Plans for Information Technology Systems.
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.	The application has role-based security with rules to verify that users can access only the minimum information required for their role. For example, providers can only access their own information. For operational and state users, requests for new user IDs and changed privileges must be in writing and approved by the user's manager before a systems administrator fulfills these requests. Our configurable system security module supports this requirement.
SEC24	All Contractor's module components shall adhere to any applicable the Department system security practices, configurations & procedures.	All module components of our system adhere to industry best practices including state and federal requirements. All components of our solutions will meet applicable Department system security practices, configurations, and procedures.
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.	Through our easy-to-use user management interface, authorized users can grant or remove access through role-based security on various items for a role.
SEC26	The Contractor's solution shall allow access and role changes to be made in real-time with appropriate authorizations.	Through our easy-to-use user management interface, authorized users can grant or remove access through role-based security on various items for a role. These changes are real-time and take effect immediately.
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.	Our security platform includes multiple layers of security and the associated functionality related to integration within a larger infrastructure. See *Exhibit 3.1.10-1: MAXIMUS Provider Services Solution Security Architecture*. Our solution fully complies with this requirement.
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.	Through our easy-to-use user management interface, authorized users can grant or remove access through role-based security on various items for a role or group.

CONFIDENTIAL

ID	Security Requirement	MAXIMUS Summarized Response
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.	MAXIMUS is proposing to use AWS for our cloud-hosted environments. The AWS data centers are extremely secure and do not allow any authorized access. In addition, MAXIMUS will use the Denver, CO office to support much of the system implementation services. The offices are secured under the MAXIMUS security procedures and are available if the State requires access. The AWS sites perform regular audits that can be made available to the State.
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.	Our solution was developed to address all security controls included in the NIST standards. See *Exhibit 3.1.10-1: MAXIMUS Provider Services Solution Security Architecture*. We perform security planning and risk assessment during DDI and annually once we have implemented the system.
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.	
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.	
SEC42	The Contractor shall have an overall data security process that supports data security auditing.	The MAXIMUS OIS requires that all projects containing protected information undergo security audits. We have proposed that our OIS will coordinate creation of project specific procedures and validate compliance. In addition, we will coordinate third-party audits on a yearly basis.
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.	Our solution was developed to address all security control included in the NIST standards. We will validate compliance with the with the security processes outlined in the "Security and Privacy Controls Requirements" document during the creation of our SSP during DDI.
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.	Our security platform includes multiple layers of security and the associated functionality related to integration within a larger infrastructure. We include a set of security monitoring tools in our solution and leverage the cloud-based toolkits provided by AWS as part of hosting solution. We are assigning a full time security resource to the project who will report and mitigate any security incidents.

CONFIDENTIAL

ID	Security Requirement	MAXIMUS Summarized Response
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.	Our system allows authorized user to de-activated/terminated any user account with immediate effect through the web based user interface. Our configurable security model is capable of monitoring the system and generating security alerts based on security parameters. We can also use system tools to eliminate access by specific users as needed.
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	[redacted]
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.	Our solution can generate report for users based on user defined parameters with details regarding the access granted to each user or this list can be seen in real-time on-line.
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.	MAXIMUS will Implement policies and procedures to address security incidents under Security Control Framework. See *Exhibit 3.10.1.2-4: Security Control Framework*.

CONFIDENTIAL

ID	Security Requirement	MAXIMUS Summarized Response
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.	[redacted]
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.	[redacted]
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.	Our solutions electronic signature allows providers to complete and submit an application, revalidation or data updates without the need for a paper signatures. Our solution meets all CMS requirements.
SEC53	The Contractor shall comply with the Harmonized Security and Privacy Framework - Exchange Reference Architecture Supplement Version 1.0 and as required by CMS.	MAXIMUS understands the various requirements included in the Harmonized Security and Privacy Framework. As a long time Medicaid vendor supporting extensive PHI and PII, we meet each of the applicable standards. We will perform a risk assessment during DDI that will validate our compliance with this requirement. We have completed similar audits for our Nebraska and District of Columbia implementations.
SEC54	The Contractor shall comply with the OASIS Web Services Security - Simple Object Access Protocol (SOAP) Message Security Version 1.1 Specifications as required by CMS to build secure web services to implement message content integrity and confidentiality.	[redacted]
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.	As required by the contract, MAXIMUS will be performing security assessments as well as using a third party company to provide audits. If we identify risks that require a response during these reviews we will use 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.
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.	As a corporate standard every employee at MAXIMUS is trained in HIPAA security and privacy requirements. In addition, the OIS will perform project level training as required. Our subcontractors that may have access to protected information are required to sign and comply with a BAA.
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.	At a project level, our hosted environments are specific to a single state. We segregate each of our customers into their own virtualized environments based one size, performance standards and up time requirements. As a rule we do not share data across or customer base for provider. Our solution includes a layered architecture for logical segregation of various components. Various security measures are applied at each layer to prevent unauthorized disclosure of states' data. See *Exhibit 3.1.10-1: MAXIMUS Provider Services Solution Security Architecture.*

CONFIDENTIAL

ID	Security Requirement	MAXIMUS Summarized Response
SEC58	The Contractor's solution code shall never run from a system level account with unlimited privileges such as "root" or "administrator".	[redacted]
SEC59	The Contractor shall ensure the confidentiality, privacy, and security of all state data passing through the Contractor and subcontractor networks.	The state data is transmitted through https secured protocol; thereby avoiding any packet sniffing. SSL certificate with the highest level of encryption is used. We have developed policies and procedures that our solution will meet.
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.	MAXIMUS will work on a contingency plan to establish and implement policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster). See *Exhibit 3.10.1.2-4: Security Control Framework*.
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.	Our system meets this requirement. Our security platform includes multiple layers of security and the associated functionality to protect data from improper alteration or destruction including authentication mechanisms. See *Exhibit 3.1.10-1: MAXIMUS Provider Services Solution Security Architecture*.
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 system is through the web portal. The security banners, headers and footers are configurable. We will work with the state on what needs to be displayed and verify that they adhere to Federal, state, and other applicable standards.
SEC63	The Contractor shall utilize cloud-based technology wherever advantageous to maximize the efficient and effective utilization of technology.	MAXIMUS is proposing to host the solution on AWS cloud. . AWS provides a highly reliable, efficient, scalable, low-cost infrastructure platform in the cloud.
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.	Each user account is tied to a role which is specific to this project. For MAXIMUS employees and contractors, these accounts are tied directly to the MAXIMUS accounts so that terminations are automatically handled. As staff leave the project, we eliminate access to the environment both at the corporate level and at the system level. For other users, MAXIMUS will put a process in place to do a quarterly review to validate user accounts are appropriate.
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	Our solution meets this requirement. The password length, character, expiration, etc. requirements in our solution are configurable. The password is locked after 3 unsuccessful attempts. The session length is also configurable.

ID	Security Requirement	MAXIMUS Summarized Response
SEC67	The Contractor's solution shall track disclosures of ePHI; provide authorized users access to and reports on the disclosures.	Within our solution, access to information is based on a user account, interface transaction or report review access. Our solution maintains an audit trails of all ePHI disclosures. As part of workforce security, we will implement policies and procedures to confirm all members of its workforce have appropriate access to ePHI and reports on ePHI disclosures, as specified in the associated HIPAA Security Rule. See *Exhibit 3.10.1.2-4: Security Control Framework*.
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	MAXIMUS will work with the state in developing Privacy Impact Analysis for collection, use, sharing and maintenance of PII and PHI.
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.	In our solution, PII and PHI data is either redacted or de-identified for entities not authorized to receive PII and PHI, for example public searches, etc. The PII and PHI data is de-identified and re-identification using encryption algorithms.
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.	Any data PII/PHI extracted from the production for testing or other purposes is either masked, for example only last 4 digits of an SSN or Medicaid id field are displayed. We use TDE for data at rest for the production data, and any data extracted will stay in that form.
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.	MAXIMUS has a corporate decommissioning policy that we use for project. In this instance, all of the hardware is virtualized and hosted in the cloud. All software products are included based on RFP requirements. Our corporate infrastructure staff has a listing of all software and licenses and conducts audits to validate a valid license and to validate that the software continues to be used. Any hardware or software that become unnecessary will be presented to the State for approval to decommission.
SEC73	The Contractor will provide the completed reports with the results of the service organization control (SOC) 1 Type II audit annually on date identified by the State. The Contractor shall provide a mitigation plan for all areas of non-compliance. Issues found to be non-compliant shall be corrected within forty (40) calendar days of the report submission to the Department.	MAXIMUS will use a third party that is certified to perform this level of audit. As part of the scope of work, MAXIMUS will receive reports will the full results of the audit. MAXIMUS will develop mitigation plans for areas of non-compliance and correct the deficiency within 40 days. Our OIS project resource will coordinate the activities.

3.10.1.3 Hosting and Environments

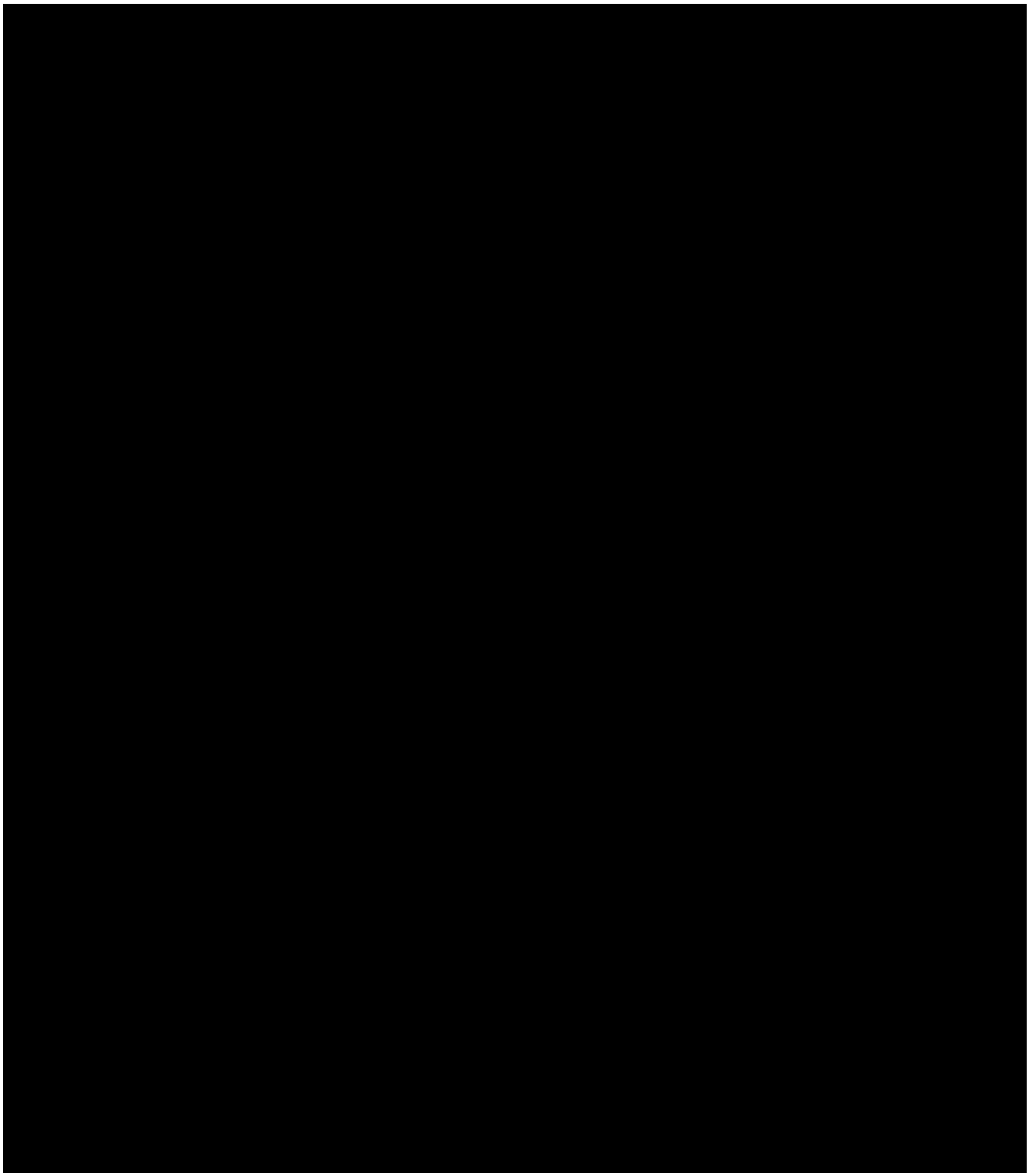
3.10.1.3 Hosting and Environments

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

CONFIDENTIAL

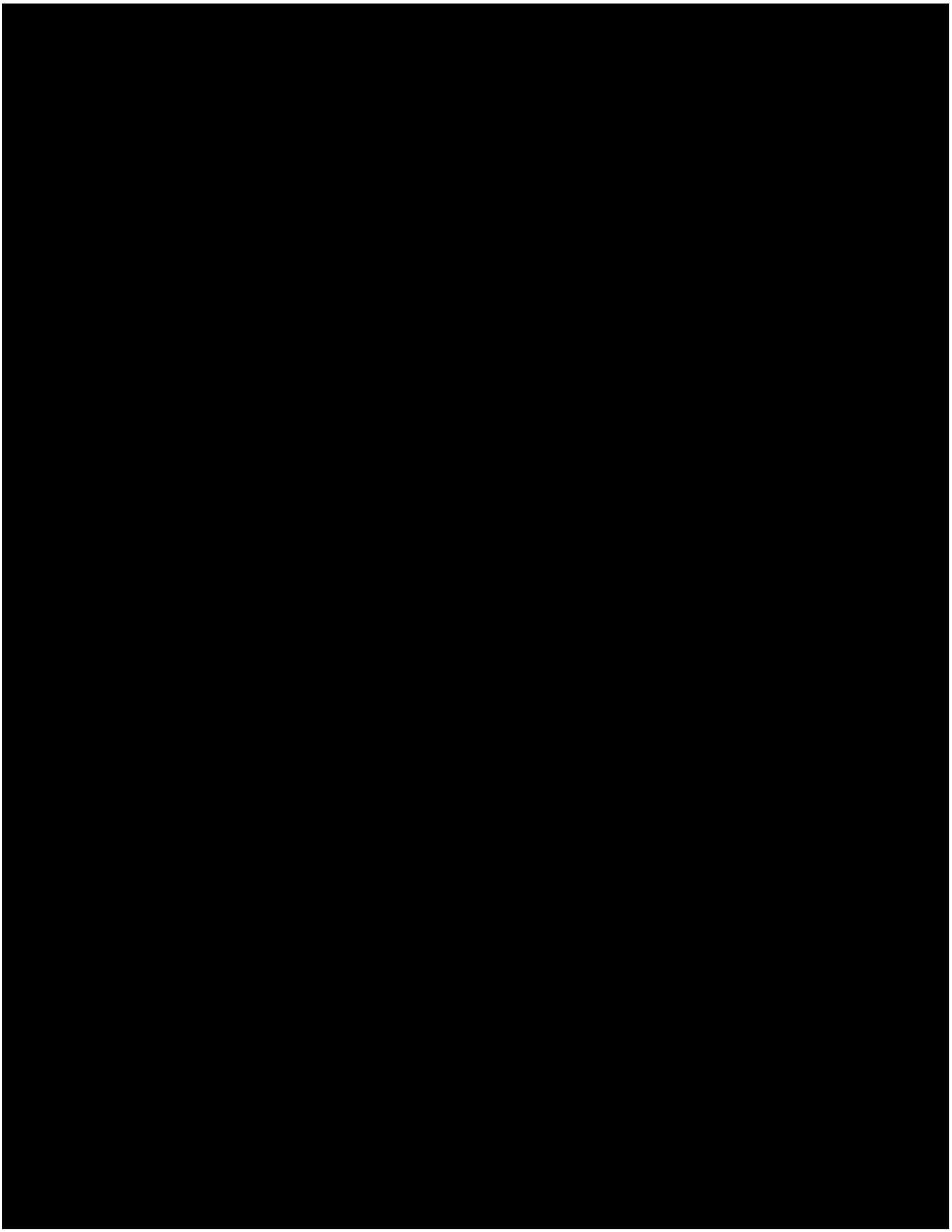
compliance, or has a documented NIST 800-53 rev 4 at a "moderate" system risk assessment designation. In addition, the Contractor is required to demonstrate that their hosting solution is Statement on Standards for Attestation Engagements (SSAE-16) SOC 1 Type 2 and SOC 2 Type 2 compliant.

In their response, the Offeror must describe their approach to solutions and services that meets State and federal regulations, security and performance requirements detailed in Attachment F, Requirements Matrix.



CONFIDENTIAL

CONFIDENTIAL



CONFIDENTIAL

CONFIDENTIAL

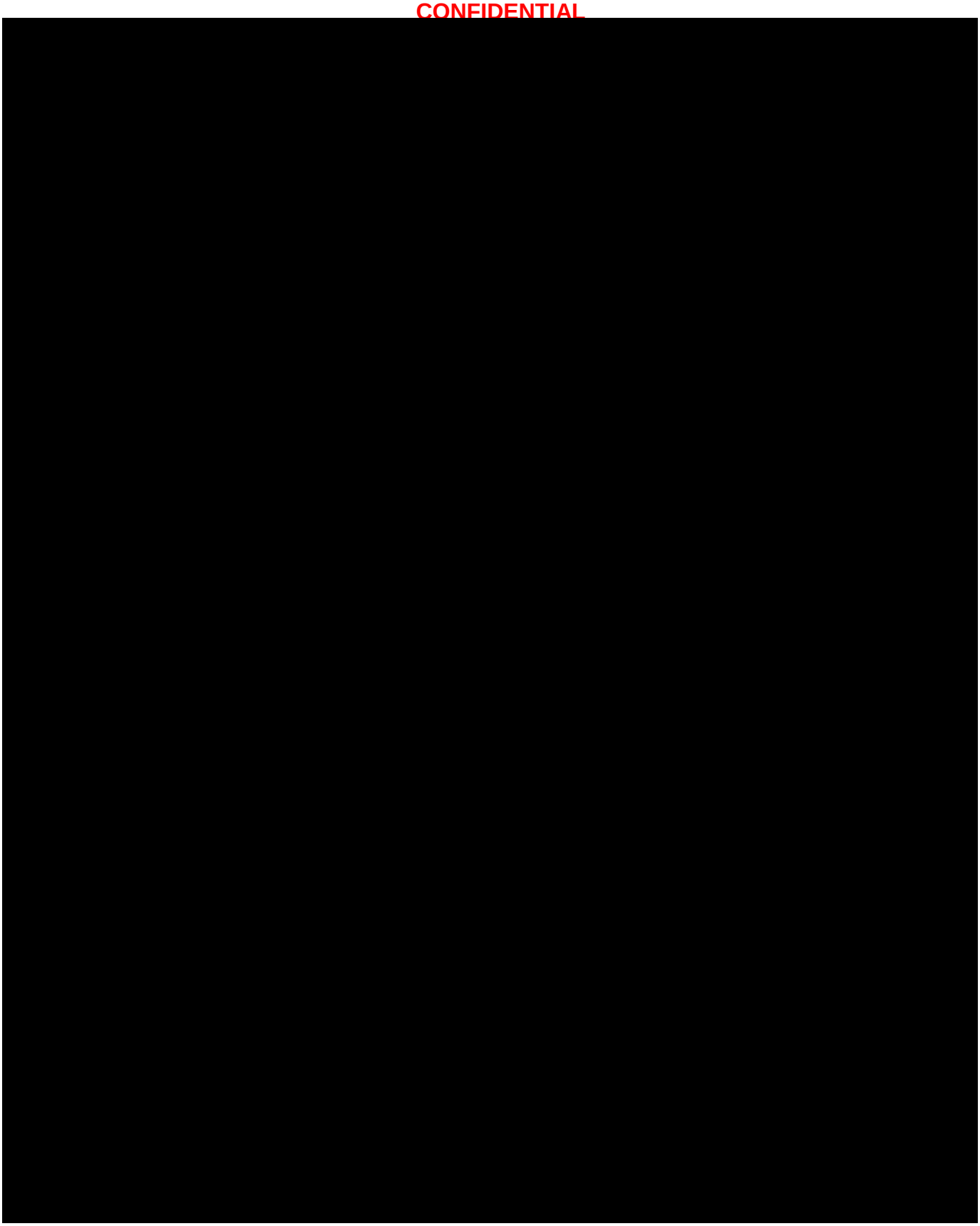
3.10.1.3.2Host Center Environments

To support our solution, MAXIMUS proposes a set of environments that will be in place for the life of the project. Our solution includes development, integration/system test, user acceptance test (UAT), Training, and production environments, each with its own hardware requirements. To support the specific RFP requirements, MAXIMUS has configured the production environment to provide redundancy and meet the system availability 24x7 with 99.5 percent availability.

We are leveraging our existing infrastructure to provide the necessary application support environments for the State, using our development and production sites as the basis for our integrated solution. *Exhibit 3.10.1.3-2: Technical Specifications for Hardware and Software* shows the configurations of the servers we will use to support the Provider Services solution.

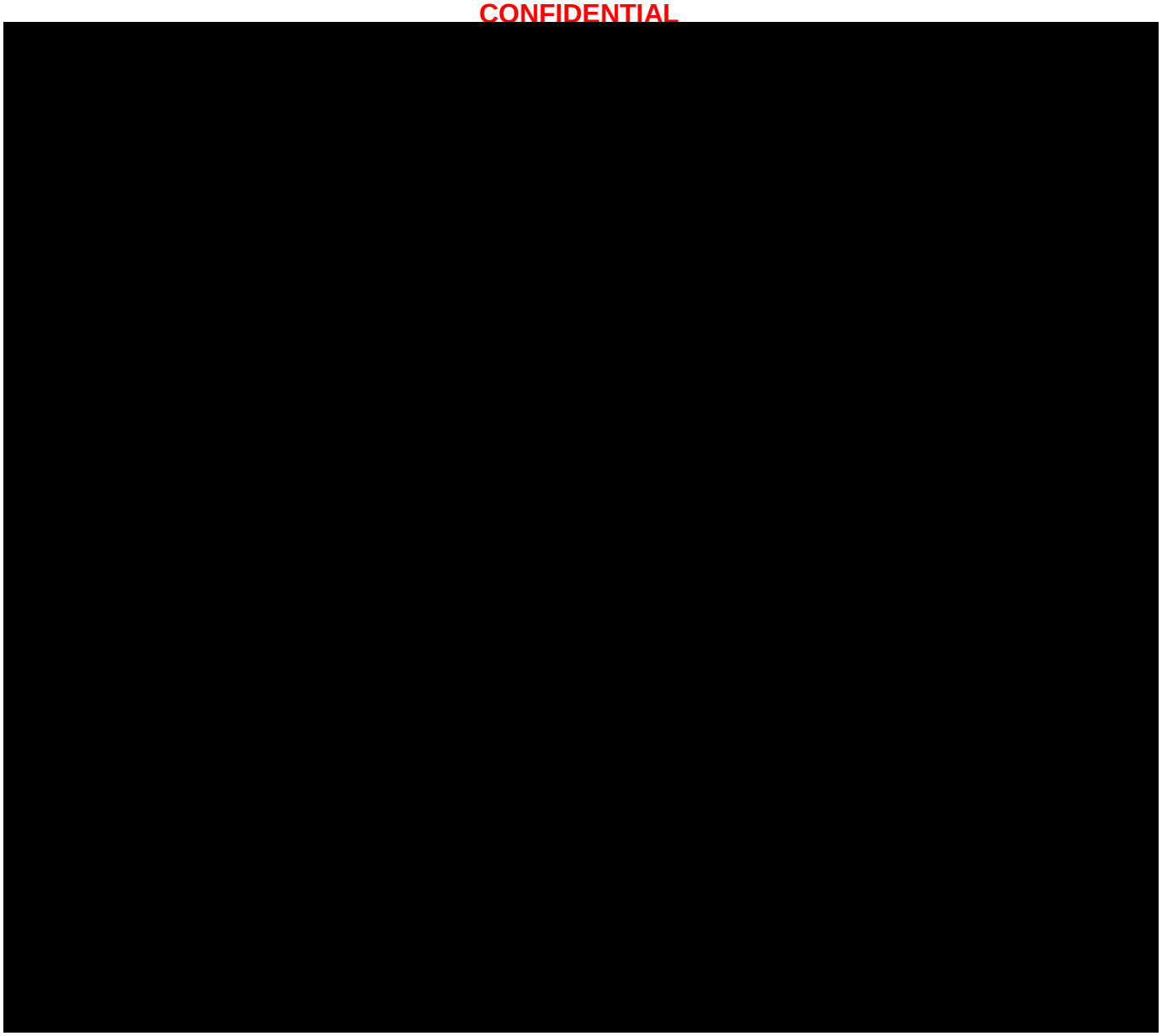
CONFIDENTIAL

CONFIDENTIAL



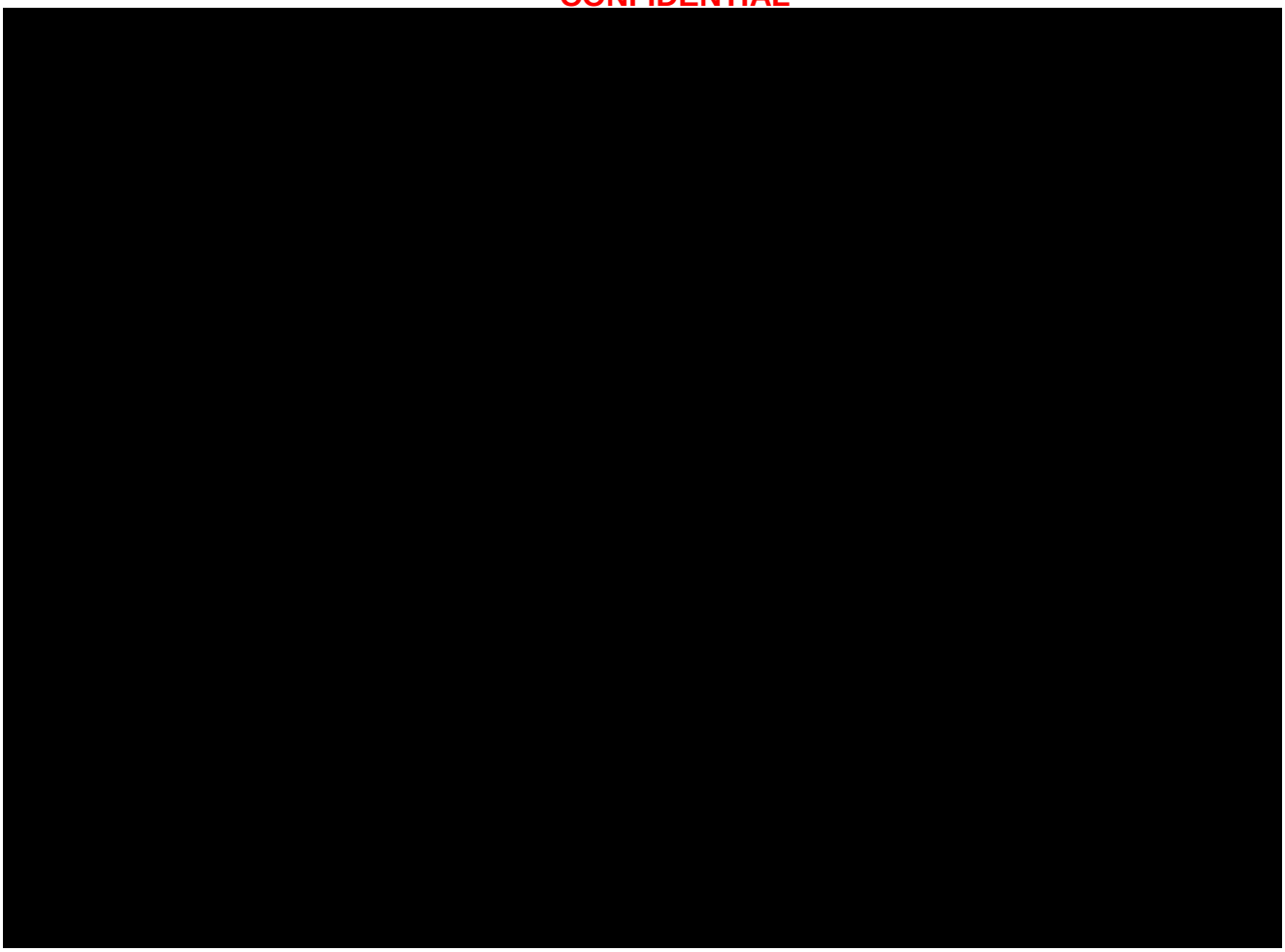
CONFIDENTIAL

CONFIDENTIAL



CONFIDENTIAL

CONFIDENTIAL



3.10.1.3.4Monitoring

MAXIMUS Provider Services AWS deployment comprises different availability zones and regions and will require monitoring across multiple facilities and clouds. If the application encounters downtime or performance issues, it can have an immediate and significant impact on Provider enrollment. Consequently, establishing effective, continuous monitoring of AWS environments is critical to identify bottlenecks and fix issues. To be effective, MAXIMUS proposes Amazon CloudWatch and AppDynamics for tracking and managing performance, availability, utilization, and service levels.

Using CloudWatch in conjunction with AppDynamics allows us to monitor and manage the entire Provider Services application ecosystem, from the browser client request through to network, backend databases, applications servers, and interface performance. With the help of these tools, MAXIMUS provides real-time view of complete health of Provider Services application by monitoring load, average response times, and error rates. There are several out-of-the-box reports and dashboards available. These will be used to report performance to the State. Backup and Archiving

MAXIMUS is using AWS storage solutions to have full backup and archiving capabilities. The two storage mechanisms we use in AWS are Amazon EBS and Amazon S3. All of the Amazon EBS storage is stored as snapshots in Amazon S3 and can be retrieved based on need. Amazon S3 has highly durable and provides redundant storage. Amazon S3 has different storage classes for that allows for archiving data

CONFIDENTIAL

CONFIDENTIAL

with different options for access to archive, from a few minutes to several hours. These will be used on as-need basis.

Hosting and Environments Requirements

The following table includes Attachment F–Hosting and Environments Requirements and our summarized response to each requirement.

ID	Hosting and Environments Requirement	MAXIMUS Summarized Response
ENV02	The Contractor shall provide hosting services that shall meet all state requirements.	MAXIMUS is providing cloud based hosting that is flexible to integrate with other solutions. Using AWS, we can scale as required while providing high-availability options and disaster recovery as an integrated component.
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.	MAXIMUS is proposing to host the solution on AWS. AWS provides industry standard interoperability and allows integration with any number of systems. Our solution is flexible to integrate other solutions for security and regulatory purposes. The proposed model is cost effective with burst capacity that can be implemented seamlessly.
ENV04	The Contractor's hosting environment for all module components shall be compliant with Statement on Standards for Attestation Engagements (SSAE-16) SOC 1 Type 2 and SOC 2 Type 2 and has Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance, or has a documented NIST 800-53 rev 4 at a "moderate" system risk assessment designation.	Provider Services Solution's hosting environment for all module components will be compliant with Statement on Standards for Attestation Engagements (SSAE-16) SOC 1 Type 2 and SOC 2 Type. It has a documented NIST 800-53 rev 4 at a "moderate" system risk assessment designation.
ENV05	The Contractor's solution shall be available and accessible twenty-four (24) hours a day, seven (7) days a week, with the exception of planned downtime due to system upgrades or routine maintenance. All planned downtime and maintenance outages shall be coordinated and approved by the Department at least five (5) business days in advance.	MAXIMUS is proposing a set of high-availability production environments so we will be available 24 hours a day, 7 days a week. We will coordinate any planned downtime and maintenance outages in advance with DPHHS and obtain approval at least 5 days before the outage.
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).	MAXIMUS has engineered high availability production environments supported by a replicated DR site. Our cloud hosting solution contains the full variety of development, testing, UAT, training, production and DR environments built to be independent and run simultaneously without any contention.
ENV07	The Contractor shall identify the physical location(s) where the Contractor's solution is installed and operating. The Department must have transparent access to this location(s).	[redacted]

3.10.1.4 Integration

> 3.10.1.4 Integration
>
> This section addresses integration requirements for the Contractor's solution(s) and operations. As part of the DDI, the successful vendor will be required to interface with the legacy MMIS and the MPATH Integration Platform once it is established. Once the MPATH Integration Platform is implemented, the Department expects the vendor to integrate with the MPATH Integration Platform through standardized interfaces. The ESB is the communication broker and web services orchestrator for MPATH Integration Platform which is administered by the MPATH Systems Integration Services Contractor. The Provider Services component(s) must ensure all service endpoints/APIs are clearly defined, exposed to the ESB and be able to receive and submit messages through the ESB to facilitate standardized data exchanges throughout the MPATH

CONFIDENTIAL

> Integration Platform. The offeror must describe their approach to meet each of the integration requirements detailed in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services Solution platform has a flexible design to allow for integration with different services and applications with a focus on configurability. This is achieved by taking advantage of a mixture of mature technologies and a system architecture built to change and adapt. To provide interoperability with other systems, our solution exposes well-defined service components based on open standards and is able to support data exchanges in any manner that a trading partner prefers. Our solution takes advantage of the open standard to efficiently integrate with disparate systems and we have successfully integrated with all required trading partners in our three current modular implementations of our Provider Services solution.

MAXIMUS Provider Services solution is built on the Microsoft Technology stack and is built with standards including WS-* to allow it to interoperate with variety of systems. Our system integrates and interoperates with other State systems using a variety of interface mechanisms including web-services, flat files and other transfer mechanisms used by our trading partners. In addition to SOAP and WSDL for WS-* compliance, our solution can also expose web services as REST, UDDI, ODATA and JSON-WDP formats for clients and trading partners that are capable of consuming them. By using web services, our solution can be used to integrate with an ESB as a centralized integration engine. Wherever an ESB is not available, we have integrated with disparate systems using point to point communication models.

MAXIMUS understands that it is likely we will have to integrate with the legacy MMIS using secure flat file transactions until the System Integration module is implemented. We have extensive experience implementing integration with legacy vendors and we currently integrate with a legacy Conduent MMIS in the District of Columbia. This experience and understanding of the Conduent operating structure will help speed the design of the interface and if possible may allow the reuse of the District of Columbia solution.

Once the System Integration Module is implemented, we will update this data integration to utilize the new standards and ESB that will be in place. Over the course of time, we have collaborated with distributed and scattered applications that are built on different operating systems and programming languages. With this, we have built and used a number of adapters to that we can leverage when we do our integrations in our future implementations. We plan to use this experience is a manner where much of the legacy MMIS interface will remain in place after the System Integration module is available so that we do not have to make major changes to an interface that will be proven. We can focus on data integration and the processes around providing and receiving data via the ESB.

3.10.1.4.1 Interface Adapters

MAXIMUS Provider Services solution uses MS SQL Server backend for storing data in data repository. If needed, we can integrate with different databases, such as ORACLE. Our solution is capable of sharing and federating data in the format needed by other vendors. We have provided flat file based, SOAP, and XML based formats to MCOs and other trading partners in our previous implementations. Based on specific trading partner needs we will clearly define APIs and other endpoints as well as cataloging all web service interactions.

MAXIMUS Provider Services solution comes with several adapters as configurable options to be ready for varied integrations. It can be configured to handle different adapters like ODBC and is working with different protocols like FTP, SFTP, FTPS, HTTPS, SSH, POP3, SMTP and TCP. Our solution is capable of working with asynchronous communication protocols and message queuing technologies like MSMQ, ActiveMQ, etc. These adapters are primarily configurations in our solution that can be easily pluggable. MAXIMUS solution has done different transformations using our transformation engine from one format to another as part of doing interface data exchange.

3.10.1.4.2Event and Transaction Modeling

MAXIMUS Provider Services solution is built on a SOA based architecture to modernize the Provider management using MITA principles. Our solution is augmented with several COTS products to extend specific functions and allow user input thus making a number of interconnected sub-systems to make our solution. Also, our solution plays a role of module in a large set of disparate and distribution systems. To overcome the challenges of co-relating events happening in across different sub-systems or across systems, our solution puts all the events in a centralized location. In our solution, we have processes in which there are transactions. We have developed mechanisms through which we identify a process and the transactions that happens as part of the process. Each process will have a number of events that happen in them. These transactions and the events that happen in a given process are related. These co-related events and transactions that happens in a given process are presented in an aggregated and integrated manner in our application. This model of aggregation of data gives us the ability to federate data with data sharing partners. Other data sharing and federating abilities are discussed in detail in *Section 3.10.1.5–Data Management*.

3.10.1.4.3Business Process (Workflow) Engine Integration

The MAXIMUS Provider Services solution Business Process Engine is built on an event driven workflow mechanism that enables high-performance, flexibility, and extensibility to the solution. The Business Process Engine automatically executes the appropriate business process model based on the inputs from the business rules engine. More on the architecture of business process engine is found in *Section 3.10.1.9–Workflow* section. Our workflow event driven mechanism can be based on automated or manual processes. It can also be configured to be scheduler driven event. An example of scheduler driven event is that if an application is not submitted in 10 (configurable) business days, cancel the application.

The MAXIMUS business process engine brings several unique features that allow a broad, flexible, and transparent automation. In our previous implementations, with the help of our business process engine, we are able to clearly define, model, execute, monitor, refine, and automate the business processes with ease. Our engine has standard tasks like web-based manual tasks, workflow queue tasks, email tasks and custom tasks. Our business analyst experts will work with DPHHS to understand the processes and define the workflow model with a combination of these tasks. On each of these tasks, we will be defining the task triggers to allow of manual and automation processes. These triggers will allow the process engine to take inputs from the presentation layer, scheduling framework and other external automation models to complete an end-to-end process that can be orchestrated in the engine. Each task and task trigger has a security layer to allow only certain users to perform orchestration of the specified tasks.

The business process custom tasks can be built to connect to web services to gather data from external entities as part of a business process. For example, MAXIMUS is building a complex background check processes in our District of Columbia implementation that initiates finger printing with 3rd party vendor selected by the District as part of screening of high-risk providers. The custom processes are built to call web services of third party to initiate background checks, send appropriate communications to providers, and monitor for background check results. If background checks results are not available within 30 days, the scheduler tasks will send appropriate messages to remind providers and put them in termination queue as needed. If background check results are received, our workflows are configured to route the provider application to appropriate operators based on positive and negative results. This advanced level of orchestration of workflow based on the presence or absence of results by integrating with third party is possible because of our SOA compatible business process tasks. Our business process engine can be easily integrated to any ESB.

3.10.1.4.4ESB Interoperability and EDI Integration

MAXIMUS will work with DPHHS and the Systems Integration Services Contractor to allow for exposing the web services from Provider Services solution to other applications. The MAXIMUS solution has all the capabilities to consume web services from ESB and we are able to exposure services as well that will enable other system to use provider data as needed for their business processes.

In our Tennessee implementation, our solution has become gateway for all information for Providers with implementation of CAQH CORE requirements. MAXIMUS created and consumed services that are exposed via ESB in building the claims and eligibility requirements for the State of Tennessee. MAXIMUS solution is able to provide Electronic Remittance Advice (eRA), 835, 271/272 and 276/277 EDI transactions to providers through Provider Services solution in Tennessee. This is achievable due to our flexible SOA model and our interoperability standards. The MAXIMUS Provider Services solution has proven technological capabilities to connect to any ESB.

As part of all of our implementations, we have integrated with MMIS for information exchange. In our Tennessee implementation, we have exchanged information via ESB for MMIS integration. In our other implementations, we have accustomed the protocols that the MMIS is capable of. Wherever available, we will integrate with ESB as per the discussion and requirement with the State. MAXIMUS has built-in staging tables and alert mechanisms that we receive from MMIS to be shown to the users as part of integrations. In case of errors, the errors are written to a report and the application notifies the necessary parties so the errors can be looked into. Due to our versatile interface framework, we are able to provide web services, XML and flat file based interchanges with different systems. Provider Services includes exception and error handling modules to capture and recover from the issues raised during the batch interface processes.

The bulk processing capabilities of Provider Services Solution facilitate the processing of transactions for multiple Providers simultaneously. The bulk processing is used to perform updates/adds for Providers, group affiliations and any other Provider information in a very efficient manner. The bulk processing capabilities are wrapped around exception handling. Our exception-handling model for bulk operations allows for processing all the successful transactions while putting the error transactions in a queue for manual review and intervention.

The interface processing happens at different batch schedules and can also be instantaneous based on file triggers or web service calls. *Section 3.10.1.6.7 subsection–Interface Scheduling* discusses batch-scheduling capabilities in detail.

3.10.1.4.5GIS Integration

The MAXIMUS Provider Services solution provides a real time link to the USPS address verification service to validate all addresses that are entered into the system. Providers have the ability to select the validated address or to keep the originally entered address. The Address Verification function also captures the geo-coordinates of the address and stores these in data store to enable the Geographical Information System (GIS) search capability. Our solution supports retrieval and presentation of data associated with various geographic indicators such as State, County, zip, peer group, etc. Please refer to the *Exhibit 3.10.1.4-1: MAXIMUS GIS Search* for further details on how the system handles address verification.

3.10.1.4.6NPI Validation and NPPES Integration

For the majority of providers, our solution requires the entry of a valid NPI. We edit to ensure that organizational providers utilize a Type 2 NPI (Organization) and Individual Providers use a Type 1 NPI (Individual). These edits are enforced during the initial enrollment process through a real time service call to NPPES. Once the Provider's NPI is entered, the system validates that the NPI is active and is of the correct type per the type of Provider enrolling. With these edits, the system will not allow a Group NPI to be entered for an Individual and conversely, will not allow a Group to enroll using an Individual NPI.

Different States use different rules for enrolling Atypical Providers. In our most recent implementation for the District of Columbia, an NPI is required to be entered for all Providers, regardless of Provider

type. In our Nebraska and Tennessee implementations, entry of the NPI is not required for Atypical Providers. In either case, the system is configurable (using Provider type) to set a parameter to indicate if an NPI is required for the Provider type. This is a simple rule change we make to the system once we confirm the requirements for each State. For the Provider Services solution Montana implementation, the default configuration will not require NPI for the Atypical Providers.

3.10.1.4.7Data and Document Sharing

MAXIMUS Provider Services system is built to Open Interface standards that allows us to provide all the data that we collect from providers to other systems. In our other implementations, we have provided data in various formats for MCOs, CVOs and other trading partners on a recurring basis to satisfy the needs of the state. MAXIMUS will work with DPHHS and other vendors to identify the requirements on the data needed for different modules. MAXIMUS will expose the APIs needed for this via ESB to allow for other systems to consume the data.

MAXIMUS will work with the centralized ECM vendor and System Integration vendor on the APIs to be exposed for transferring provider documents into the centralized ECM. MAXIMUS has prior experience in building the APIs necessary to transfer documents from our application to a centralized ECM. In one of our Medicaid Provider Incentive projects for the State of Iowa, we have transferred all the documents uploaded by the provider into the State's centralized ECM. MAXIMUS will expose/consume necessary APIs to transfer all provider documents to centralized ECM. MAXIMUS will also expose APIs so documents from other systems can be transferred from other systems into the Provider Services solution. We will expose APIs for other systems to provide the provider information, metadata about the document and the document itself. We will store the transferred documents into our ECM and tag it with the provider metadata. We will show the document in the provider file along with the rest of the documents.

3.10.1.4.8Maintenance and Operations

The MAXIMUS maintenance and operations support model is designed to keep the Provider Services solution in good operating order. A key component of our support model is ensuring that the hardware and software infrastructure operates on the latest versions available. Our overall hosting solution includes the requirement to keep hardware and software on at least the n-1 version with built in upgrades as new products become available. The virtual nature of our environments and the use of a Cloud Service Provider (CSP) add to our focus on keeping our environment using the latest technology.

MAXIMUS will provide the State, at no additional cost, the hardware, software, and upgrades needed to confirm the solution operates with the latest version or the n-1 version as approved by the State, and necessary for fulfilling the scope of work defined in the contract. MAXIMUS will also provide and support all maintenance, upgrades, and updates for Provider Services solution. Product maintenance and updates will be provided at no additional cost to the State and will be completed within the timeframes approved by the State. MAXIMUS will provide electronic notification including detailed release notes for all maintenance, patches, updates and fixes deployed to the production environment. Our processes for system maintenance can be found in *Section 3-10-4 Operations, Maintenance and Configuration*.

The MAXIMUS integration model includes implementing the system as fault tolerant. MAXIMUS has used enterprise patterns to ensure discrete systems are utilized to provide availability, reliability, and acceptable performance. MAXIMUS will work with the system integration vendor to ensure the systems

are loosely coupled so they can be changed quickly. If another system experiences an outage, upon recovery the MAXIMUS solution has built-in mechanism to catch up on the transactions that needs to be sent and to continue to operate without manual intervention. In our Tennessee implementation, regular maintenance to EDI transaction services do not interfere with the Core Provider Services modules and as the EDI services come back, our solution automatically resumes service.

The MAXIMUS Provider Services solution has been integrated with a number of State and third party systems and databases such as MMIS, Screening databases, CMS and so on. MAXIMUS will work with the system integration vendor and DPHHS to develop comprehensive operational procedures for system maintenance, system downtime and disaster recovery scenarios. MAXIMUS will develop any services and processes needed to automatically report system availability to the SI availability solution.

3.10.1.4.9Integration Requirements

The following table includes Attachment F Integration Requirements, our summarized response to each requirement, and the section(s) in our proposal in which we provide our detailed response.

ID	Integration Requirement	MAXIMUS Summarized Response
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 MAXIMUS Provider Services solution allows for searching for providers based on geographic indicators. This is discussed in the section on GIS Integration. We can show any data that is stored in the data store.
INT10	The Contractor shall develop operational procedures in coordination with other enterprise module vendors to restore system availability.	MAXIMUS has proposed a high availability configuration that should eliminate most down time. We have also included in DR site to support recovery from a disaster in less than 4 hours. As part of our DR plan, MAXIMUS will work with the Department and other enterprise module vendors on procedures to restore system availability and specific items that need to be taken into account in the event DR sites are used to restore availability.
INT15	The Contractor's solution shall use XML standard messaging format to ensure interoperability.	Our solution is based on an Open Interface framework and uses SOAP-XML standard messaging formats. Our solution is integrated with other systems in different implementations using SOAP-XML standard messaging format. We will follow the guidelines established by the System Integrator.
INT22	All service endpoints/APIs shall be exposed to the ESB and are able to receive and submit messages through the ESB.	Our solution is designed to expose and consume service endpoints on an ESB. Our solution is integrated on an ESB in our previous implementations and we can receive and submit messages through ESB. As described in the vendor questions and answers we plan to move all available interface into the ESB but will also support legacy and other integrations required by partners systems.
INT35	The Contractor shall provide an architecture that has clearly defined service endpoints.	Our solution meets this requirement. MAXIMUS creates SOA services as domain driven and use case based so they are relevant to the existing business processes and granularity recognized by the user as a meaningful service. Our solution has a web services registry that documents the web services available, the service endpoints and the mechanism in which the services can be consumed. The Provider Services Solution web services registry is re-built automatically when a new service is added or when an existing service is modified.
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.	MAXIMUS will provide technical, functional, performance and other documentation as required by IV & V Contractor for the solution to support identified IV & V reporting needs.

ID	Integration Requirement	MAXIMUS Summarized Response
INT52	The Contractor shall collaborate with all State enterprise contractors and solutions to accurately collect, process, and distribute applicable HIPAA EDI transactions.	MAXIMUS has experience building HIPAA EDI transactions in our previous implementations. We will work with all State enterprise contractors to accurately collect, process, and distribute the EDI transactions. We anticipate implementing a solution that integrates multiple different modules of MPATH to meet this goal.
INT54	The Contractor's solution shall require (when appropriate), capture, and maintain the 10-digit NPI.	The MAXIMUS solution verifies NPI entry via a real-time web service call to NPPES. Our editing ensures that Organizational Providers enroll using a Type 2 NPI (Organization) and Individual Providers enroll using a Type 1 NPI (Individual).
INT55	The Contractor's solution, shall accept the NPI in all applicable standard electronic transactions mandated under HIPAA	MAXIMUS will work with DPHHS to identify the electronic transactions that accept NPI and will send NPI as part of the electronic transactions. We anticipate processing HIPAA transactions in conjunction with partner systems. We will work collaboratively to implement the best process available.
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.	MAXIMUS will ensure all the 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.
INT60	Unless otherwise mutually agreed to in writing, Contractor must maintain any and all hardware and software products required to support the Contractor's solution at their most current major version the (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.	MAXIMUS will work with DPHHS on maintaining all hardware and software products required to support the Contractor's solution at their most current version. For any exceptions, we will work with DPHHS to get the exceptions in writing.
INT61	The Contractor's solution shall allow internal and external stakeholders to upload and view electronically submitted documents.	The MAXIMUS Provider Services solution is designed to index and store all the electronically submitted documents in ECM. The documents are available for authorized internal and external stakeholders to view and upload. Multiple functions within our solution support this requirement.
INT62	The Contractor's solution shall ensure information and event notifications include aggregated and integrated information.	Our solution has aggregated and integrated event notification models. This is discussed in *Section 3.10.1.4.2–Event and Transaction Modeling.*
INT63	The Contractor's solution shall have business process orchestration in an event-driven environment that maximizes process automation.	Our workflow business processes are event driven and are based on automated or manual processes. The processes can also be configured to be scheduler driven event and are designed to maximize process automation. This is discussed in *Section 3.10.1.4.3–Business Process (Workflow) Engine Integration.*
INT65	The system shall provide the ability to share and federate data with other data sharing partners.	Our solution has the ability to federate and share data with other data sharing partners. This is discussed in *Section 3.10.2.5–Data Management.*
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 MAXIMUS Provider Services solution has a wide variety of processes that will enable the ability to create/edit, send, receive and process X12, NIEM standardized transactions and NCPDP D.0 transactions. We have implemented an integrated module for creating and processing X12 EDI transactions through integration with EDIFECS. We anticipate working closely with the State to determine how best to meet this requirement taking into consideration the functions included in other modules.
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.	MAXIMUS will collaborate with the System Integrator to automatically report system availability to SI availability solution through exposing this information to the ESB. The frequency of Provider Services module can be defined by the department.

ID	Integration Requirement	MAXIMUS Summarized Response
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.	MAXIMUS has identified the software and license we use to implement our solution. MAXIMUS will ensure all the licenses necessary for the scope of work to support the infrastructure with sufficient bandwidth and redundancy to ensure accessibility, reliability/fault tolerance, and acceptable performance.
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.	MAXIMUS has deployed Provider Services solution in three different states. We have expertise in understanding the business processes, suggesting changes, and automating them. During the DDI effort, we will work with DPHHS to understand business processes for Montana, automate and orchestrate the workflows, business rules, data flow and metadata within the solution. We will work collaboratively with the SI. Please refer to *Section 3-10-2-8* for more details on our implementation approach.
INT74	The Contractor's solution shall have the ability to identify errors in transactions and immediately notify the source system of the specific errors including whether the errors have precluded loading and/or using the data.	Our solution has event and transaction aggregation mechanisms through which we can identify error events in transactions and immediately notify the same. MAXIMUS will work with other vendors on the method for notification and an SLA for correcting specific errors.
INT78	The Contractor shall provide an environment where components can be added or replaced quickly.	MAXIMUS has adopted agile oriented practices. Our modular system is built to quickly add/update components for faster turnaround times. We follow continuous integration and continuous delivery practices to allow the changes to be deployed to production faster. Our implementation approach is based on our ability to take components from each or our implementations to meet Montana specific requirements.
INT79	The Contractor's solution shall allow internal and external users to enter data using electronic forms and receive documents electronically from other systems.	Our solution allows internal and external users to enter data using electronic forms. We will work with SI vendor to build APIs/Services needed to receive documents electronically from other systems. Our ECM provides the ability to receive documents from other systems and automatically index and store them on the provider record based on parameters passed from the sending system.
INT80	The Contractor's solution will interface with the State's designated financial processing solution.	The MAXIMUS Provider Services solution can be integrated with State's designated financial processing solution. We have developed interfaces that are SOAP-XML based and also flat file based interfaces in our previous implementations. Our interface capabilities are described in *Section 3.10.1.6–Interfaces*.
INT81	The Contractor's solution shall have the capability to receive and display data, messages, and alerts from other systems in real-time.	Our solution has event and transaction aggregation mechanisms through which we can receive and process alerts from other systems. With SOA integration with other systems, we can display the messages, data and alerts from other systems in real time. During DDI we will identify the specific use cases for this function and integrate it into our solution as required.
INT85	The Contractor's solution shall support web services, specifications, and adapters: (e.g., ODBC, Web Service (WSDL, WS-*, SOAP, REST, UDDI, ODATA), JSON-WDP, MS SQL, SQL Server, Oracle, FTPS, SFTP, HTTPS, MSMQ).	The MAXIMUS Provider Services solution supports all of the various protocols as described in section Interface Adapters.
INT86	The Contractor's solution must be capable of receiving, translating, and processing data to and from the variety of protocols (e.g., FTP, FTPs, SFTP, HTTP, HTTPS, JMS, JDBC, ODBC, NET, AS2, AS3, POP3, SMTP, SSH, TCP, CICS). The Contractor shall include in their response a list of protocols supported.	The MAXIMUS Provider Services solution supports various protocols as described in section Interface Adapters.
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 MAXIMUS Provider Services solution provides context sensitive help as the provider goes through enrollment process and maintenance activities. We work with the client during DDI to identify how best to expose the help functions as different clients have different requirements.

ID	Integration Requirement	MAXIMUS Summarized Response
INT88	The Contractor shall implement a solution where module components are loosely coupled and can be added or replaced quickly.	Our system is built with modular approach. The individual modules have unit and integration tests and are loosely coupled with other modules. This gives us the ability to quickly add/update components for faster turnaround times. We follow Continuous integration and Continuous delivery practices to allow the changes to be deployed to production faster.
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.	MAXIMUS will provide electronic notification including release notes for major and minor versions, patches and updates and fixes deployed to production. This effort is defined in our Maintenance and Operations procedures and we follow those for every system build and release. Our processes for the same are described in *Section 3-10-4 Operations, Maintenance, and Configuration*.
INT94	The Contractor shall work collaboratively with module vendors to reconcile ODS data elements with the all data elements for each module component.	MAXIMUS will work collaboratively with module vendors to reconcile ODS data elements for each module component.

3.10.1.5 Data Management

> 3.10.1.5 Data Management
>
> Data management within the Offeror's proposed solution and operational data management policies must at a minimum meet HIPAA, HITECH, ARRA and other federal and state privacy and security requirements as they exist on the release date of this RFP and be configurable to assist in meeting future requirements. The Offeror must describe their approach to meeting each of the Data Management and Data Services requirements detailed in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution is designed to deliver flexibility and adaptability to accommodate the needs of the client. The MAXIMUS Provider Services solution is loosely coupled which enables reuse and improves maintainability for post deployment extensibility. The MAXIMUS Provider Services solution uses data to control most aspects of how the system functions. Data, in conjunction with Corticon rules engine, controls workflow and business rule decisions as well as forms the basis for the creation of dashboards and other reports showing the status of the Program. MAXIMUS uses structured processes and procedures to control how data is stored, edited, and ultimately used and reported.

Our data repository is scalable and extensible, providing a flexible structure to meet processing, reporting requirements and increasing amounts of data. The data model stores all the data related to the Provider and all the revisions of a Provider application in a very efficient manner. Our solution can accommodate new categories of data, as the approach for adding new categories is a configurable process. We first identify the data structure needed to support the business. Once we create the data structure and the UI component, the configuration of the allowable CRUD operations is auto-generated by the system.

3.10.1.5.1 Reference Data Management

Our solution provides robust reference data management functionality and is driven by a data model that has reference data for all the Provider management functionality. The reference data management interface enables State approved users to administer and update the reference data. All data provided by external sources is stored as reference data. This includes Provider types and specialties, program identifiers and application types. We build referential integrity between related reference data and provide system functionality to support, maintain, and track these identifiers and their relationships to each other.

To maintain reference data, the system contains a variety of online functions that are used to add, modify, or delete data fields and elements in the Provider Enrollment Master File and tables. Audit trails exist to

track any changes to reference data. The reference data maintenance is discussed in more detail in *Section 3.10.1.5.4–Application – Data Management/Reference Files.*

3.10.1.5.2 Extract, Transform and Load Module

Our solution has Extract Transform, Load (ETL) programs to load data from different data sources. The ETL loads data from third parties as well as CMS and State databases such as SSDMF, NPPES, OIG LEIE, and EPLS/SAM. The ETL framework is extensible to add new data source formats. The data extraction module has the capability to download the data files available on the other MPATH modules' web sites, unzip the file, and load the data into the database in an automated fashion as per a pre-defined schedule. We also use these capabilities as part of the data conversion effort where we define transformations and conduct numerous test runs to validate data is moved correctly.

The data extraction module is capable of automatically extracting data from a variety of data source formats. Using this function, we connect directly to http URLs, download data and depending on the format of the data, unzip if needed and load the data into the respective data source. Some data sources (for example, SSDMF) are protected. MAXIMUS follows HIPAA guidelines to store protected and private data. The data extraction module authenticates to the web site and downloads the files during the data extraction process. We can quickly configure our solution to add new data sources like certification, licensure, and contract data from State and State approved agencies. MAXIMUS has used these functions repeatedly during our implementation projects to expand the data we bring in from internal systems. During our District of Columbia implementation, we added a CLIA interface with a State approved agency to extract CLIA data on a monthly basis and update the Provider record. Under this contract, we will gather such requirements and create automated processes to exchange and process certification, licensure data with State agencies during the DDI phase. We are willing to discuss the integration of any data stores the state currently owns, licenses, or has access to. We believe the greater the integration of data, the stronger the audit and screening capabilities.

Our solution's data extraction module has a scheduling capability to download data from data sources on any schedule. We use this to execute extract and load processes from data stores based on their update schedule. This capability is used extensively in our interfaces as discussed in *Section 3.10.1.6–Interfaces*.

3.10.1.5.3 Audit Trail

MAXIMUS has built a robust audit mechanism in our data repository. This audit trail data includes information about who made the change, when and where it was done, and the actual information added, changed, or deleted. The auditing model is a core feature of our software framework and is deployed in all of our implementations.

There are three types of audit trails in our MAXIMUS Provider Services solution. The first allows a user to click on a history icon while viewing a screen to view the history of changes that may have been made to the data fields displayed on that section of the screen. *Exhibit 3.10.1.5-1: View Audit Trail* provides an example of a Provider viewing changes made to Organization Information name for the Provider.

CONFIDENTIAL

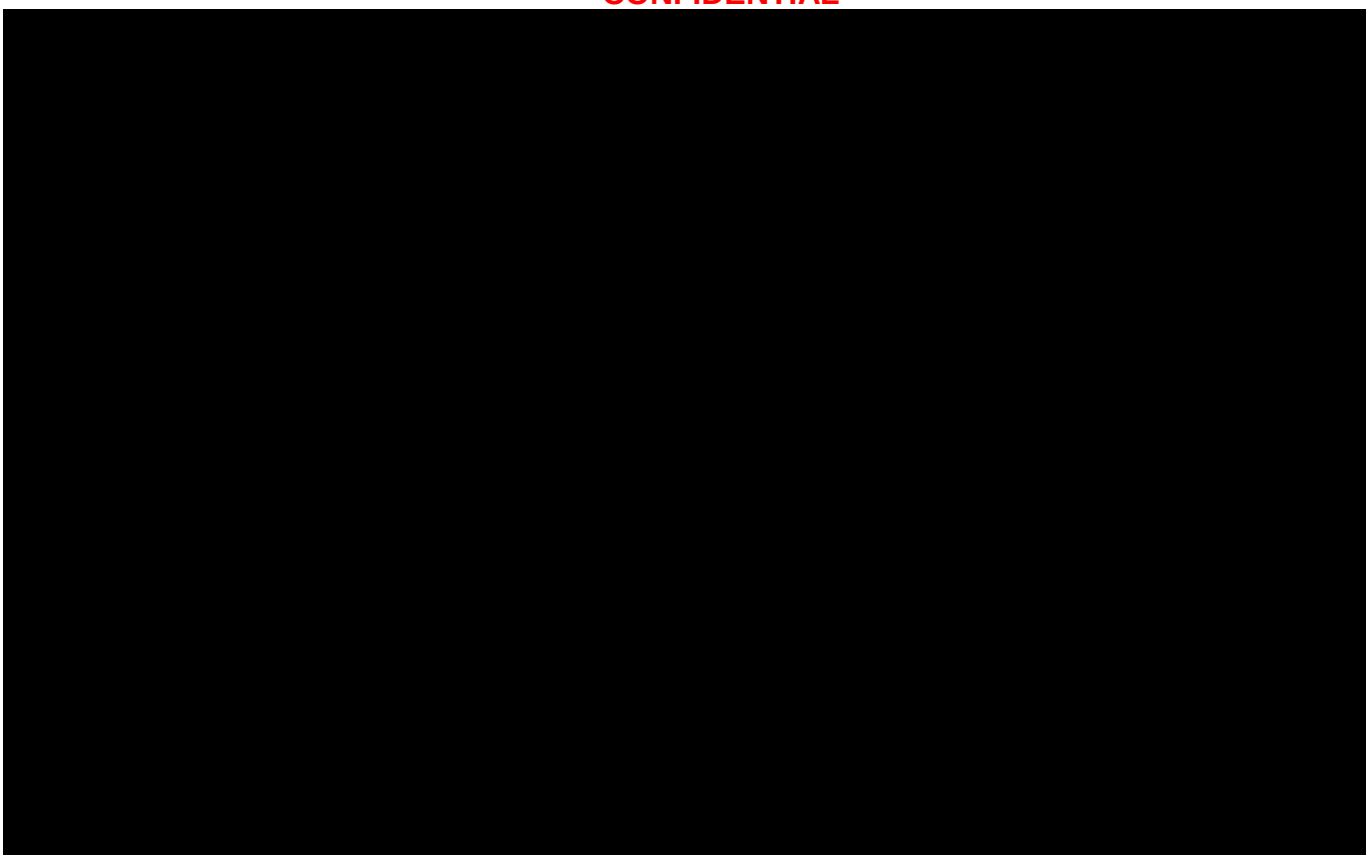
Users view the current data for the Provider in the summary grid. A user can view the history of changes made to any of the data in the summary grid by clicking on the history icon below the grid. In the example above, a user has clicked on the history icon to view the history of changes. The system shows that the organization history was changed by the user “phill” and the operator “SPOperator”.

The system keeps a log of all steps in the Provider workflow and when that step occurred during the workflow. This feature is useful in determining what actions were taken during Provider enrollment by any user involved in the workflow. This feature is discussed in more detail in *Section 3.101.9.3–Provider Registration and Workflow, subsection Provider Application Routing*.

Our solution also provides the Application Audit Trail report. This report includes before and after values of data element(s) that were changed, along with ID of the user that made the change, including changes that were made via interfaces or batch processes. *Exhibit 3.10.1.5-2: Application Audit Trail Report* provides a snippet of the on demand report available to internal users for viewing a complete audit trail of changes made to Provider data.

CONFIDENTIAL

CONFIDENTIAL



Our solution tracks changes to the data definitions and reports in the source repository and can provide the changes to data definitions and reports to the State when required.

3.10.1.5.4 Application – Data Management/Reference Files

The MAXIMUS Provider Services solution data model has been defined based on the specific CMS requirements for Provider enrollment and screening and the latest Certification Checklists. Based on our experience we have augmented our data model to include data that are used to manage and support the Provider community. We utilize a relational database model built in Microsoft SQL Server Enterprise and enforce referential integrity between tables in the system for accurate data. We also integrate reference tables into the model with referential integrity to verify specific information reported by Providers and other MPATH modules is correct and accurate for the Provider type and specialty.

The reference data is modeled based on recommendations from industry and domain experts. All reference data is stored in the database and can be updated using web-based user interface. Using Corticon, we have integrated many of our reference tables into the rules engine for direct use in business processing. As part of our conversion methodology, MAXIMUS will load the database with initial reference data by looking at the MMIS and other valid data sources during the DDI phase. Once loaded, the reference data is validated with a combination of scripts and the user interface to verify the accuracy in the reference data. Reference data changes/updates timelines will be provided to the State as part of DDI plan.

MAXIMUS will work with the MMIS and other State agencies as needed to get all the details needed for importing the initial Provider Enrollment Master File into the database. MAXIMUS has extensive

CONFIDENTIAL

CONFIDENTIAL

experience in converting Provider data from other systems. Our data analysts will validate the Master File from MMIS, working with the stakeholders to identify any discrepancies as we load. We will reuse many of the conversion routines that were developed for our other installations, but anticipate some customization required to implement the routines for MMIS. The conversion routines will be developed according to internally designed data mapping specifications that are based on the initial Provider enrollment file provided by MMIS. We will perform several iterations of the entire data load to validate there is no impact to the system due to data issues.

Our experience in converting data other state MMIS systems provides our team with a wealth of knowledge about how locally defined codes are used and how we can best convert non-standard data with minimal impacts across the enterprise.

Reference Tables Structure

MAXIMUS Provider Services solution has a well-defined data structure and data dictionary for the reference tables. Our base system includes all national code sets used within the Provider subsystem and additional reference tables based on our hands on. We have also implemented reference tables to support our business rules processing and our workflow configuration processes. Our reference data structure is designed to be simple and easy to understand with metadata for each table and what it is used for. The reference data structure will be available during the DDI phase and we will provide instructions on how the State can view the data as we are making updates. We will also include configurable ad hoc queries that will enable full data dumps of the reference tables for review. The data store can be updated quickly as we understand all the necessary details in the data sources provided by the State.

Each MAXIMUS Provider Services solution reference data table has the following main components as shown in *Exhibit 3.10.1.5-3: MAXIMUS Provider Services solution Reference Data Table Components*.

CONFIDENTIAL

Reference Data Modifications

Reference data is critical for business rule and workflow processing. In addition, many of the reference tables are incorporated into the rules engine. MAXIMUS provides a standard process for maintaining the information within the reference tables and ties reference table updates to system releases as required.

MAXIMUS Provider Services solution allows for modifications to reference data. Currently, access rights for reference data modifications is restricted to administrator roles. In most cases, our solution will not allow modifications to internal identification and external identification when source data is owned by an external entity or system. However, we do allow code table updates so that customized descriptions can be shown. Reference table changes are typically controlled through a screen that allows the administrator role to modify reference data that is not controlled by third parties or updated from national code sets. The reference data model updates have a validation mechanism to maintain reference data consistency. For example, if a user is trying to add a new taxonomy, the system presents an option to select application type, Provider category type and Provider type as dropdowns so that the user does not mistype information and add a Provider type that does not exist. There are also validations to verify a specialty/taxonomy is only added for existing Provider types. *Exhibit 3.10.1.5-4: MAXIMUS Provider Services solution Reference Data Update for Adding/Updating Taxonomies* provides an illustration of updating taxonomies in MAXIMUS Provider Services solution.

CONFIDENTIAL

MAXIMUS will implement all State-approved reference file changes in the system within State-approved timelines so that Providers are enrolled and identified correctly. Our process is to control updates to reference tables as part of a system release so that specific requirements, documentation, testing and sign off is included before we implement the changes. This also allows us to validate that no functionality is adversely affected by the update. We have found that reference data updates can have unanticipated consequences. For example, the seemingly simple change of setting the number of days before a revalidation is due from 60 to 45 could impact a large number of providers who may have already received notices or might even be in a revalidation workflow. We will work with DPHHS to determine how best to manage reference table updates to ensure limited impacts to providers in different workflows.

CONFIDENTIAL

Reference Data Integrity

MAXIMUS uses a standard set of ETL load processes to edit and store reference data. These processes are documented and specify the methods to edit and verify all data elements for completeness and consistency before the Provider Enrollment Master File and tables are updated. We have integrated consistency and accuracy verifications into the processes and we routinely use the processes in our other system implementation projects. All new reference data loads will be designed in the same manner. We also utilize our business team to manually check the data once loaded for an additional verification.

In the event our programs or staff finds any discrepancy in the data, we will notify the State within one (1) business day of identification of any discrepancies found with reference table updates. In addition, if we find data integrity issues in any of the Provider Enrollment Master File data, we will notify the State and all appropriate State-authorized personnel within twenty-four (24) hours of discovery of any errors in data integrity.

As part of BI platform, MAXIMUS will make available to users an online library of standardized or frequently used ad hoc queries and selection criteria that can be requested and run by authorized State staff and State-approved users. These can be used for verification purposes on any aspects of the MAXIMUS Provider Services solution data.

Provider Data

The MAXIMUS Provider Services solution database is made up of all data required to support Provider management within the Medicaid Program. We maintain comprehensive information on all Provider applicants and enrolled Providers including type of service information, relationship information between Providers, Provider groups, switch companies, billing agents and persons with ownership or management interest. Over the course of data conversion and system design, we will review the entire data model and verify it contains all required data fields used by DPHHS. We also include extensive data on practice locations, billing offices, correspondence addresses. Each address is geo-coded when stored using an industry standard postal verification service. We will verify the geo-coding as required by the State.

We have defined a data model that includes both the required data as well as date spans on enrollment data where necessary. This includes data such as Provider sanction indicators. As part of the design process, we will work closely with DPHHS to identify Provider enrollment data that must contain effective date spans and change dates. We typically find that much of this analysis occurs as part of the Data Conversion effort from the MMIS because we get to the specific business rules that must be supported during these activities. This information will be assessable from the application online. We will also implement a process that verify date-specific Provider demographic information and run it on a State-approved schedule.

Our automated workflow process guides the providers seamlessly through the application/registration process. Authorized user can save their application in any status and come back later for finishing the application. Our system also provides the capability to cancel the update at any time. The cancel functionality will discard any changes made in the current update and take the provider to their previous configuration.

As the project progresses and data continue to be added, MAXIMUS will implement data archiving processes. In the event an archived Provider must be restored, we will confirm the restore process has the ability to retrieve and restore online access of archived Provider records within twenty-four (24) hours of

request. In the event we identify any corrupt data or identify data loss, we will notify the State within one business day. In the event that repository processing deadlines will not be met, MAXIMUS will notify the State within agreed upon timeframes.

Data Storage and Access

MAXIMUS is using AWS storage solutions to host the data. Within the AWS infrastructure, there are different regions. We can specify the exact location we want our data to be hosted, that way the data will always reside within United States. Data will be accessible to authorized users inside the United States only. Data will not be accessible outside of the United States. Both AWS regions being used for the duration of this project are certified to be in the United State of.

Data Consolidation and Optimization

Having a clear strategy for managing, consolidating, and optimizing data is critical. Underestimating the complexity of data moves, the time it will take, the skills required to do the job, the hardware needed, is more the rule than the exception when it comes to relocation and consolidation. This is especially true when taking into account the complex application dependencies.

MAXIMUS understands that MMIS data is critically interrelated with the other MPATH modules, as a result we will perform detailed, comprehensive study to understand the current environment so that we can take a holistic view in design, improve and scale the data as business needs change.

We apply the expertise we've gained to design, construct, fully test, and integrate the database into the organization's business.

The MAXIMUS Provider Services solution is the single source of information for provider enrollment. Our system will be pre-populated with converted data from the legacy MMIS. Ongoing sources of information include the provider manual input, responses from OIG, MCSIS, SSDMF, SAM/EPLS, PECOS (manual and automated), NPPES and Medicaid IDs from MMIS. However, the system is considered the source of truth for all provider enrollment data. The MAXIMUS Provider Services solution is the source for providers to use to update their information, but manual updates are possible where needed. The providers can log onto a web-based portal and update their information in real time. The majority of the background searches are automated, requiring fewer staff to review and screen. This results in an accurate and more complete provider profile. MAXIMUS exposes well-defined service components via ESB to provide real time access to all transaction data.

MAXIMUS is using several performance optimization techniques like indexes, parameter sniffing, etc. to optimize system performance and queries at the database level. MAXIMUS uses Amazon EBS Storage for storing files on the EC2 instances. The storage is I/O optimized for database servers. AWS provides us with a services for monitoring performance optimization which calculates the cost which is generated due the unused or underutilized resources and recommends corrective actions. During the Implementation effort, we will carefully consider performance as part of testing and make updates as required to meet the performance service level agreements.

Data Management Requirements

The following table includes Attachment F Data Management Requirements, our summarized response to each requirement, and the section(s) in our proposal in which we provide our detailed response.

CONFIDENTIAL

ID	Data Management Requirement	MAXIMUS Summarized Response
DM04	The Contractor's solution shall maintain record/audit trail of errors during update processes, accounting for originating source and user.	MAXIMUS keeps an audit trail of all errors. The audit trail includes information about who made the change, when and where it is done, and the actual information added, changed, or deleted.
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.	[redacted]
DM10	The Contractor shall ensure that all narrative descriptions of codes and abbreviations are available for reporting.	MAXIMUS Provider Services solution has a well-defined data structure and data dictionary for the tables. Our base system includes all national code sets used within the Provider subsystem and additional reference tables based on our hands on experience in Tennessee, Nebraska, and the District of Columbia. We provide code tables with narrative descriptions of codes and abbreviations which are available 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.	Our system is hosted on MS SQL Server Enterprise and contains a data dictionary for the entire data store. We have the ability to report on the data module using any fields that are included in the design. We will work with the State to identify the exact format and provide the data model as necessary.
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.	MAXIMUS is using AWS storage solutions to have full backup and archiving capabilities. The two storage mechanisms we use in AWS are Amazon EBS and Amazon S3. All of the Amazon EBS storage is stored as snapshots in Amazon S3 and can be retrieved based on need. Data is retained for minimum 7 years or more depending upon the requirement. We can show the capabilities of these products as needed.
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.	MAXIMUS Provider Services solution repository stores complete electronic audit trail(s) of all changes made in the Provider Enrollment Master File and tables including but not limited to the type of change (update, add, delete, revert), user and date on which change was made.
DM15	For audit and reporting purposes, the system shall provide and maintain the following data for all reference codes: a. Effective date b. End date c. Date when last changed d. Who made last change e. Short description f. Long description	MAXIMUS has a well-defined data structure and data dictionary for the reference tables. We support all of these fields. See *Section 3.10.1.5.4–Application – Data Management / Reference File*, subsection *Reference Table Structure*.
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.	MAXIMUS will work with the State to understand and approve any updates to applicable codes and provide timelines that specify planned activities for the updates that will be submitted and approved by the State. For State supplied data, we will update all MAXIMUS Provider Services solution operational data store object descriptions and list of values within seven business days from the availability of the State-approved data source unless otherwise specified by the State. Reference table changes from existing sources are controlled and we build load processes to meet the data update requirements.

ID	Data Management Requirement	MAXIMUS Summarized Response
DM18	The Contractor's solution shall perform batch control including logging and reporting.	While most of the requirements are met through our real-time web portal and the ESB interface, MAXIMUS also has a robust Interface Scheduler Interface Scheduler for batch processing and reporting. The Interface Scheduler can be used to configure batch programs to run based on State's needs. The scheduler is currently used to schedule all kind jobs including of periodic reports, periodic processing, emails, paper mails, file transfer, etc. We use different logging for the various interfaces processes so enable restart and resubmission of data when errors occur.
DM19	The Contractor's solution shall archive all versions of reference information and update transactions.	Reference data and update transactions are part of the systems configuration management processes and are kept current by system release.
DM20	The Contractor's solution shall have the ability to void or reverse recent changes by rolling back to prior configurations.	All configuration and code changes are managed by our configuration management software. We have the ability to rollback application changes along with all associated support data and processes if a release has an issue or it is decided that the past version is correct. In addition, we also take data backup on a daily basis which enables us to restore the database to a specific period of time. The application also contains functions that enable providers to revert their changes using the cancel registration functionality. This option reverts any changes made by the provider in their application and take them back to the previous configuration. See *Section 3.10.1.5.4–Application – Data Management / Reference File*, subsection *Provider Data*.
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).	MAXIMUS managed data integrity at various levels. We implement system controls to tightly control data updates and ensure logging and audit trail. We develop specific data integration processes with user IDs and passwords to ensure only authorized sources can access data. We create secure platforms and specific folders when we transfer data in our out of the system. When the ESB is implemented we will use subscriptions to verify the appropriate source or consumer of the data. System edits validate both the transactions are correct in terms of format and processing edits verify the data is correct for the business process. We also use policy and procedures to ensure our staff understand and follow applicable policy related to different types of data.
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.	All of the data contained in MAXIMUS Provider Services solution is available online. Our system includes comprehensive search capabilities that enable Providers to be found using a variety of configurable search filters including many identification numbers. We will work with the DPHHS during the DDI period to identify the search criteria that is necessary and configure MAXIMUS Provider Services solution to use the appropriate search filters. MAXIMUS is packaged with pre-defined reports available to search information in audit trail.
DM23	The Contractor shall provide real-time access to transactional data for all module components	Our web interface displays the most current data stored in the application. We keep an audit trail of all actions (add, update, delete), including start and end time. Pre-defined or custom reports can be generated to validate and review the action history for timing.
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.	All MAXIMUS reporting information will be included in report definitions and/or design/technical specifications. The documentation will be comply with the most current version of MECT 2.x for specific documentation requirement. The State will have access to our specifications as needed.
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.	MAXIMUS will work with the state to identify all reports which are needed. Our configurable reporting tool provides users the option to choose from pre-built defined parameters to generate customized reports. We will create and maintain a suite of pre-defined reports for State and MAXIMUS use.

ID	Data Management Requirement	MAXIMUS Summarized Response
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.	The solution will be hosted at Amazon Web Services (AWS) cloud infrastructure in the United States. All of the MAXIMUS team is resident in the United States and no one outside of the country will access any data from this project.
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.	The system is integrated with the USPS address verification web service. All addresses entered into the system are verified in real-time through use of the USPS web service. As part of the address verification the Geo coordinates are captured for the address, which gives us the ability to present users with the GIS search option. See *Section 3.10.1.4.5–GIS Integration*.
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.	The MAXIMUS solution performs all data processing in real-time. While we do have load processes that are run from batch based on partner requirements, as updates are performed, the data is available immediately to all system uses and all online reporting processes. In our past implementations we have built data validation processes to ensure our system and the MMIS are in sync. Often times we have seen that the legacy vendor does not turn off access to provider updates and then can cause the systems to be out of sync. We will work with the State and other module partners to implement these processes.
DM38	The Contractor's solution shall optimize and consolidate data management storage.	Through our implementation in other states we have devised various techniques to optimize and consolidate data management storage. We use a centralized data store for all data storage and optimize data structures, indexes and stored procedures so we meet performance standards.
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.	The MAXIMUS solution will maintain all required data to meet the business requirements for the Provider Services module. After implementation of each module, seven (7) years of electronically imaged documents and data will be kept in that module. After seven (7) years, the data will be purged (deleted) from that module. All active records (active providers, 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.
DM40	The Contractor's solution shall maintain a normalized RDBMS with referential integrity and is optimized to meet performance requirements.	As part of the development of our solution, MAXIMUS created a data model that normalized how provider data was stored. We generally account for a provider a single time with relationships to various other data including group participation, practice location and other items. We utilize a relational database model built in Microsoft SQL Server Enterprise and enforce referential integrity between tables in the system for accurate data. We also integrate reference tables into the model with referential integrity to verify specific information reported by Providers and other MPATH modules is correct and accurate. We provide system functionality to support, maintain, and track these identifiers and their relationships to each other.
DM41	The Contractor's solution shall provide a method to access, query, and report against archived data external to the Operational Data Store (ODS).	As part of our Provider Services Solution, MAXIMUS is proposing to implement a data reporting platform supported by MicroStategy. The reporting platform will have automated capabilities to access, query and report on the production database and to create real-time items such as dashboards directly from the production data.

ID	Data Management Requirement	MAXIMUS Summarized Response
DM43	The Contractor shall demonstrate through data analysis that the implementation outcomes have been validated and are accurate.	Our solution can perform data analysis and validations at various levels. During the initial data conversion load, we use a combination of scripts and the user interface to verify the accuracy in the data. There are also validations to verify a specialty/taxonomy is only added for existing Provider types. Other validations are performed as and when user enters the data for example NPI, address, CLIA, etc. In addition to these methods, our reporting system will enable mass changes to be made and then reviewed at a consolidated manner. Our Rules Engine enables rules changes to be modeled against existing to determine impacts. Our team is also a big part of the data validation process. They understand what the data should look like and can quickly uncover potential issues.
DM45	The Contractor's solution shall maintain a history of provider information (i.e., full audit history or equivalent capabilities). All transactions, including the execution of database scripts, need to be recorded in the full audit history.	MAXIMUS has built a robust audit mechanism in our data repository. This audit trail data includes information about who made the change, when and where it is done, and the actual information added, changed, or deleted. See *Section 3.10.1.5.3– Audit Trail.*
DM46	The Contractor shall develop and maintain a process to archive and access archived data (including legacy MMIS component data).	MAXIMUS is using AWS storage solutions to have full backup and archiving capabilities for the current tables and the audit trail. Amazon S3 has different storage classes for that allows for archiving data with different options for access to archive, from a few minutes to several hours. During the DDI phase, we will work with the state to define the archiving and retrieval process.
DM47	The Contractor shall participate in ongoing data governance meetings as required by the Department.	MAXIMUS plans to work closely with the Department and Data Integrator as the ESB is implemented. We will have business and technology staff available to participate in ongoing data governance meetings and will provide lessons learned and best practices from our past projects.
DM51	The Contractor's solution shall provide the ability to modify transactions in real-time."	All of the provider data is stored and maintained by the system and updates are made real time. There is no limit to the types of changes that can be made but business edits will control how some features operate. Also all current transactions can be accessed by other modules through the ESB.
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.	The MAXIMUS solution has all the capabilities to create and consume web services from ESB that gives us the ability to quickly accept new data from module components. As module functions are implemented, we will create new ESB integrations to enable data sharing between systems.
DM53	The Contractor's solution shall provide an address type, effective dates, and the ability to select the type of address for provider mailings.	MAXIMUS captures various kinds of addresses including type during provider registration. MAXIMUS will work with DPHHS to define the address data needs. We will implement a user interface through our web portal that will allow providers to indicate which type of address should be used for mailings.
DM54	While the Department prefers real-time/event driven process, the Contractor shall provide a tool to easily administer and execute scheduled events (e.g. reports, file transfers, processes, notifications) to be performed on a regular basis (e.g. daily. weekly, monthly).	The MAXIMUS solution is focused on real-time updates and has limited batch processing. However, the MAXIMUS Provider Services solution Scheduler will be used to configure batch programs to run based on State's needs. The scheduler is currently used to schedule all kind jobs including of periodic reports, periodic processing, emails, paper mails, file transfer, etc. See *Section 3.10.1.6.7 –Scheduled Interface Processing,* subsection *Interface Scheduling.*
DM55	The Contractor shall provide a conceptual data model (CDM) that identifies the data elements required for an end-to-end business process execution including the identification of data standards that will reduce future rework to achieve successful data sharing across the enterprise and for intrastate/interstate exchanges. The CDM is required to be used as a reference to provide high-level overview of the data and relationships used by the enterprise and to provide a tool for ensuring the completeness of the business model.	MAXIMUS Provider Services solution has a well-defined data structure and data dictionary for the data elements. Our base system includes all national code sets used within the Provider subsystem. A full or simplified conceptual data model can of the current system can be provided on-demand.

ID	Data Management Requirement	MAXIMUS Summarized Response
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.	To provide interoperability with other systems, MAXIMUS exposes well-defined service components via ESB and is able to support data exchanges in any manner that an MPATH module prefers. See *Section 3.10.1.6.1–Interfaces with Other Applications*.
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.	MAXIMUS is using AWS storage solutions and data is retained for minimum 7 years or more depending upon the requirement. MAXIMUS will work with the state to provide a user interface for accessing the reports online.
DM60	The Contractor shall be responsible for data management including ensuring the architecture addresses data semantics, data harmonization, and shared-data ownership.	MAXIMUS supports data harmonization by bringing data together and storing in our database using national codes and standards. Our solution is the single source of information for provider enrollment. The system is pre-populated with converted data. Ongoing sources of information include the provider manual input, responses from OIG, MCSIS, SSDMF, SAM/EPLS, PECOS (manual), NPPES and Medicaid IDs from MMIS. The data will be shared with other MPATH modules via the ESB interface. We will provide a conceptual view of the system for other modules.
DM62	The Contractor's solution will ensure current and historical provider IDs are linked back to one universal/common identifier.	Provider identifiers are stored as information about a provider. Any number of identifiers can be stored for a provider. The MAXIMUS solution stores one universal ID for each provider record allowing any number of related records to be attached.
DM63	The Contractor's solution shall assign standardized unique internal identifiers for entities and prevent the creation of duplicate records.	The MAXIMUS Solution assigns unique internal identifier to each Provider. Duplicate entry is controlled during the creation of a Provider account. We control how Providers obtain accounts based on the capture of initial information about the Provider. At the onset of the project, we will define the data that constitutes a single Provider record and ensure that duplicate Providers cannot be stored in the MAXIMUS Provider Services solution.
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.	MAXIMUS is using AWS storage solutions to have full backup capabilities. These will be used on as-need basis to meet the project requirements.
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.	Reference data can be viewed and modified online. The data can also be sorted by column. MAXIMUS will work with DPHHS to customize search functionality on the reference tables. See *Section 3.10.1.5.4–Application*, subsection *Reference Table Structure*.
DM70	The Contractor's solution shall maintain user controlled parameters for all standards and messages.	Our solution utilizes on-demand configuration and centralized management. All messages and standards are thru parameters, mostly in the database and some in configuration files. Our requirements gathering process includes identification of configurable items while building new features. MAXIMUS will work with the System Integrator to identify the parameters that will be included in all standard messages.
DM71	The Contractor's solution shall verify that all dates are valid and reasonable.	All date fields entered through the user interface are validated. We will obtain a list of reasonable dates from DPHHS where applicable. The rules engine will be configured to validate those date ranges. Date validation will be executed on the conversion data to make sure all dates are in valid range. Cleansing of conversion data will happen to correct any anomalies. See *Section 3.10.2.5 Data Conversion, Cleansing and Migration*.

ID	Data Management Requirement	MAXIMUS Summarized Response
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).	MAXIMUS solution uses rules engine to define validation rules. These rules can be quickly changed by a business policy expert as needed. Data input validations will always occur on the server side before information is written to the database, thus avoiding vulnerability threats like cross-site scripting. Client-side validation scripts will also be used to improve the end user's data entry experience.
DM73	The Contractor's solution shall capture and maintain the data items needed for State or Federal reporting requirements.	Our solution has been developed to conform to Federal and State requirements for storing and accessing data. Our base configuration includes all CMS required data sources. In our solution the basis for the reporting functions is the database structures that store all information about the enrollment and screening process and a uniquely defined reporting layer that makes standard and ad hoc reports easy to create and maintain.
DM74	The Contractor's solution shall validate calculated data items.	MAXIMUS business rules for validation are defined in the rules engine and once they have been tested should always be correct. It provides onboard diagnostics tools to verify the changes before going live. For example rules are written to make sure 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, etc.
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.	The MAXIMUS solution provides a web interface which validates the input data. Identifiers such as NPI, CLIA number, etc. are validated for self-checking digits. Our solution is natively compliant with NPI and has an interface with NPPES to validate the NPI (when required).
DM79	The Contractor's solution shall support the Extract, Transform and Load (ETL) processes from real-time web services or batch processes.	The MAXIMUS Provider Services solution has pre-built Extract Transform, Load (ETL) programs to load data from different data sources. These can be configured based on State's needs. See *Section 3.10.2.5–Data Management*.
DM108	The Contractor's solution shall provide a configurable workflow process for resolving near matches for providers that can link, void or end date extraneous records (i.e., duplicate provider records).	Business rules executed within workflows edit data so that duplicate entry is not possible. Typically, providers enter the system multiple times and if they are able to add a new records issues are possible. In our solution, we build a set of business rules that define what constitutes a unique provider and we ensure that duplicates cannot be entered. Similarly, during data conversion we also run the data through these edits and create errors so that duplicate data is not loaded. However, we have found situations where states want the duplicate data converted and then linked. Our system contains functionality to void or end extraneous records. MAXIMUS will work with the state to define and allow near matches and come up with an algorithm to link, void or end date extraneous records if necessary.
DM115	The Contractor's solution shall collect, store, and maintain the data necessary for T-MSIS reporting as required by CMS.	Our system is considered to be the system of record for all provider enrollment data. We will convert all legacy MMIS provider data and collect data for new registrations. We anticipate making this data available to the data warehouse for T-MSIS reporting.
DM116	The Contractor's solution shall capture and maintain the provider related data items needed to support Payment Error Measurement (PERM) processing.	Our solution will convert all provider data provided by MMIS. New provides data (including eligibility) is captured through the provider enrollment process. Our solution has an established method to create and deliver Provider Enrollment Master Files or provide secure web-based services that allow Fee For Services (FFS) providers and Managed Care Organizations (MCO) to consume and provide specific Provider data. Once imported the data is maintained in our operational data store and can be accessed through various secure methods.

ID	Data Management Requirement	MAXIMUS Summarized Response
DM117	The Contractor's solution shall retain in the module, after implementation, seven (7) years of electronically imaged documents and data. After seven (7) years, the data will be purged (deleted) from that module. All active records (active providers, active members, active cases, etc.) and 100% of all history for any entity or case that has been active within the last seven years will be retained. Any entity and/or case that has been continuously inactive for the last seven years will not be retained, will be purged, and will no longer be accessible by users in that module.	Our operational data store hosted in Amazon AWS cloud maintains the active provider data. History of all entities (add, update, delete, view) is maintained through our audit trail. Our solution maintains status and history for all entities, we can easily determine whether a record have been active or not. The MAXIMUS Provider Services solution is capable of purging data from our solution and backups. Our solution has features to make documents obsolete to confirm to document retention policies and is integrated into our ECM component. Our solution's ECM component also has Records Management module to support the special access control, disposition, and retention needs for declared records throughout their entire life cycle.

3.10.1.6 Interfaces

3.10.1.6 Interfaces

This section addresses interface requirements for the Contractor's solution(s) and operations. The Contractor's Application Program Interfaces (APIs) and components must comply with industry standards (e.g., National Information Exchange Model (NIEM), National Institute of Standards and Technology (NIST) and HIPAA compliance standards). In the response, the Offeror must describe current methods of electronic data exchange, detail the industry standard formats currently used and describe any proprietary formats used. The Offer must also describe their approach to meet each of the interface requirements detailed in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution will provide ongoing support for the timely and accurate operation of all required interfaces for the State's provider solution implementation. We will accurately process and deliver 99.5 percent of the interfaces based on State-approved JIP. Our solution is capable of providing data synchronization interfaces across different internal and external data processes via ESB. Our ESB compliant framework allows connectivity to a variety of modern and legacy systems.

3.10.1.6.1 Interfaces with Other Applications

The MAXIMUS Provider Services solution will interface with MPATH modules and legacy systems to obtain Provider verification information and deliver updated, consolidated information regarding a Provider's enrollment in the Medicaid Program. The solution enables the synchronization of Provider data across internal and external data processes to maintain data relationships and integrity. We will adhere to State-approved interoperability requirements and provide an approved set of file transfer and data interoperability services that will allow secure access to the Provider Enrollment Master File and the Excluded Provider File. Our solution currently provides a variety of data exchange mechanisms including but not limited to:

- **ESB Interface -** Our solution can expose web services as SOAP, WSDL, REST, UDDI, ODATA, XML and JSON-WDP formats for clients and trading partners that are capable of consuming them. By using web services, our solution can be used to integrate with an ESB as a centralized integration engine.
- **Secure Web Service Calls** –Demonstrable capabilities to connect with systems like java, .NET, and native C++ SOAP client that are able to consume interoperable web services in a secure manner.

- **Trigger Tables** – When within a shared domain, MAXIMUS Provider Services solution can access or provide trigger tables with the request and response information to allow automated data transfers with older systems that do not use web services.
- **Secure File Transfer Protocol (FTP) and Batch Interfaces** – To cater to legacy mainframe systems and many other partner systems, MAXIMUS Provider Services solution contains a secure FTP site couple with a set of configurable batch interfaces that can automatically process inbound and outbound files using agreed upon file formats. We will process 100 percent of inbound files within the period defined by DPHHS.

As the project proceeds, the MAXIMUS Provider Services solution will continue to support all required file transfer protocols. However, we will continue to focus on supporting and implementing advanced interoperability functions and will help other application interfaces using a standard catalog of web services via ESB.

3.10.1.6.2MMIS Interface

Based on our experience, we understand that the interface with the MMIS will be the most critical interface that must be implemented. We have successfully implemented this interface in previous projects using mechanisms including flat file transfer via SFTP on the legacy MMIS system. In the District of Columbia, we interface with the Conduent MMIS and have experience with their system and how they like to structure these data sharing process. When MMIS is moved to the more modern system, the MAXIMUS Provider Services solution can quickly move to the new data exchange format. The MMIS Interface file definition is packaged with defined transactions using standard Provider data to exchange data with any State's MMIS. The MMIS Interface file definition includes transactions that allow for add new Provider, update Provider, terminate Provider, terminate with sanction reasons, add affiliate, and update affiliate. These transaction definitions are configurable and can be extended based on the need of the State.

Our solution also has the ability to send "emergency" transactions. These scenarios are available in cases where a Provider is found to be sanctioned and needs to be stopped from receiving payments immediately. The use of such transactions is dependent on the MMIS system and the ability to immediately process transactions that are sent. We will work closely with DPHHS and the MMIS vendor to implement a process that will work with the MMIS system.

In addition to the MMIS, Montana is exploring the ability to receive enrollments directly from the CMS Provider Enrollment, Chain, and Ownership System (PECOS). While we have not yet implemented an automated interface with this source, our Open Interface Framework will enable our solution to receive and process as file from the TIBCO Managed File Transfer Service or other comparable CMS data matching service. Given the complexity of editing inbound data and dealing with potential issues or data mismatches, MAXIMUS will spend extensive time during DDI to explore the best way to implement this function.

The MAXIMUS Provider Services solution has the ability to process transactions real-time and we provide critical data exchange delivery during agreed upon uptime 100 percent of the time.

3.10.1.6.3SOA Interfaces

MAXIMUS understands that the Provider Services module will have a SOA interface via the MPATH Enterprise Service Bus (ESB). In our Tennessee implementation, we have integrated using SOA based web services via the ESB. This became feasible due to our flexible SOA model. We can configure our SOA based services depending on the state's needs. For example, we can send a request to MMIS as soon as a new provider is approved in Provider Services solution. MAXIMUS will work with the System Integration vendor to follow the security guidelines for the SOA web services and will configure our web services with the appropriate security.

3.10.1.6.4Screening and Credentialing Interfaces

As described in *Section 3.10.2.5–Data Management*, the data extraction module is used to connect to a number of data sources for purposes of downloading data. When possible we download an entire verification source so that we have flexibility in how we process initial and on-going screening. The Screening module is configured to validate Provider information using both automated and manual methods. During Design, we will identify each screening source required by DPHHS and determine who owns the data, how we will access the data, and what keys are available in the data for matching purposes. These data sources are configured to be loaded in the system based on when they are updated by the source and in some instances (e.g., NPPES) a secure web service can be called real-time to validate Provider data during entry. *Exhibit 3.10.1.6-1: Verification Sources Used in the District of Columbia* shows the list of data sources that are currently used in District of Columbia implementation. Because of different State requirements, the complete list of screening sources tends to vary by State.

Database	Description	Method
OIG LEIE	Office of Inspector General List of Excluded Individuals and Entities	Automated
MED	Medicare Exclusion Database	Automated
SAM	System for Award Management, formerly the Excluded Parties List System (EPLS)	Automated
SSDMF	Social Security Death Master File	Automated
NPPES	National Plan and Provider Enumeration System	Automated
MCSIS	Medicaid and CHIP Information Sharing System	Automated
PECOS	Provider Enrollment, Chain, and Ownership System	Manual/Automated
SAVE	Systematic Alien Verification for Entitlements Program	Manual
License Verification	Search the State's License Database	Manual
Sexual Offender Registry	Search Sexual Offender Registry	Manual
DEA	DEA Verification	Manual
Controlled Substance Verification	Controlled Substance Verification	Manual

Exhibit 3.10.1.6-1: Verification Sources Used in the District of Columbia. *We identify the full list during design based on DPHHS requirements and configure each verification source based on how the data is accessed.*

Our preference is for all screening and credentialing sources to be automated. However, we are limited in some States where there is no available web service or file exchange to allow for automation. If, for

example, there is an available interface with the State's Licensure Board, MAXIMUS prefers to exchange data electronically. However, we are still able to include manual data sources in the screening workflow and require operations staff to perform the screening and record the results into our solution, which enables the workflows to continue as required. We store verification URLs for manual sites within MAXIMUS Provider Services solution to allow operations staff to directly access the site without having to look for the URL.

Access to CMS' Provider Enrollment, Chain, and Ownership System (PECOS) requires manual intervention in our current states. However, we understand that CMS is piloting data sharing process using TIBCO Managed File Transfer Service or other comparable CMS data matching service. We will work closely with DPHHS to implement this interface because of the processing benefits it offers. This key source is used for a variety of reasons including validating participation in Medicare, identifying if a site visit has already occurred for a related program, whether a fee has been paid or if a sanction or background check has negative results. We understand a modernization project has been initiated by CMS and we will implement an automated interface if it is available before the system design is finalized. We anticipate this process to be complex but our solution will handle both manual and automated processing as we implement this function.

In the same fashion that we are able to input data, we are also able to export information for sharing with other applications. We can specifically extract the data required for sources such as the Medicaid Fraud, Abuse Detection System or any other components of MPATH module and send it on a regular schedule using an approved format and file transfer mechanism.

3.10.1.6.5 Interfaces with Managed Care Organizations (MCOs)

The Montana Medicaid Enterprise is supported by a large number of Providers who perform both fee for service work as well as provide services for Managed Care Organizations (MCOs). The MAXIMUS Provider Services solution has an established method to create and deliver Provider Enrollment Master Files or provide secure web-based services that allow MCOs to consume and provide specific Provider data. In Tennessee, we receive MCO files that detail participation of Providers within the various MCO networks. This enables contract verification to occur on the Provider networks and the ability to use geo-location to verify Providers have adequate coverage in all service areas. We also provide data to the MCOs so they are able to confirm whether a Provider is enrolled in the Medicaid Program before they are contracted with. MAXIMUS will work with DPHHS and the contracted MCOs to develop a structure and interface control mechanisms that will enable two-way communications with the MCOs.

3.10.1.6.6 Interfaces with Credentialing Verification Organization (CVO)

While we understand that this project does not require an interface to a CVO, our solution has a proven interface to support this integration if the state decides to move forward at a later day. We provide the information as further evidence of the ability of our system to integrate with all provider partners as well as providing the state evidence of qualifications and expertise in making this connection.

The use of CVOs as part of the Medicaid Program is growing in popularity especially in states that are moving aggressively to Managed Care. In the MAXIMUS Provider Services solution installation for the State of Tennessee, MAXIMUS has implemented a 2-way interface with Council for Affordable Quality Healthcare (CAQH). CAQH is responsible for credentialing individual Providers and accepting

applications, which are then forwarded automatically to TennCare for inclusion in the Medicaid Program. MAXIMUS understands how CVO data is collected and where deficiencies in editing must be addressed. We currently interface with CAQH in XML as well as flat file formats and we will tailor our solution to work with the CVO in Montana. Our provider services solution is driven by the Corticon rules engine that makes the configuration changes easy and error free. Since the business logic is transparent and defined in user readable format.

Our process includes an outbound file to initiate the application process and inbound files that load the full Provider record from the CVO into the MAXIMUS Provider Services solution database. The interface program has rules and edits to verify all the required data is present and because Medicaid rules are strict, we have had to implement an entire editing and exception process before we are able to load the CVO data. In the case of missing information, the system generates an email that is sent to the Provider to return to the CAQH portal and enter the missing information.

We process update transactions for Providers that have already been loaded into the system. Data ownership is a critical piece of this process. We will work with DPHHS and the CVO to build data ownership and update rules based on who owns particular data. Our extensive experience in working with CAQH can be leveraged to interface with the CVO selected by the State.

3.10.1.6.7 Scheduled Interface Processing

Interface processing is comprised of a variety of scheduled processes that include approved file transfer mechanisms run on an approved schedule. We will receive, process, and retain Provider data from State-authorized sources and use the data as required in the larger Provider enrollment and screening process.

Interface Scheduling

MAXIMUS Provider Services solution interfaces can be processed on various schedules including multiple times throughout a day, daily, or a specific day of the week. In addition, we are able to expose web services that can be accessed real-time platform to reduce the need for bulk data transfers. Through collaboration with the State and other applications, our team will review existing, external interfaces to determine the schedule of interface jobs. During design, we will identify each interface, specify the interface control document and specifications for processing and agree to an execution schedule and transfer protocol type. We will then configure the batch schedule to execute the processes on the schedule approved by DPHHS.

The interface data can be delivered via secure web services, encrypted email, SFTP, or FTP. MAXIMUS utilizes an automated windows service, which executes any pending jobs or processes. The notifications are generated when an exception occurs, allowing staff to intervene and take corrective actions. This automated notification process allows users of the MAXIMUS products to offer pre-emptive service to end users instead of waiting for users to escalate to MAXIMUS staff when a problem has occurred.

Interface batch jobs are scheduled by populating tables that contain the job information. The information includes items such as job name, schedule, type, description, and needed parameters. The job service allows the following job types: SQL, Stored Procedures, Views, Send, or Receiving files via SFTP/FTP, .NET interfaces, and Web Services. This flexible design allows us to provide a wide variety of outputs for the State on configurable schedules to meet internal and external needs. *Exhibit 3.10.1.6-2: Job Scheduler* shows the job scheduler model created in our solution.

CONFIDENTIAL

Our solution reports on the pre-defined transactions to make sure the processing dates and the number of successful and failed transactions are accounted for in each interface run. Automated alerts are generated on each interface run to bring attention to issues; including processed and failed transactions.

3.10.1.6.8 Interface Exception Processing

The MAXIMUS Provider Services solution has an error-handling module that provides a mechanism for exceptions, which occur during processing of interfaces transactions. These exception processes are directly integrated with each interface process so that we are able to either restart an extract process or process another inbound transaction completely while identifying any issues with inbound data. Error codes and descriptions along with their categories are available as reference data. This allows for reporting and notifications when rules have been violated. The system also has error 'override' capabilities available to certain user roles that can be used in specific situations. Each interface process is designed to complete processing while ensuring all errors are accounted for and missing data can be resent or reloaded.

3.10.1.6.9 Interface Maintenance and Operations

The MAXIMUS Provider Services solution has been developed to conform to Federal and State requirements for accessing verification data. Our base configuration includes all CMS required data sources and our ESB integrated Framework enables the quick and efficient implementation of any new interfaces.

Through our implementation with other states, MAXIMUS understands that accurate interfaces is one of the most important aspects of the system. Through collaboration with the State and other stakeholders in the State's healthcare programs enterprise, our team will review existing external interfaces, we will identify each interface, specify the interface control document and specifications for processing. The ICD

CONFIDENTIAL

will include documentation of the data layout, inbound/outbound capability. Our configurable Interface Scheduler can be easily configured to match the frequency of all interfaces. We will analyze our existing data layout and modify/add based upon the new requirements and then we will define the data mapping crosswalk.

All interface code, data models and documentation will be maintained by MAXIMUS.

We will report all data extract problems. For any problems that can be corrected automatically through inference or transformation, we will resolve them in the exchange of data to maintain data relationships and integrity. Our solution will provide the ability to fix data that requires manual correction; and we understand that we are not responsible for any manual correction of corrupt or missing data from MPATH Systems Integration Services Contractor.

3.10.1.6.10 Interfaces Requirements

The following table includes Attachment F–Interfaces Requirements and our summarized response to each requirement.

ID	Interfaces Requirement	MAXIMUS Summarized Response
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)).	Our modular architecture is designed to share data with other systems. Through internal business rules or in partnership with other system modules, MAXIMUS is able to adhere to the set of national standards including HIPAA, NIST, NIEM, HL7 and FHIR requirements. We incorporate advanced tools that enable data exchange with a variety of modules using an open interface platform.
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 MAXIMUS interface design allows connectivity to a variety of modern and legacy systems. This makes our solution capable of providing data synchronization interfaces across different internal and external systems. Through collaboration with the MPATH Integration Module, MAXIMUS will provide an automated, secure, audited and scheduled method for transferring interface files internally within the system and externally with other modules and meet the requirements of Department policy, and federal and State rules and regulations. We will support the variety of interface methods necessary by the various data partners.
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.	The system uses an ESB integrated interface Framework that allows us to send receive real-time transactions based on file triggers or web service calls to reduce the need for bulk data transfers. We anticipate working closely with DPHHS and the System Integrator to determine when and how each real-time interface will occur.
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.	To cater to legacy mainframe systems and other MPATH modules, our solution contains a secure FTP site coupled with a set of configurable batch interfaces that can automatically process inbound and outbound files using agreed upon file formats. The files are stored on NFS storage from an IBM V7000 Unified running on RAID 5 encrypted disks. We will verify a role based interface exists to provide an electronic copy of all files based upon state's requirements. We currently keep an unlimited amount of files but will work with DPHHS to implement the retainage schedule.
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.	To cater to legacy mainframe systems and other MPATH modules, our solution contains a secure FTP site coupled with a set of configurable batch interfaces that can automatically process inbound and outbound files using agreed upon file formats. The files are stored on NFS storage from an IBM V7000 Unified running on RAID 5 encrypted disks. We will verify a role based interface exists to provide an electronic copy of all files based upon state's requirements. We currently keep an unlimited amount of files but will work with DPHHS to implement the retainage schedule.

ID	Interfaces Requirement	MAXIMUS Summarized Response
INR07	The Contractor shall document all interfaces in an Interface Control Document (ICD) which will include data layout documentation, data mapping crosswalk, inbound/outbound capability and frequency of all interfaces.	MAXIMUS will work with DPHHS and other State agencies to develop a structure or interface control document. During design, we will identify each interface, specify the interface control document and specifications for processing and agree to an execution schedule and transfer protocol type.
INR08	The Contractor's solution shall include a process and toolset to maintain interfaces, code, and data models.	We perform all development functions using Visual Studio as our Integrated Development Environment. SQL Server Enterprise has an integrated toolset to support data model development and maintenance. All source code is kept within our configuration management tools together we maintain interfaces code and data models.
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.	MAXIMUS will work with DPHHS and other stakeholders to develop a structure or interface control document. During design, each interface will be identified, the processing specified and the timeframe and transfer protocol agreed to. All of this will be documented in the ICD.
INR12	The Contractor shall ensure proprietary interfaces and protocols between modules are not used.	Our system integrates and interoperates with other State systems using a variety of interface mechanisms including web-services, flat files and other transfer mechanisms used by our trading partners. In addition to SOAP and WSDL for WS-* compliance, our solution can also expose web services as REST, UDDI, ODATA and JSON-WDP formats for clients and trading partners that are capable of consuming them. By using web services, our solution can be used to integrate with an ESB as a centralized integration engine. We do not use proprietary interfaces and protocols. We do not use proprietary interfaces or protocols although we will leverage the existing interfaces we have implemented for other customers as a starting point for Montana.

3.10.1.7 Business Rule

> 3.10.1.7 Business Rule
>
> This section addresses Business Rule requirements for the Contractor's solution(s) and operations. The Contractor shall describe the proposed solution's capacity to configure, support and maintain business rules (i.e., add, modify, or remove/retire rules) and the type of resource and necessary skill set(s) required for business rule configuration. Describe the change management processes associated with business rule configuration. In addition, the Offeror must describe their approach to meet each of the Business Rules requirements detailed in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution architecture adheres to MITA principles by incorporating Progress Corticon; a widely used business rules engine (BRE). Corticon is a fully functional BRE that contains industry standard functions to author, test, debug, and deploy business rules. MAXIMUS evaluated different rules engines looking at functions, features, and integration methods for our application. We choose Corticon because it offers a cost effective solution built with flexibility on how we implement various features.

The Progress Corticon BRE has been successfully implemented by many states as the business rules engine of choice for varied application scenarios. The following table provides additional justification for our use of Corticon as part of the MAXIMUS Provider Services Solution.

Components	Description
Support for Shared Services	Our goal is to create a rule and use the rule in different scenarios. Progress Corticon allowed us to create rules and expose rules as web services. For Provider Services module, providing rules as services, we are able to build a robust set of shared services that are changeable based on rules in the rules engine. These shared services are used across the solution and can also be exposed for 3rd party applications to consume. Thus, we are able to build SOA based shared services for business rules.
Enhanced Control	Progress Corticon rules are simple to design with easy to use interface and allows for subject matter experts to write, test and implement new rules and rule changes. It provided us onboard diagnostics tools to verify the changes before going live.
Timeliness of Service Delivery	In addition to enhanced control to create rules, Corticon provides a faster way to promote rules to production environments. This allows us to deliver faster changes to business rules without having the need to execute an entire software development life cycle.

3.10.1.7.1 Rule Language and Rule Modelling

To create rules that are easily understandable and human readable, MAXIMUS has put extensive effort into creating a vocabulary set. This vocabulary is the building blocks with which business rules are implemented. Provider Services vocabulary consists of various entities, their attributes and their relationships to other entities. On the vocabulary, when developing the rules, MAXIMUS added natural language text annotations to the rule conditions. It allows for DPHHS department resources and subject matter experts to create, configure and maintain rules in a user friendly graphical user interface. This allows for subject matter experts or technical resources to write natural language business rules. The rules engine allows for exporting the business rules for creating Business Rules catalog in html format. This allows for creating a documentation of all the rules as changes are made to the rules.

CONFIDENTIAL

MAXIMUS has tested the individual rules with built-in rule testing mechanisms. As we built our rule base, we are able to create rule tests and test the rules by doing scenario based testing. We created rule tests to test specific scenarios. These rule tests are stored as tests long with the rule base. We are able to test and re-test our scenarios as we change rules over the course of time. The rule tests serves as unit testing for the rules so we can evaluate the existing scenario changes and catch any missing conditions as part of rule design and rule changes. Our rules engine also provides tools to debug a rule set at design time. We have successfully used the scenario cases to emulate production data to perform what if testing and compare before and after outcomes. We are able to use our business rules engine to get data from different data sources to test database that has production data to validate the rules.

The rule sets are combined to create a rule flow that allows for conditional branching based on parameters applicable. In *Exhibit 3.10.1.7-2: MAXIMUS BRE Rules to Check for Provider Site Visit*, we are showing a rule flow that checks if a provider is a new provider and has a high- risk level, perform background check process. The rule can be modified based on specific implementation. One of the changes we made to this rule is that even if the provider is doing an update, if he changes the location, the outcome is that we need to perform site visit.

CONFIDENTIAL

CONFIDENTIAL

3.10.1.7.2 Rule Orchestration and Decision Services

We used rule dependency graphs in our rules engine to prioritize, sequence and allow administrators to control the processing of the rules. This allows to identify the sequencing and prioritize the rules and to control processing of the rules. These graphs are also used to know how one or more attributes are used in a rule flow.

We exposed all the business rules as interoperable SOAP API and created shared services in our application layer. By integrating the Provider Services module with the rules engine, we gained tremendous flexibility on orchestrating business rules. We created decision services that orchestrate as part of Provider Services module. The business process engine consumes decision services as part of specific business process. For example, when a new application is submitted by the provider, our business process engine executes a step to calculate the risk level for a provider. The calculation of risk level has a logic on which we determine if the provider needs to be assigned Low, Medium or High risk level. This is created as decision service that internally executes a rule flow to determine the provider risk level. The decision service takes into consideration various parameters that constitutes a provider and passes it on to the rule. The rule can be changed to take into different parameters into consideration based on state's needs. One of the notable requirement changes in one of our Provider Services implementations was to factor Provider specialties, in addition to the Provider types, when determining the risk level for a Waiver Provider. We were able to quickly modify the rules to include specialty as a Risk level parameter for the waiver Providers.

Another notable use of decision services is supporting data collected on all Providers like practice locations. We have experience implementing different models that are used to identify Providers, some of which use location as part of the uniqueness validation and require a provider number for each location. Using decision services, our solution can be configured to change the definition of how a unique Provider is defined. In the Tennessee implementation, Providers are identified using a Tax ID and NPI combination. We collect primary practice location for the Provider and store additional locations as secondary / satellite locations. In this model, Providers are able to add an unlimited number of satellite practice locations based on the Tax ID and NPI and there is no restriction on the number of satellite

CONFIDENTIAL

locations. In the model used by the District of Columbia and Nebraska, a unique Provider is defined by NPI, Provider Type, Taxonomy and Zip Code+4 combination so location is used to define a Provider for these programs. We have successfully implemented both models and during requirements validation, we will work with DPHHS to define what constitutes a unique Provider, analyze how the MMIS stores and enumerates Providers, and configure the business rules based on the outcome of this analysis.

Business Rule Requirements

The following table includes Attachment F–Business Rule Requirements and our summarized response to each requirement.

ID	Business Rule Requirement	MAXIMUS Summarized Response
BR01	The Contractor shall configure, support and maintain a business rules engine (e.g., add, modify, or remove/retire rules) based on the Service Architecture (SOA).	The MAXIMUS business rules engine allows for configuring, supporting and maintaining in a SOA based architecture.
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.	Rules in our BRE are easily understandable and human readable. Our BRE also has a GUI that is user friendly. It allows for DPHHS department resources and subject matter experts to create, configure and maintain rules without making 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.	All rules tied to a system release are kept together in a rules catalog. Our BRE provides functions to export rules in various electronic formats. MAXIMUS can provide the catalog in real time to DPHHS
BR04	The Contractor shall update the Business Rules Catalog with all additions or changes.	As our business rules catalog is exportable from rules engine by the click of a button, any additions or changes to the rules are updated immediately.
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.	MAXIMUS will integrate business rules engine into testing environment that contains production data to allow users to perform what if testing. We have development licenses to use our BRE in development, test, UAT and production so we can perform a variety of tests before we implement new rules.
BR06	The Contractor's Business Rules Catalog shall include granular check-out and check-in rules and an audit trail of business rules changes.	Our BRE rules are stored as flat files in source control. This allows for check-in, check-out and audit trail of changes to business rules using the standard source control procedures.
BR08	The Business Rules Engine shall allow changes to be made to valid values without impacting production rules engine availability and operations.	MAXIMUS BRE rules are changed in the test environment first. After testing the rules, the rules will be promoted to production environment. Rules can be changed but until they are approved they don't go live. Thus, the changes to rules will not be impacting production rules engine availability and operations.
BR09	The Business Rules Engine shall include the ability to debug business rules at rule execution.	Our BRE has features to debug business rules at rule execution.
BR10	The Contractor shall provide the ability to allow multiple users to work concurrently on different parts of the same rule base.	Our BRE allows for multiple users to work concurrently on different parts of the same rule base.
BR11	The Business Rules Engine shall have the ability to rollback to prior versions of rules without impacting production rules engine availability and operations.	Our BRE rules are stored as flat files in source control. This allows for auditing and rollback to prior versions of rules without impacting production rules engine availability and operations.
BR12	The Contractor shall provide and maintain a graphical representation of business rule flow(s) and orchestration for all business rules.	Our BRE provides a graphical representation of business rule flows for all business rules.

ID	Business Rule Requirement	MAXIMUS Summarized Response
BR13	The Business Rules Engine shall have mechanisms to identify which rules are executed for each specific business process.	For each specific business process, there is a graphical representation that shows what rules constitute the business process. This way, one can identify the rules that are executed for each specific business process.
BR14	The Business Rules Engine shall be able to produce a report on rules passed or failed for all transactions.	MAXIMUS has built-in mechanism to log the rules that get executed for each transactions. This logging will have the result (pass or fail) of the rule that is executed.
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.	Our BRE provides alerts at different times during the rule processing. At design time, it has the ability to identify conflicts in rules. These conflicts are alerted to the user so they can modify the rules. Also, when rules are being built to orchestrate, the dependency graph shows alerts if the rule inputs are not matching. We also enable enterprise-wide monitoring using AppDynamics to support alerts based on failures within a production environment.
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).	Our BRE allows for annotating rules with natural language and show rules in human readable format.
BR17	The Business Rules Engine shall provide the ability to prioritize, sequence, and allow administrators to control processing.	Our BRE provides dependency graphs to allow for prioritization, sequencing, and controlling of processing.
BR20	Where applicable, the business rules engine shall use standardized business rules definitions.	Our BRE uses standardized rule definitions for all rules.
BR21	The Contractor's business rules shall execute in a runtime environment.	Our BRE runs in a runtime and all the rules are executed in a runtime.

3.10.1.8 Enterprise Content Management

> 3.10.1.8 Enterprise Content Management
>
> This section addresses Enterprise Content Management requirements for the Contractor's solution(s) and operations. The MPATH Integration Platform will include a centralized enterprise content management solution. The Contractor's solution will be required to send all documentation to the MPATH Integration Platform for storage in the centralized enterprise content management solution. The Contractor shall describe the proposed solution's capacity to configure, support and maintain an enterprise content management solution and the type of resource and necessary skill set(s) required for enterprise content management and configuration. Describe the change management processes associated with enterprise content management. In addition, the Offeror must describe their approach to meet each of the Enterprise Content Management requirements detailed in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution contains content management capabilities based on Hyland OnBase. OnBase is recognized as a market leader in enterprise content management (ECM). MAXIMUS has deployed Hyland OnBase in our Nebraska and District of Columbia implementations for all paper applications, documents, and attachments uploaded by Providers during the enrollment process and all converted documents that come along with conversion of providers. Our integrated solution contains a paper entry component and system integration directly with the web-portal to receive and display electronically uploaded documents.

OnBase provides a suite of products and features out of the box with easy configurability and customizability. It comes as a modular application, to which we can add modules as needed, thus offering us an effective way of adding features to the overall solution. It also enables customers to build a solution with only those functions being used to save cost and time. Our solution incorporates the imaging, document management, workflow, and business process management modules. The ECM provides several collaboration features across different devices through its web and html client. It also has mobile apps for iOS and Android. The ECM component has robust role based security features that comes out of the box. It provides granular access to various features by explicit and detailed authorization access for

CONFIDENTIAL

each role. This is essentially a matrix of document type to role/user group. Revision management is built into our ECM component at its core. For editable documents like MS Word, documents are checked out, revised, and checked back in as a new version automatically for those with the proper permissions. For Image documents, if a newer version is received, the system can be configured to insert the new version as a 'revision'. The most current revision is always displayed when the document is accessed, however, a visual identifier is show to alert the user than the document has older versions.

Our integrated ECM component allows users to create custom indexes and metadata for the documents and provides user-friendly user interface to associate metadata with documents. In our implementation, provider documents are indexed but show directly within the Provider Management module. Providers are able to see only documents they uploaded, internal users and administrators can see all documents and can upload additional items during enrollment or screening.

OnBase is directly integrated into the provider enrollment process. Depending on the specific State, providers may needs to submit Documents and attachments (for example, proof of License) during the enrollment process. As providers initiate an upload to Provider Services solution, our solution calls APIs to upload the documents to ECM. MAXIMUS ensures these documents are encrypted as part of upload. On a successful upload, our solution adds a number of metadata elements to that uploaded document including but not limited to NPI, document types such as liability insurance, Provider Id, etc. As providers submit the applications for review, our solution presents all of the uploaded documents with the provider record for the screener to validate.

During the conversion process, MAXIMUS will convert related provider documents into the ECM. Our solution will link these documents to the provider record. This enables system users to access all Provider documentation within the Provider record or to search, retrieve and view Provider enrollment documentation with functions that connect to the document repository included with Provider Services Solution. Documents can be viewed or printed as needed.

CONFIDENTIAL

CONFIDENTIAL

Conversion documents and documents uploaded internally are only viewable by staff authorized to access the specific web page where the document was uploaded. This control mechanism confirms that users that cannot access the web page are also not able to access the document. During JAD sessions, we will meet with DPHHS to discuss the specific confidentiality requirements for specific documents. We will then implement a scheme that matches State requirements as well as meet federal security requirements.

Paper Applications Processing

Our Provider Services solution supports the scanning and indexing of paper enrollment forms and stores them in a document repository. Our solution includes integrated workflow for paper application processing. The ECM software can be configured to work with a variety of scanners and supports integrations with scanning solutions. Our solution works with a variety of scanners. The ECM supports ad-hoc and batch scanning. The ECM workflow consists of a user interface that will allow the internal operator to index the documents with all the necessary information. The uploaded paper applications are reviewed by operations after indexing. The ECM workflow can be configured to add additional steps as needed. All paper documents submitted by Providers are time-stamped, stored in the imaging and document repository, and linked to the Provider's enrollment profile for the entire lifetime of the Provider in Provider Services solution. *Exhibit 3.10.1.8-2: MAXIMUS Provider Services ECM Integration* shows the result of a scanned document.

The ECM workflow transfers the approved metadata from the paper to the Provider Services module. This initiates the process of the electronic entry and review of data submitted in a paper application, as shown in *Exhibit 3.10.1.8-3: Review and Entry of Paper Application Data*. The paper application data also goes through the solution's error processing sub-module. After an application is successfully entered, paper applications and electronic applications follow the same workflow.

CONFIDENTIAL

CONFIDENTIAL

ECM Requirements

The following table includes Attachment F–ECM Requirements and our summarized response to each requirement.

ID	ECM Requirement	MAXIMUS Summarized Response
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.	Our ECM component supports all common file types and can be integrated seamlessly with common document viewing and editing tools. Documents can also be rendered into other formats if needed.

CONFIDENTIAL

ID	ECM Requirement	MAXIMUS Summarized Response
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.	Our Provider Services Solution integrates directly with our ECM so that no external platform is needed and documents are automatically connected to the appropriate provider record. We do not envision directly access to documents through the ECM, but our ECM includes web client is based on html 5 and accessible across (desktop, web, and mobile) platforms. Additionally, it has a native mobile application for an even richer experience if desired. It provides viewers for image and text files but requires a viewer be available for other common file types. Alternatively, it can be configured to convert various file formats into Image or PDF if desired.
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."	We integrate access to documents using the Provider Services web portal where role-based security governs what data can be seen. We anticipate using these controls for the project. However, our solution's ECM integration provides role based security for the users. The ECM integration allows for seeing only the documents that belong to a provider in a granular way for preview and access. There are options to make the documents obsolete as deemed by the department.
ECM05	The Contractor's ECM solution must include a flexible search engine, including document and content search capabilities.	We are proposing to integrate our ECM with our Provider Services Solution so that we can take advantage of the role-based security and automated workflows contained in the system. We do not envision documents being accessed directly from the ECM because they don't have the same content as they would within the solution. However, our solution's ECM component has flexible search based on the indexes available. Searches can be as elaborate as desired adding any time constraints (before, after or between two periods) where specific keywords equal certain values (can use wild cards) and can combine values with clauses such as AND, OR, or greater or less than. Our solution's ECM component also has a full text module allowing for searching by documents by their content versus its indexing.
ECM06	The Contractor's ECM solution must allow users to associate metadata with documents.	Our solution's ECM Component allows for associating metadata to the documents. This is generally done to support paper processing. Electronic uploads are automatically indexed with a preset of metadata by the application.
ECM07	The Contractor's ECM solution must support simple integration with scanning solutions (support for bulk-scanning).	Our solution's ECM component supports ad-hoc and batch (bulk) scanning. Bulk Scanning is licensed per workstation since it must be connected to a scanner. A variety of scanner hardware can be used.
ECM08	The Contractor's ECM solution must support version control.	Revision management is built into the ECM component at its core. For editable documents like MS Word, documents are checked out, revised and checked back in as a new version automatically for those with the proper permissions. For Image documents, if a newer version is received, the system can be configured to insert the new version as a 'revision'. The most current revision is always displayed when the document is accessed however a visual identifier is show to alert the user than the document has older versions.
ECM09	The Contractor's ECM solution must be configurable to comply with the Department's document retention policies.	Our solution has features to make documents obsolete to confirm to document retention policies, this is integrated into our ECM component. Our solution's ECM component also has Records Management module to support the special access control, disposition, and retention needs for declared records throughout their entire life cycle.
ECM10	"The Contractor's ECM solution must support document workflows with review/approval ability with digital signature support	Our solution's ECM component has a module for workflow and an integration with DocuSign for electronic signatures. We are not currently planning to implement digital signature given the nature of the documents being uploaded. The correspondence management solution will support out going documents.
ECM11	The Contractor's ECM solution must scan all uploaded documents for viruses prior to storage.	All our documents are stored on a file system via our ECM component and are covered by virus software on the server.

ID	ECM Requirement	MAXIMUS Summarized Response
ECM12	The Contractor's solution shall be able to index, link and display incoming correspondence or uploaded documentation with the entity record.	Our solution has all the correspondence stored along with the provider information. It is indexed, linked and is displayed along with the provider record automatically.
ECM13	The Contractor's solution shall send all documentation to the Systems Integration Services module for storage in the centralized ECM.	MAXIMUS will work with System Integration Services vendor and centralized ECM vendor on the APIs that are needed to send all documentation to the centralized ECM. We are able to send index files and the images as required.
ECM14	The Contractor's solution shall have an integrated electronic document management solution to meet the business needs of the State's enterprise.	MAXIMUS Provider Services solution is integrated with Hyland OnBase, to meet the business needs of the state's enterprise.
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).	Our solution is designed to store all the documents in ECM as the documents are uploaded into the system. All we need is metadata, index fields and the image.
ECM16	The Contractor will configure, support and maintain Enterprise Content Management (ECM) functionality (including Document Management and Workflow) to meet the business needs of the State's enterprise.	The MAXIMUS solution is configured for ECM functionality (including Document Management and Workflow) to meet the business needs of the State's enterprise. We will support and maintain this EMC functionality throughout the contract.

3.10.1.9 Workflow

> 3.10.1.9 Workflow
>
> This section addresses Workflow requirements for the Contractor's solution(s) and operations. The MPATH Integration Platform will exchange data with all MPATH components to support enterprise wide automated business process orchestration. The Contractor's solution shall include a configurable workflow solution for process definition, execution, monitoring, and management. The Contractor shall describe the proposed solution's capacity to configure, support and maintain a workflow solution (i.e., add, modify, or remove/retire existing workflow configurations) and the type of resource and necessary skill set(s) required for workflow management. Describe the change management processes associated with workflow management. In addition, the Offeror must describe their approach to meet each of the Workflow requirements detailed in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution's business process framework is referred to as the Business Process Engine (BPE). The BPE automatically executes the appropriate business process model based on the inputs from the business rules engine. MAXIMUS designed and developed the Business Process Engine as part of the initial deveopment of our solution. We have successfully implemented and configured our solution in Tennessee, Nebraska and the Distict of Columbia and bring to the Provider Services module project a large library of business workflows that can be used as the basis for Montana to save time and effort.

During the system design, MAXIMUS will work DPHHS in defining automated workflows for all or most of their processes. All workflows are discussed and mapped out to manual and automated processes that must occur and the workflows are then assigned to user types and application processes. The results of the design are configured within the rules engine so as workflows are dynamically created based on data or user actions, the workflows are presented to complete required tasks. We have found that the definition of state specific workflows requires the most time to understand and effort to configure of any

particular activity in the implementation project. For this reason, we take a lot of time to review these to get them right the first time.

3.10.1.9.1Workflow Definition Tool

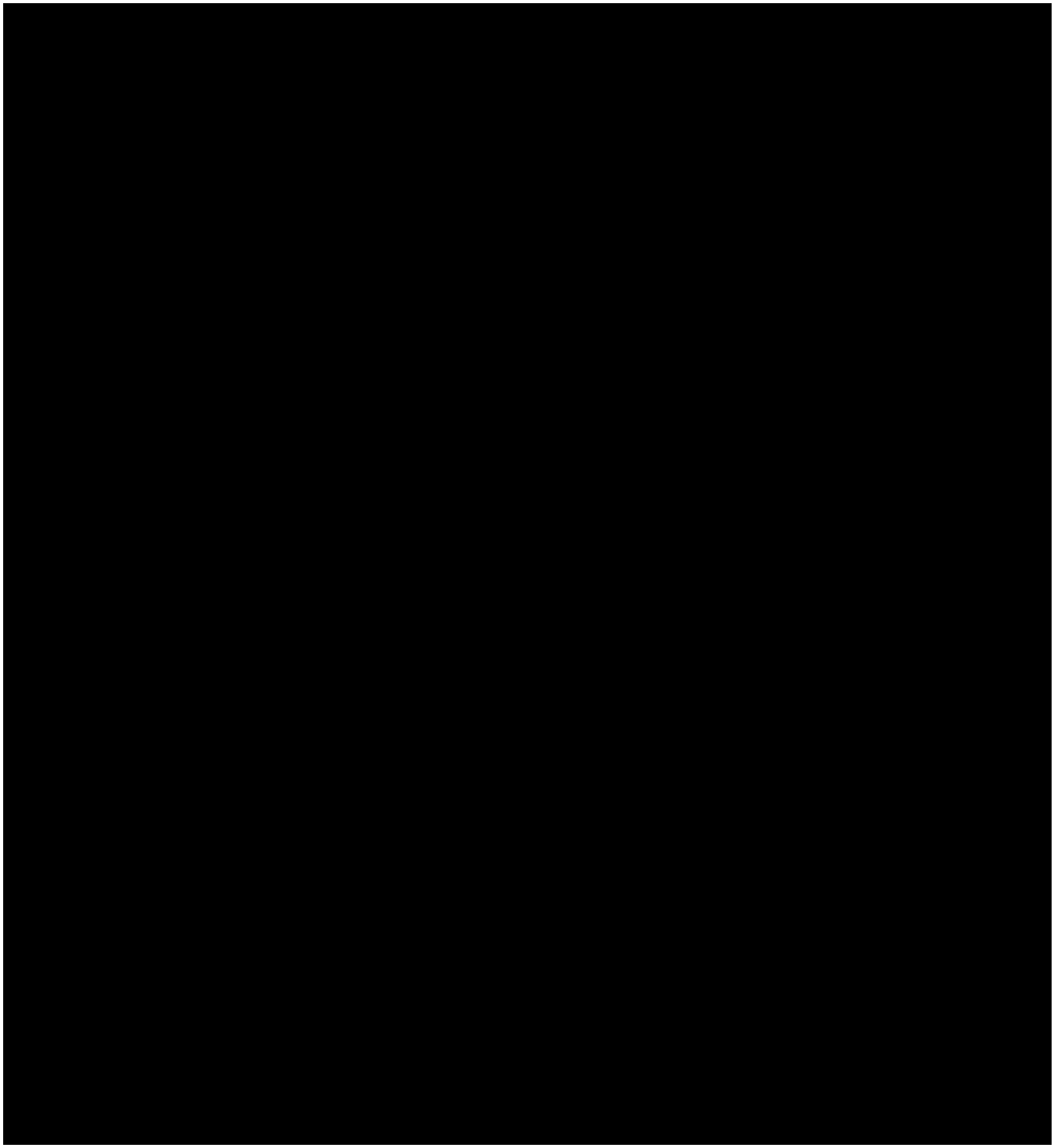
Although all most workflows will be defined during the design effort, there is always a need to modify existing workflows or create new ones. Our solution provides a role-based Graphical User Interface (GUI) for process definition that leads the user through the steps of defining the workflow associated with a business process. The user can choose a trigger for the workflow which will start the workflow, the trigger can be a scheduled event, API call or user interaction (forms). User can define tasks for the workflow, the tasks can be either manual user driven tasks or automatic system tasks. The tasks can be parameterized, user can select these parameters from a predefined values. Also, they can select roles for the tasks, which roles or specific should be performing the tasks. For example manual screening should be done by the operations staff, while data entry can only be done by the provider. Then for each task, they can create or choose and existing action or rule to determine how workflow-related data is to be processed, routed, tracked, and controlled. The rules are created by the business rules engine. As an example, one rule might generate automatic email notifications when a condition has been met. Another rule might implement conditional routing of documents and tasks based on the content of fields. The workflow is then tested in the lower environments like INT and UAT. Our system generates an XML that can be deployed in production.

3.10.1.9.2Worker Queues

MAXIMUS has many pre-defined user roles. We will configure the roles based upon DPHHS requirements. When the tasks are defined, the worker role is also identified. For example, any type of adverse action task will always be assigned to the state administrator while provider review and screening tasks are assigned to the operator. An administrator can configure worker queues based on the expertise required for completion. *Exhibit 3.10.1.9-1: Configuring Worker Queue* shows the ability for the administrator to configure the worker queue by adding specific Provider types to a specific user role or by adding specific workflow types to a user role. This enables an Administrator to create groups of enrollment specialists that can specialize in the review and approval of certain types of Providers and/or certain types of enrollments (e.g., new enrollments versus re-enrollments). An administrator can also assign individual applications to various roles or reassign multiple Providers using our bulk update functionality.

The ability to retrieve and review certain types of Providers, or certain types of workflows can be defined for each review role. For example, the Administrator could configure the user to only be able to review Medical Doctors that are submitting a new enrollment or as is the case in our existing implementations, next in queue functions can be used so that all review specialists review applications regardless of type. These configurations will be defined during design and can be modified as needed.

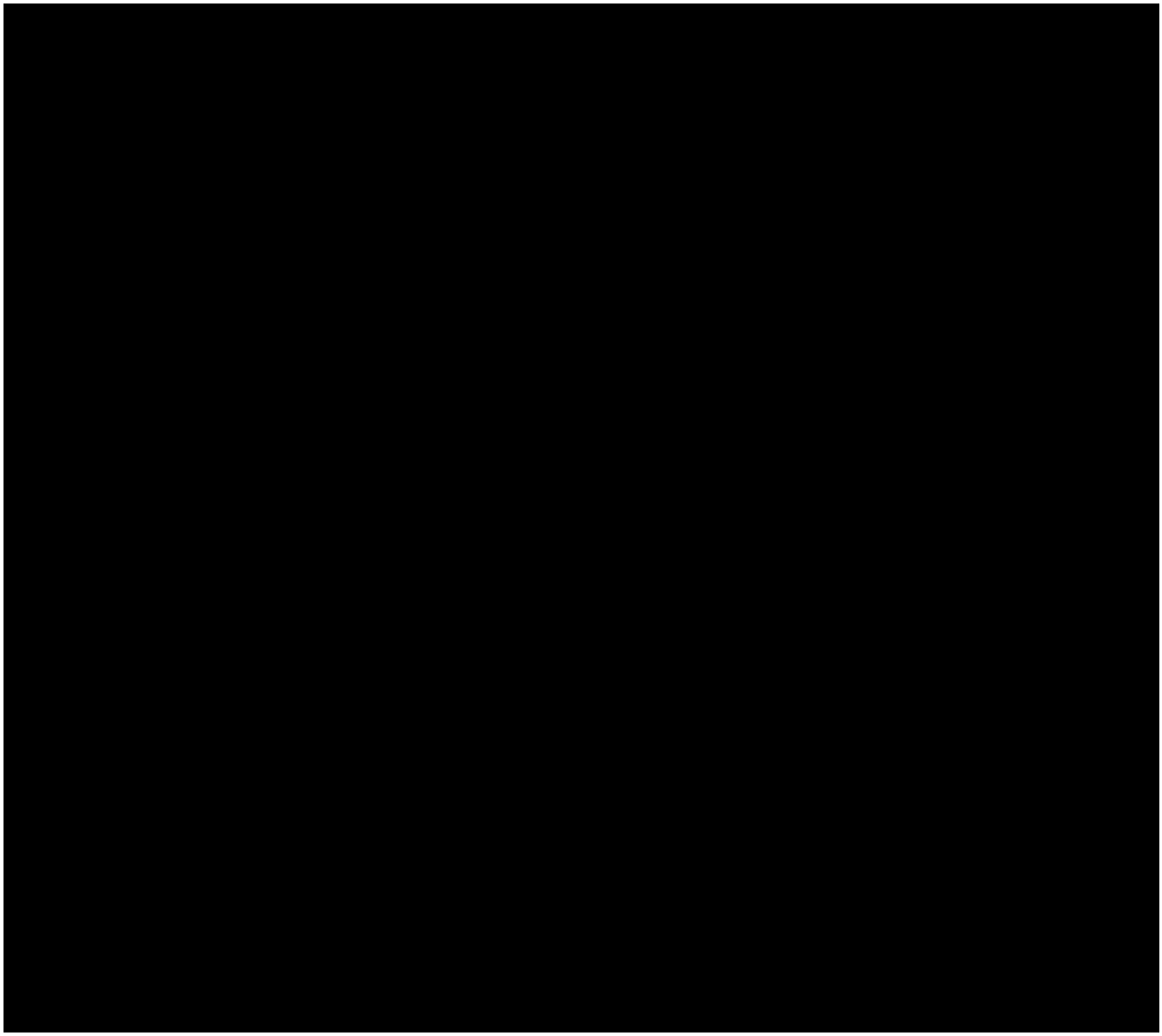
CONFIDENTIAL



Due to timeliness requirements and the overall operations approach, we generally find that the enrollment specialist role processes all application types. Regardless of how the process is configured, review roles have work queues that are setup by the system automatically based on the routing rules for applications. *Exhibit 3.10.1.9-2: Provider Enrollment Specialists Queue* shows the dashboard and assignment list for the Provider Enrollment Specialist.

CONFIDENTIAL

CONFIDENTIAL



A worker's landing page is their work queue. Tasks remain in a particular work queue until they meet all edits of the workflow and perform all required tasks. The BPE guides operational users through the application review, screening, and approval processes. Operational users are able to add or view notes about the Provider within the Provider record. Calls with the Provider are also tracked and included in the Provider record. Notes can also be added at any stage of the application process by any non-Provider role. Along with the note, type of note, user and date of note are stored in the system. Type of notes can be customized based on State's needs. The application review/approval process takes the user through the necessary steps and have indicators for finished and unfinished tasks. The process also features tickler functionality. The Notes functionality also allows for a "To Do" Notes type.

The work queue screen is an extremely useful productivity tool within the MAXIMUS Provider Services solution. Users are able to view a summary of their current assignments in the "My Dashboard" section of the screen. Administrators are also able to navigate to the work queue screen and have the added ability to

CONFIDENTIAL

view assignments based on each individual worker. Operational workers use this screen to prioritize their daily screening and review workload. Our solution is designed to add rules as required by the State to identify and review specific parts of the applications to alert the State authorized user on impact of changes prior to approving an application.

3.10.1.9.3Provider Registration and Workflows

The provider registration process can begin in multiple ways. New Providers must enter a new application and will be routed to one of the new provider workflows based upon business rules (program type, data type, risk level, etc.). Existing Providers enter into different workflows depending on business rules related to the revalidation timeframes. All existing Providers are presented with their information and can begin the process by entering only the new information required by the business rules. The data initially comes from the data conversion process we initiate during DDI phase where we populate the database with MMIS Provider data. Providers are able to view and change their information at any time. Business rules control major items such as a Tax ID change but in general, Providers are able to directly update their information and submit it based on business rules. If the Provider falls into the reenrollment/revalidation period, they will be required to revalidate instead of only updating a piece of information. The re-enrollment workflow displays all current data, but the system ensures the Provider reviews and validates all data similarly to the process for a new Provider. This is also configurable and will be discussed with DPHHS during the system design phase.

Application Submission

The application submission process is designed to occur automatically based on actions taken by the Provider. This workflow ensures that all required data has been entered and edited, agreements have been reviewed and the application has been electronically signed. The application workflow status changes based upon what action has been taken and is always current. This process also initiates background processes that begin to track the application and the time it has been in the process.

Application Review and Processing

The MAXIMUS Provider Services solution is also accessible to internal operations and State staff. Access to the application review, screening, and approval functions are controlled through a single sign-on function. The application has role-based security with rules to verify users can access only the minimum information required for their role and once authentication has occurred, the user is able to access all components of the application their role allows. Our solution review functionality allows authorized users to view Provider data in the centralized Provider data repository, update reference data contained in the centralized Provider data repository, and maintain disclosure information including principals, ownership, and other information that was originally entered by the Providers during the application process.

Once the application/revalidation is submitted by the Provider, a work queue item is generated for the designated review specialists. The required workflow is configurable and will be based on the results of the system design sessions. In other implementations, we have configured extensive workflows to complete a review of the submitted information before the applicaton is screened to verify the information is complete and that the required documentation was uploaded correctly. In Montana we can streamline the process as required by the State. Ultimately, the review and screening workflows will control what

data must be reviewed and approved and how screening results, approval or denial processes will function.

Once a Provider submits an application through the web portal, the rules engine determines which review workflows will be initiated and creates a task in the appropriate work queue. During system design, all workflows are discussed and mapped out to manual and automated processes that must occur and the workflows are then assigned to user types and application processes. The results of the design are configured within the rules engine so as workflows are dynamically created based on data or user actions, the workflows are presented to complete required tasks and track their status real-time. Our solution is designed to track and display the real-time status and location of each application within the workflow.

Among our various implementations, we have a mixture of automated approvals and manual review for approval. However, in all instances, the system is configured to create a work queue item for the State administrator anytime an adverse action is possible. This gives the State the ability to view the impact of changes before the action is taken. From this function, the action can be overwritten, approved or the application sent back to the review queue for further action. Statuses are required that track the decisions and all updates are stored in the Provider's audit trail. While adverse action review for State staff is currently configured, it can be modified based on DPHHS business rules.

An administrator can configure worker queues based on the expertise required for completion. See more in *Section 3.10.1.9.2–Worker Queues*.

Screening

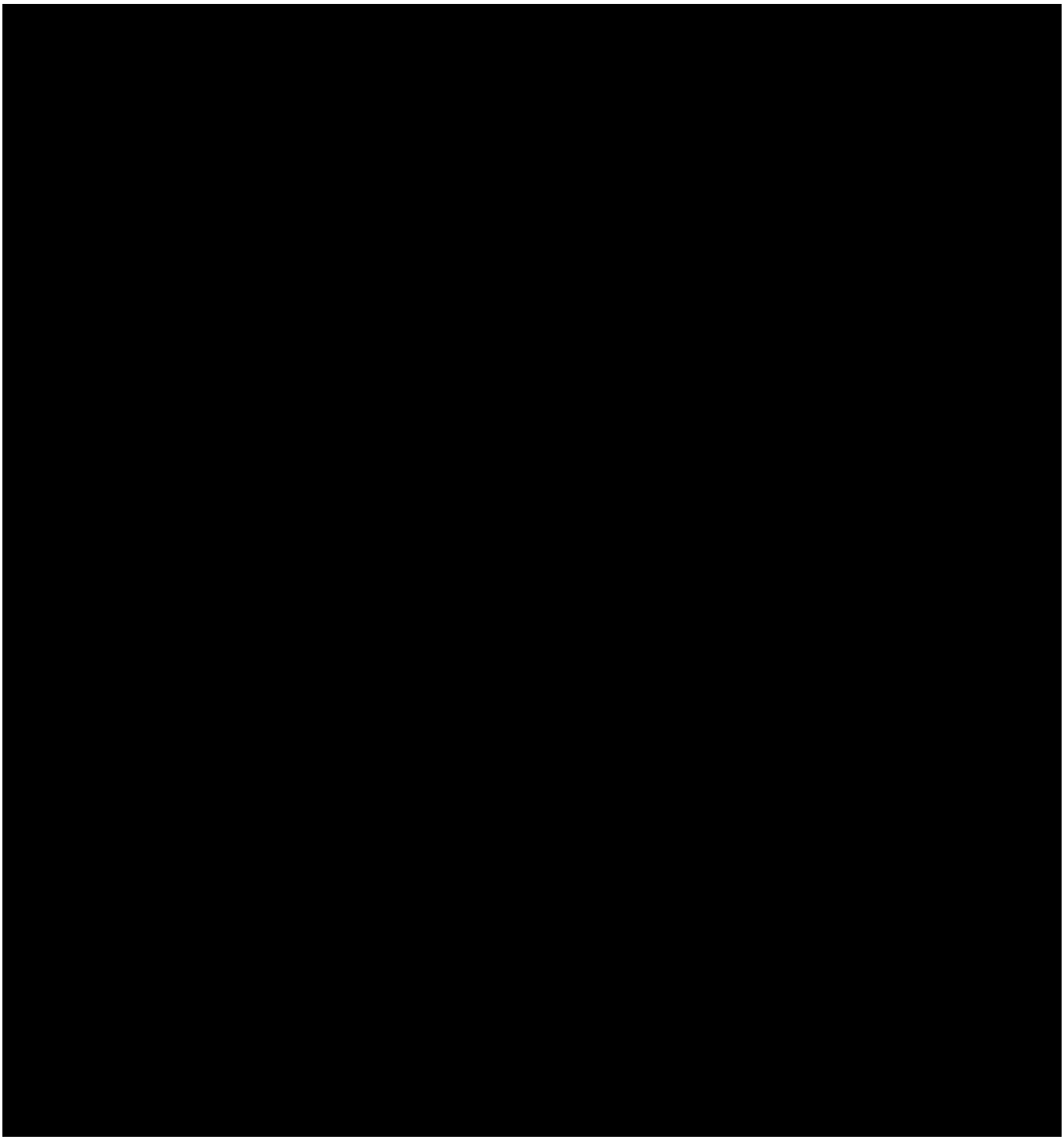
A key component of the MAXIMUS Provider Services solution workflow application is the inclusion of workflows that guide Provider screening against various data sources. Depending on the configuration that is determined by DPHHS, once an application has completed the review edits (manual or automated), screening processes are initiated based on the screening workflow related to the Provider and application type and risk level. Screening requirements are fully configurable for each unique combination. Each screening source is defined during design as automated or manual. While we focus on automating as many data sources as possible, we have found in our current implementations that some screening sources must be reviewed manually either because of lack of an automated interface or because the matching criteria in not detailed enough to validate the Provider actually exists (e.g., name vs. SSN matches).

For each automated data source, we maintain State-approved automated processes to update the Provider Enrollment Master File and tables with data from various boards and licensing or certifying entities. Each entity has an approved update schedule and automated processes used to update the database within State-defined timeframes. We will verify the timeframes for updating the data adhere to the processing schedule as specified by State or federal laws, rules, regulations or guidelines.

Once the automated screening sources have been run, the application is setup in the screening review workflow based on the configurations defined by DPHHS. At this point, the Enrollment Specialist can proceed to the review and verification of matches on the automated interfaces or complete any manual steps that are necessary. *Exhibit 3.10.1.9-3: Provider Screening Summary* shows the results of the initial screening workflow and the screening actions that need to be performed for the application/revalidation. In this example, we are displaying an individual Provider (Physician MD). The Enrollment Specialist is able to view the Provider's profile at the top of the screen and the summary of the screening actions in the

CONFIDENTIAL

Screening and Enrollment Summary section. Users can click on the link on the Status link to view more details of the action required or view the results of an action already taken.



The system will be configured to contain a list of interfaces or external systems that must be checked before approving the application submitted by the Provider and each source will be designated as manual or automated depending on how the data is accessed. Our workflow solution allows for a multitude of data access options and we will determine how each data source is accessed during design. This

CONFIDENTIAL

CONFIDENTIAL

configuration will be based on the Provider type indicated on the Provider's application. A Wizard model is also used for this purpose clearly showing that items are complete and which are remaining. Enrollment Specialists can begin screening and finish later. The requirements for each screening source and the level of manual interaction will be defined during design and configured into the final MAXIMUS Provider Services solution.

For each screening item, a decision is tracked regardless of whether the verification is automated or manual. Valid hits on a screening data source may automatically trigger an adverse action workflow while success across the entire review may initiate an approval workflow. The workflow is configured to trigger an appropriate workflow after all screening and review is completed so a complete profile of the Provider status is available before a final decision is made. Once the Provider Enrollment Specialist has completed the full review of a Provider enrollment package, an approval or denial workflow is triggered based on the specific actions taken.

Provider Application Routing

Once the Provider Enrollment Specialist has completed the review of a Provider enrollment package, the application can be directed to be reviewed by operations management, a State authorized user or it can be directly to be sent to the MMIS without review. Our solution can be configured to automatically process the approval or denial workflow or create a work queue items for a specific resource to review the results of the screening and make a final determination. In addition, it is also possible for an individual application to be manually forwarded to a State review work queue for action. For quality assurance and quality control, applications can be routed to State IG (or other applicable group) by configuring the workflow for that application role. The workflow engine will be configured to change the process flow to fit the needs of DPHHS and the specific process that will be used with external partners such as the State IG. The workflow tasks and steps are stored and displayed to reflect the real-time status of an application. *Exhibit 3.10.1.9-4: Steps Performed for an Application* shows the MAXIMUS Provider Services solution view of tasks performed by the system and the user in an application process. Using the dropdown, an authorized user can view the tasks performed for previous revisions. This graphical interface shows the application status real-time within the workflow.

CONFIDENTIAL

The workflow engine stores all the information on the tasks for every application in the system. Using our business intelligence tool, we can produce status, inventory reports, and Provider processing statistics for individual users with aggregate totals for daily, weekly, monthly or annually. Any time an application is placed into a State work queue, a user action is required to move the application to the next available workflow. Applications that are approved will result in the enrollment of the Provider and a transaction will be sent to the MMIS so that all required documents are sent. An adverse action will be noted and a transaction sent to the MMIS based on business rules for existing versus new Providers.

Electronic Communications

The MAXIMUS Provider Services solution contains a communications framework that allows us to create and configure the content of any system generated e-mail based on business rules, workflow items and events that occur within the system. Our solution also sends mass email/print notifications in scenarios such as Provider re-enrollment, license expiration, 10-day application cancellation, etc. business rules can be configured to send emails to workers based upon different criteria. The notifications can include any information deemed required and applicable to the notification. This includes providing instructions for revalidation as well as links to additional information available for the Montana Provider community and any pertinent attachments. Our solution tracks notifications to Providers, generating follow up notifications at predetermined intervals.

3.10.1.9.4Workflow Requirements

The following table includes Attachment F Workflow Requirements, our summarized response to each requirement, and the section(s) in our proposal in which we provide our detailed response.

ID	Workflow Requirement	MAXIMUS Summarized Response
WKF01	The Contractor's workflow solution shall provide a runtime engine that facilitates process events throughout the work type lifecycle.	Our solution has a business process framework, called the Business Process Engine, which enables execution and maintenance of process workflows. Our Business Process Engine enables high-performance flexibility, extensibility to the MAXIMUS Provider Services solution. The MAXIMUS Provider Services solution Business Process Engine automatically executes the appropriate business process model based on the inputs from the business rules engine. The Business Process Engine has a process repository, a server based process execution engine, monitoring, reporting and analytics.
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.	Our solution's workflow engine provides the ability to distribute work based on user roles. Workflow tasks are categorized and are assignable by the task type. For example screening tasks can only be assigned to the screening specialist, site visit tasks can be assigned to the site visit operator, etc. Tasks can be redistributed based on criteria like age, priority, etc.
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.	Our solution provides a role-based Graphical User Interface (GUI) for process definition that leads the user through the steps of defining the workflow associated with a business process. See *Section 3.10.1.9.1–Workflow Definition Tool.*

ID	Workflow Requirement	MAXIMUS Summarized Response
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.	MAXIMUS will assist the state in defining the workflows and workflow steps based upon business requirements. The Business Process Engine stores the workflow steps in the Corticon Rules engine which provides a flexible user friendly interface for defining and changing the workflow tasks and steps. Our flexible solution allows the mixture of manual and automated tasks which can easily be changed as more automation is implemented.
WKF05	The Contractor's workflow solution shall support work-type processing that includes internal and external dependencies.	The system will be configured to contain a list of interfaces or external systems that must be checked before approving the application submitted by the Provider and each source will be designated as manual or automated depending on how the data is accessed. Our Solution allows for a multitude of data access options and we will determine how each data source is accessed during design. We can add process steps to a workflow including manual follow up that might be necessary. Data entry triggers or actions will automatically restart the workflow.
WKF06	The Contractor's workflow solution shall provide the ability to view alerts and/or reminders by user, by work-type.	Our solution includes internal and external communication processes to allow automated reminders, notices and other documentation to flow electronically to users based on their work-type in the system and the associated status of those work-type. Providers and workers can see their alerts when they login. Automatic emails are also sent from the system for reminders and alerts. Because of our flexible design other mode of viewing can be incorporated on demand.
WKF07	The Contractor's workflow solution shall provide the ability to set alerts and or reminders by user, by work-type.	Our system has ability to send automatic and manual alerts. For example system sends an alert to the state admin users when a provider is assigned to their queue. The administrator can send manual alerts by going to the worker's queue. Scheduled reminders can be send using the interface scheduler.
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.	Our Solution maintains status of the Provider application throughout all steps within the workflow. The state of the work-item is based upon what steps has been taken on the work item. Other than the automatically setting the state, the system also allows workers to add notes and comments to provide more details. Also we support two types of states, internal and external. Our role-base access allows to display different values for different users.
WKF09	The Contractor's workflow solution shall provide supervisors access and control of work by type and by user.	Our solution contains supervisor functionality that shows what each worker has in their queue and provides the ability for supervisors to reassign work as necessary. Our solution contains a comprehensive dashboard that allows authorized users to view a snapshot of the entire program including a summary of the status of all Provider registrations. We show each work queue and include aging characteristics about the queue so that managers and supervisors can see how work is progressing for each Provider type. The dashboard items contain drill down capabilities to detailed Provider lists and reports and work can be reassigned as necessary.
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.	The MAXIMUS Provider Service Solution System workflow engine honors the restrictions of BPMN but documenting of our processes is descriptive without being as cumbersome.
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.	MAXIMUS Provider Services solution contains many pre-defined user roles. These roles are configured based upon DPHHS requirements. When the tasks are defined, the worker role which will complete that task is also identified. For example any type of adverse action task will always be assigned to the state administrator while provider review and screening tasks are assigned to the operator. An administrator can configure worker queues based on the expertise required for completion. *Exhibit 3.10.9.1-1: Configuring Worker Queue* shows the ability for the administrator to configure the worker queue by adding specific Provider types to a specific user role or by adding specific workflow types to a user role. This enables an Administrator to create groups of enrollment specialists that can specialize in the review and approval of certain types of Providers and/or certain types of enrollments (e.g., new enrollments versus re-enrollments). An administrator can also assign individual applications to various roles or reassign multiple Providers using our bulk update functionality. The ability to retrieve and review certain types of Providers, or certain types of workflows can be defined for each role. See *Section 3.10.1.9.2–Worker Queues*.

ID	Workflow Requirement	MAXIMUS Summarized Response
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).	Our solution's Workflow engine automates all provider management functions including the ability to enroll Providers and conduct periodic reactivation/revalidation activities electronically via a web portal, standardize and improve the data collection process through automated business edits and task-based workflows, screen Providers against verification databases, track the status of required provider site visits and other outreach activities, and monitor the payment of application fees as applicable. Our solution is designed to automatically move the application to the next person in the workflow for further work.
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.	Our solution has many pre-defined user roles. These roles are configured based upon DPHHS requirements. When the tasks are defined, the worker role which will complete that task is also identified. For example, any type of adverse action task will always be assigned to the state administrator while provider review and screening tasks are assigned to the operator. An administrator can configure worker queues based on the expertise required for completion. *Exhibit 3.10.9.1-1: Configuring Worker Queue* shows the ability for the administrator to configure the worker queue by adding specific Provider types to a specific user role or by adding specific workflow types to a user role. This enables an Administrator to create groups of enrollment specialists that can specialize in the review and approval of certain types of Providers and/or certain types of enrollments (e.g., new enrollments versus re-enrollments). An administrator can also assign individual applications to various roles or reassign multiple Providers using our bulk update functionality. The ability to retrieve and review certain types of Providers, or certain types of workflows can be defined for each role. See *Section 3.10.1.9.2–Worker Queues*. Our solution is BPMN 2.0 compliant.
WKF17	The Contractor shall configure, support and maintain a configurable document management and workflow solution that meets the State's requirements.	Our solution contains content management capabilities. Our ECM solution manages all paper applications, documents and attachments uploaded by Providers during the enrollment process, and all converted documents that come along with conversion of providers. Our solution's ECM component contains several features out of the box with easy configurability and customizability. Our solution contains a configurable workflow engine which is based on the business rules.
WKF18	The Contractor shall have configurable workflow processes to support auto notifications to providers for specific events (e.g., license expiration, revalidation).	Our solution is designed to automatically system-generate notifications based on workflow processing. The system contains triggers that are used to create system-generated notices and letters based on specific events, pre-defined tasks and their completion. In District of Columbia, we send revalidation notification 2 months and one month prior to the revalidation date, license expiration notices are also sent. These frequency and time of notices is configurable.
WKF19	The Contractor shall provide links to screening and monitoring databases in the workflow tool if the data isn't available via an automated interface.	Our solution is able to include links to data sources in the screening workflow and require operations staff to perform the screening and record the results into MAXIMUS Provider Services solution, which enables the workflows to continue as required. We store verification URLs for manual sites within MAXIMUS Provider Services solution to allow operations staff to directly access the site without having to look for the URL. Our system is flexible enough to quickly automate the process in case the data becomes available. See *Section 3.10.1.6.4–Screening and Credentialing Interfaces*.
WKF20	The Contractor's solution shall have configurable workflow to present for validation, updates submitted online/electronically by specific criteria (e.g., program type, data type, risk level).	The provider registration process can begin in multiple ways. New Providers must enter a new application and will be routed to one of the new provider workflows based upon business rules (program type, data type, risk level, etc.). Existing Providers enter into different workflows depending on configurable business rules related to the revalidation timeframes. All existing Providers are presented with their information and do not have to start from scratch. See *Section 3.10.1.9.3–Provider Registration and Workflows*.

3.10.1.10 Correspondence Management

3.10.1.10 Correspondence Management

The Contractor's correspondence engine shall be configured to generate enterprise correspondence and coordinate the print and distribution through a State approved print and mail service. The Contractor must describe the proposed solution's capacity to configure, support and maintain correspondence management functionality (i.e., add, modify, or remove

CONFIDENTIAL

correspondence) and the type of resource and necessary skill set(s) required for correspondence management functions. Describe the change management processes associated with correspondence management. In addition, the Offeror must describe their approach to meet each of the Correspondence Management requirements detailed in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution includes an integrated correspondence management module to design, manage and deliver high-volume and on-demand communications. We are using Quadient's Correspondence Communication Management solution, Inspire (formerly, GMC Inspire). This enables users to create timely, contextual, personalized, and accurate communications for all channels from one intuitive interface.

Our correspondence management module comes with a designer, a web based editor for review/approval, a repository for storing designs and a correspondence engine to create designs on-demand or batch. In addition, we are able to generate barcodes.

3.10.1.10.1 Notice Generation

The MAXIMUS Provider Services solution comes with a number of pre-built notices with the base configuration of the system, as shown in *Exhibit 3.10.1.10-1: Table of Pre-Built Notices*. These notices are generated at several different points of the provider enrollment life cycle. MAXIMUS will confirm these trigger points with the State. During the DDI phase, MAXIMUS will work with DPHHS to identify any other notices that are required during the workflow process. We will add the newly identified notices to the notice repository and get them approved by DPHHS before we go live. Here are the notices that are sent to the provider as part of the system. In addition to these, our system has a number of notifications and notices that go to the internal users.

CONFIDENTIAL

CONFIDENTIAL

3.10.1.10.2 Correspondence Template Modifications

All the correspondence templates are stored in our design repository and a user can choose to start with an existing design or start a new design using our designer. The designer allows users to browse and modify designs in the repository. These design templates can include graphics, images, text and design elements, and use rules and variables to manage the content. The designer also provides integration with other design formats like PDF. PDF files can be imported and modified to reduce design time and eliminate errors. The designer can define fields in the template that are going to be data driven like provider name, address, etc. can be replaced when the design is being printed. The designs can be created simultaneously for print and web communications from a single interface. As the designs are complete, the designer user can view the design on the fly with real data, evaluate different concepts, eliminate errors, and reduce development time.

The templates also have re-usable content components. This minimizes design time and reduces the number of templates needing to be maintained. In the content repository we can create reusable items that are common to many types of correspondence (e.g. the address of the service center, phone number, and fax information.) We can also import logos and other graphics into the content repository.

3.10.1.10.3 Barcode Technology

Our designer enables barcode support through the core Designer interface, as shown in *Exhibit 3.10.1.10-2: MAXIMUS Provider Services Solution Designer Component*. Users can simply add a barcode object to a page or communication, and then our designer offers context specific properties depending on the bar code. We support several barcode technologies including but not limited to OMR barcode, UPC A barcode, UPC E barcode, QR Code, etc. The barcodes can be added in several different ways. If the

CONFIDENTIAL

CONFIDENTIAL

barcode needs to be scanned, it will be added to the design during the design time. But, if the barcode needs to be added based on the provider data (e.g., a barcode that needs to be generated based on NPI, so that the provider can show it for fingerprinting), the design will have a placeholder. During production, it can be generated based on the provider data to be inserted into the final output.

Once the designs are created, they are checked-in by the designer into the content manager. These designs are then ready to go through review and approval process. The review and approval process can be defined and modified based on DPHHS's needs. The Content repository stores all the versioning and approvals. All approved documents are then ready for production.

3.10.1.10.4 Output Orchestration

The MAXIMUS Provider Services solution has multiple ways to instantiate the correspondence engine to create email and print output for providers. All the design templates have print and email design capability to allow for sending emails. As shown in *Exhibit 3.10.1.10-3: MAXIMUS Provider Services Solution Design Change Control Process*, our solution is based on the provider communication preferences, and can trigger email or print output for each provider. The triggers for generating outputs can be based on scheduled jobs, real-time from the provider services solution and directly from the correspondence engine.

CONFIDENTIAL

CONFIDENTIAL

Our solution includes scheduled jobs, such as license and revalidation monitoring which sends emails to providers. When these jobs are triggered, our solution sends notifications to providers. In the case of license monitoring, our solution sends multiple notifications to providers based on configuration set. For all providers' whose license is expiring in 30 days, our solution gets the communication preferences and based on the communication preference, we will send a request to correspondence engine to create a print or email. All the variable data is taken from the provider information and is sent to correspondence engine using web services for the PDF or email. The generated print or email is saved in ECM. If the output type is email, an email is sent to the provider immediately. If the output type is print, a print ready document is made available to the print vendor.

3.10.1.10.5 Print Vendor Support

Our correspondence management component has color management features and can provide output formats that are supported by a variety of print vendors. We can produce a wide range of output formats, including AFP, PostScript, HTML, PDF, and image-based and text formats. All print job assets, including fonts, can be saved within a single Inspire document file that is created into a print ready output file. This makes print jobs portable between different print vendors and different sites and reduces risk of accidental alteration when a job moves through the organization. MAXIMUS will work with DPHHS and the print vendor to tune the correspondence management component so that we can generate correspondence that is production ready.

3.10.1.10.6 Correspondence Management Requirements

The following table includes Attachment F Correspondence Management Requirements, our summarized response to each requirement, and the section(s) in our proposal in which we provide our detailed response.

CONFIDENTIAL

ID	Correspondence Management Requirement	MAXIMUS Summarized Response
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 MAXIMUS Provider Services solution has a correspondence management component that can generate correspondence. This function is integrated with the online application and triggered based on workflow. A designer can start by using a PDF, Word or any other format and create the design in the designer.
COR02	The Contractor shall configure, support and maintain a correspondence engine to generate correspondence and coordinate the print and distribution through a State approved print and mail service.	Our correspondence management component can be configured as required by the print vendor for printing and distribution. We will work with DPHHS and the print vendor on the details of the same.
COR03	The Contractor's solution shall utilize industry standard barcode technology that is approved by the Department.	Our designer enables barcode support through the core Designer interface. Users can simply add a barcode object to a page or communication, then our designer offers context specific properties depending on the bar code. We support several barcode technologies including but not limited to OMR barcode, UPC A barcode, UPC E barcode, QR Code, etc.
COR04	The Contractor shall utilize letter, notification and other templates for correspondence that are approved by the Department.	Our solution will have a review approval that will allow for DPHHS to review the correspondence templates before they are put in production.
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).	Our solution will store all the correspondence along with the provider data. This is an integrated component and will be enabled as part of our solution.
COR07	The Contractor's solution shall store all sent or received documents in the ECM.	Our solution will automatically send all sent notices in the ECM where they will be stored on the provider record.
COR08	The Contractor's Correspondence Management Solution must be able to integrate variable data to maximize efficiency.	Our solution has capabilities for variable data. During the design time, the designer needs to provide the fields for variable data into the template. They can verify that the variable data is getting populated correctly by proofing in the designer.
COR10	The Contractor shall generate applicable notices to members, providers, and other entities (e.g., enrollment/disenrollment notices, requests for information, and program information).	Our solution has a number of inbuilt notices that come with the system. MAXIMUS will work with DPHHS on the other notices that are required based on other use cases.
COR12	The Contractor's solution shall produce notices to applicants of the approval, rejection, and pending status of their provider enrollment.	Our solution will produce notices to applicants at various stages of provider enrollment.
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.	This function is supported through a combination of the documents being created and how they are formatted. The tool contains a scoring algorithm that helps validate the materials are created at the right reading level.
COR15	The Contractor's solution shall support official approval and denial notifications to the provider. The notification will support consolidated communication for multiple taxonomies in the case of split approval and denial of provider enrollment service determinations.	Our solution supports official approval and denial notifications to the provider, and supports consolidated communication for multiple taxonomies for split approval and denial of provider enrollment service determinations.

3.10.2 Project Management and System Development Requirements

3.10.2 Project Management and System Development Requirements

The Contractor will be expected to apply proven project management and system development methodologies to the initial implementation of the proposed solution and to each subsequent enhancement or iteration of the solution.

DPHHS does not require a particular project management or system development methodology. The Offeror must propose an approach that will satisfy the scope of work and incorporate all activities required, or their conceptual equivalent. The

> Contractor will be expected to adjust the project management approach or project schedules, as necessary, to collaborate with the Systems Integration Services Contractor and other contractors in order to incrementally build the MPATH modules and components. In addition, DPHHS will require the coordination of efforts among its staff and all contractors, as no single contractor can perform its required responsibilities without coordination and cooperation with the other contractors. The selected contractors shall maintain communication with other contractors and DPHHS management and staff as necessary to meet its responsibilities that pertain to this RFP's scope of work.

MAXIMUS organizational standard process (OSP) integrates and uses best practices found in the CMMI-DEV, CMMI-SVC, ISO 20000, and ISO 9001 standards. MAXIMUS uses a project management-based methodology based on the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK) to govern how we design, develop, and implement our Provider Services module and business operations. We have developed a proven implementation model accompanied by a process-based project approach that accounts for these items and includes risk mitigation and lessons learned. This gives us the ability to deliver quality, on-time work products that meet project standards and the contract requirements.

The MAXIMUS Project Management Methodology (PMM) is the approach we follow for project management and the System Development Methodology (SDM) is our methodology for delivering system solutions. We have taken steps to make sure that the PMM and SDM work together, do not conflict, and each maintain focus on their respective project areas. All aspects of Project Management are governed by the PMM. All aspects of systems and software development, particularly design, configuration, coding and testing are governed by the SDM. We use our PMM and SDM methodologies in tandem as our project management and development methodology for all our projects. We adapted our approach specifically to balance the needs of supporting routine maintenance and operations while at the same time supporting major product upgrades and implementation projects. Our approach confirms that the MAXIMUS deliverables, tracking, and monitoring functions are in line with those contained in the Request for Proposal. In this section of our proposal, we discuss our PMM.

MAXIMUS recognizes the State's need to meet ACA requirements, modernize the Medicaid system infrastructure and improve the services delivered to Medicaid members. Our project management, software development, and operational methodologies are key to meeting the State's implementation goals for the Provider Services module and integration to the other components of the MPATH platform. We utilize industry best practices and proven PMI® guidelines to:

- Assess, design, configure, and deploy the hardware infrastructure and software components necessary to satisfy the MPATH scope of work and incorporate all required activities
- Adjust and modify, as necessary, the project management approach and schedule to work collaboratively with the Systems Integration contractor and other contractors to achieve a common success
- Cooperate and coordinate our efforts with the other contractors, whose success and the success of the MPATH project is dependent upon a collaborative effort
- Manage communications with DPHHS management and other contractors to facilitate a common understanding of the responsibilities, goals, and objectives of all stakeholders.
- Move into an operational model and provide guidance and assistance to the service delivery organization and trading partners in their transition to the new Provider Services solution

MAXIMUS carefully reviewed the Montana CIO Strategic Goals, Strategic Plan, and Mainframe Exit Strategy. We are pleased with how closely our incremental approach to modernization of legacy systems adheres to the vision described in these documents. At the onset of the project, we will conduct a full review of our methodology with DPHHS. This set of activities will align our methodology to the overall project management approach being used to oversee the entire MPATH project. To achieve agreement on expectations for the Provider Services module, we will review each deliverable with DPHHS using a Deliverable Expectation Document, which will clearly define the approach, content, and approval criteria for each deliverable we complete as part of the implementation effort. As part of these documents and reviews, we will prepare an annotated table of contents that we will use to guide the walkthrough. During this process, the entire project team we will gain a common understanding and agreement on the content of each deliverable and define the review and approval process. We will obtain DPHHS sign off before starting work on any deliverables.

To develop the specific procedures for the Provider Services module project, we utilized our PMBOK-based PMM to examine the specific requirements for the MPATH project. , We have identified best practice procedures we find aid in the delivery of our solution. Integrating these best practices into daily activities reduces risk and confirms delivery of quality products and services.

The MAXIMUS project methodology is based on a comprehensive implementation approach that starts with implementation of the system and the support infrastructure required to execute the plan. We use a repeatable, proven approach to deliver a compliant solution for the State. Our methodology addresses each element of the RFP specified scope of work and includes additional activities we believe are critical to project success. Our Project Management Plan template is tailored to the requirements, deliverables and timelines specified in the RFP to address the following major project phases:

1. Project Initiation
2. Requirements Validation
3. Design
4. Technology and Infrastructure Setup
5. Configure/Build
6. Incremental Testing
7. Training the Trainers
8. System Testing
9. User Acceptance Testing
10. Operational Readiness Assessment
11. Implementation

Exhibit 3.10.2-1: Project Management Methodology depicts our approach for the MPATH project. We place significant emphasis on the software development components of the project because they form the basis for all other activities. We also closely tie the preparation for operations with the system implementation effort so that upon go live, the entire module including customer service is ready for production. We execute these activities in an integrated manner to yield a full solution that is ready for production operations and ongoing maintenance.

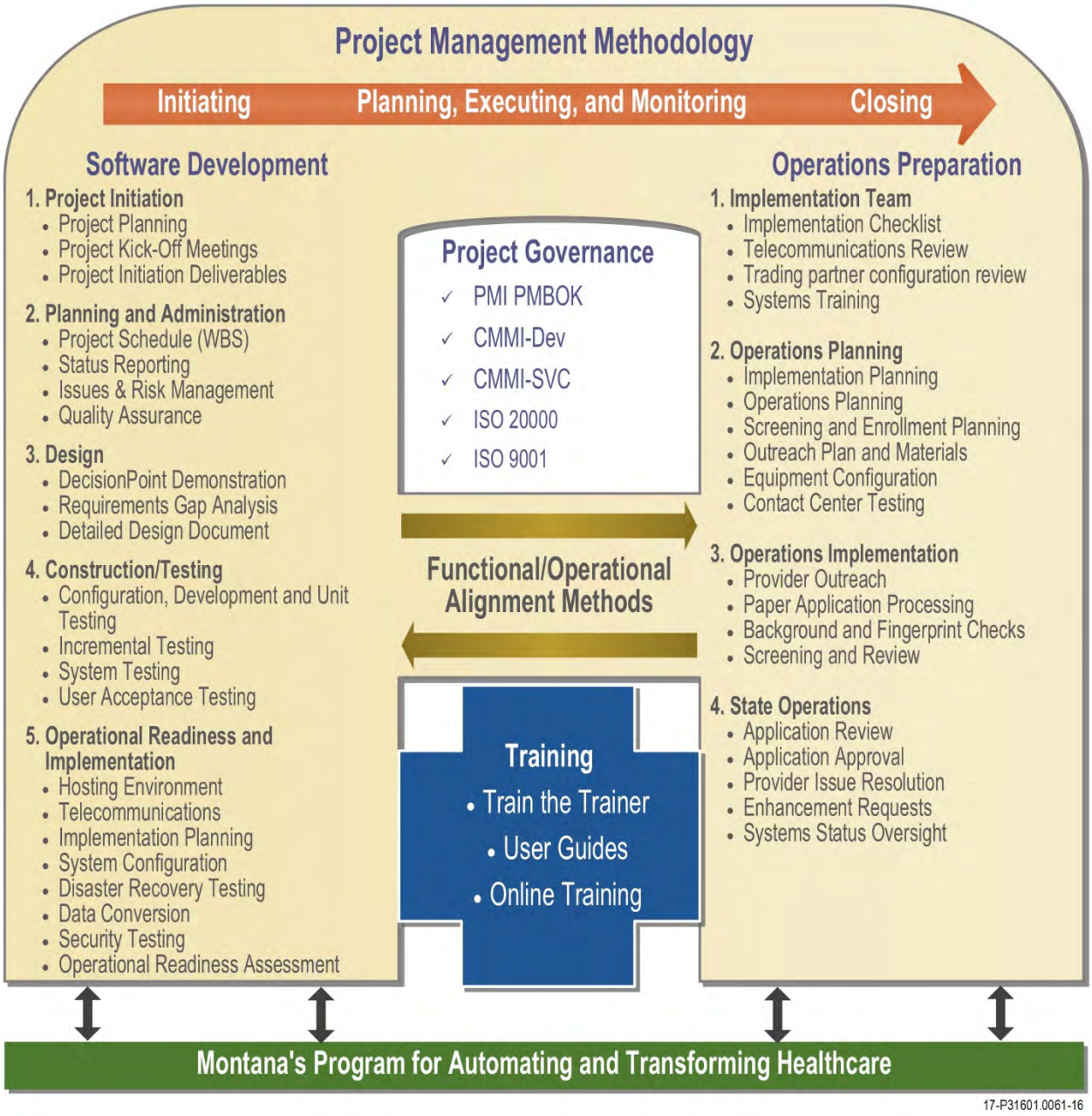


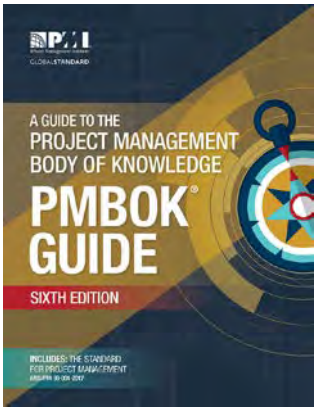
Exhibit 3.10.2-1: Project Management Methodology. *Our project management methodology delivers our projects on-time and on-budget with the appropriate focus on the technical processes required to meet the RFP requirements.*

We understand that business process operations is an optional (Option B) component of this procurement and that this capability may be procured separately or included as an integrated component of the project. Regardless of which approach is selected, MAXIMUS understands that the integrated nature of the system and the business operations requires that we work closely with the State, MAXIMUS Health Operations (if selected) or another vendor to prepare for go-live. The implementation of our Provider Services module will significantly change how providers interact with the system and the Medicaid Program. New operational models will be required to maximize impact of the new system and work with

providers under a new arrangement. Our methodology incorporates seamless connection points between the two implementation aspects of the project that allow the total Provider Management solution to be ready for production at the same time, regardless of who is responsible for provider management business operations.

We also realize that the implementation effort will be greater if a state chooses the provider self-service functions defined in Option A. To maximize the investment in both MAXIMUS and State staff, we propose to implement this set of functions in conjunction with the base system. This enables us to use the management, business, and testing staff members that are already supporting the implementation effort. We will integrate the additional tasks related to Option A into the schedule if they are chosen.

For system projects in the health and human services marketplace, we tailored the practices and methods in our PMM to the processes and procedures recommended by the Project Management Institute (PMI), and included in the Project Management Body of Knowledge (PMBOK®). We have found that the structure and reusability of the processes defined by PMI work effectively for our product support and implementation engagements. We follow the tailored practices to remain in compliance with the project specific process (PSP) and focus on implementing a structured approach to mitigating, identifying, and handling potential problems. In addition, our PSP includes all processes, procedures, and tools needed to effectively manage and control the implementation for the ongoing success of the MPATH project.



MAXIMUS follows the industry standard for project management presented in the Project Management Institute's Project Management Body of Knowledge.

The PMBOK® is a guide for managing projects by using processes that have proven successful in virtually every industry and geographic location around the world. The PMBOK® describes 42 key project management processes comprising five process groups that represent the best practices for managing projects. Our PSP also includes a two-dimensional framework:

- A functional grouping based on the contribution to the overall management cycle: initiating, planning, executing, controlling, or closing
- A content grouping into ten key knowledge areas to manage to certify the project is successful

Best Practice

We have tailored PMBOK® principles to our project management approach for implementation and ongoing maintenance to make sure all project delivery processes are disciplined and well managed, and the services we provide are delivered in a quality and timely manner. In addition to our adherence to PMBOK® principles, we have established our own best practices through years of project implementations and have compiled them into Project Implementation and Project Management Manuals that supplement PMBOK® in guiding our operational projects to success. Our team has successfully utilized this methodology in the District of Columbia, and the states of Tennessee and Nebraska as we have developed, configured, and implemented our Provider Services solution. We have structured our overall approach so our project management processes can be used regardless of the Option chosen.

Our proposed project leadership team members are experts in the MAXIMUS project management methodology and who have direct experience using our project management processes in the implementation and enhancement of modular Provider systems including the implementation of our Provider Services system implementation in the District of Columbia, Tennessee, and Nebraska. Our project leaders are veterans of modular provider projects and they have been working hand-in-hand with our Medicaid customers to implement a variety of Provider management solutions. To support the use of our PMBOK-based methodology, we seek out project leaders that are PMI-certified Project Management Professionals (PMPs). This includes our Contract Manager, Project Manager, and Certification Manager.

For each of our modular implementation projects, we applied our project management methodology to meet the schedule and quality standards established by the RFP and contract. As a best practice, we update our standards based on the lessons learned from each new project. Experience gained by being the first company to implement a modular Medicaid Provider Management system in Tennessee was extremely valuable to our implementation in Nebraska and we transferred this experience to the District of Columbia. In conjunction with our project management expertise, our management team brings extensive experience in other industry-standard project management methodologies. Our project management team also brings hands on experience in the design, development, and implementation of Provider management systems within Medicaid as well as deep credentials for system implementations across the Health and Human Services market.

We understand that every project is different and guidelines are a framework to help define those items that should be accomplished for a successful project. Our Project Management team not only understands the importance of defined procedures, they have used these procedures to successfully implement our Provider Services modules for other states. In reviewing the specific RFP requirements, we ailored the set of processes we use to plan, execute, and monitor our projects specifically for this project. We built our scope of work based on the specific RFP requirements utilizing our project management methodology as the basis for how we conduct all project, quality, and delivery activities.

Exhibit 3.10.2-2: Project Management Lifecycle and Knowledge Areas illustrates the use of PMBOK® in support of our project management methodology. Use of PMBOK® as a guide for our planning and delivery efforts has allowed us to continue our history of successful project delivery in the face of ever changing technological, legislative and policy mandates. We place all required project activities into a project lifecycle made up of the five Process Groups defined within PMBOK®, and use each of the ten knowledge areas to control the various aspects of project management that need to be considered as the project moves through its lifecycle.

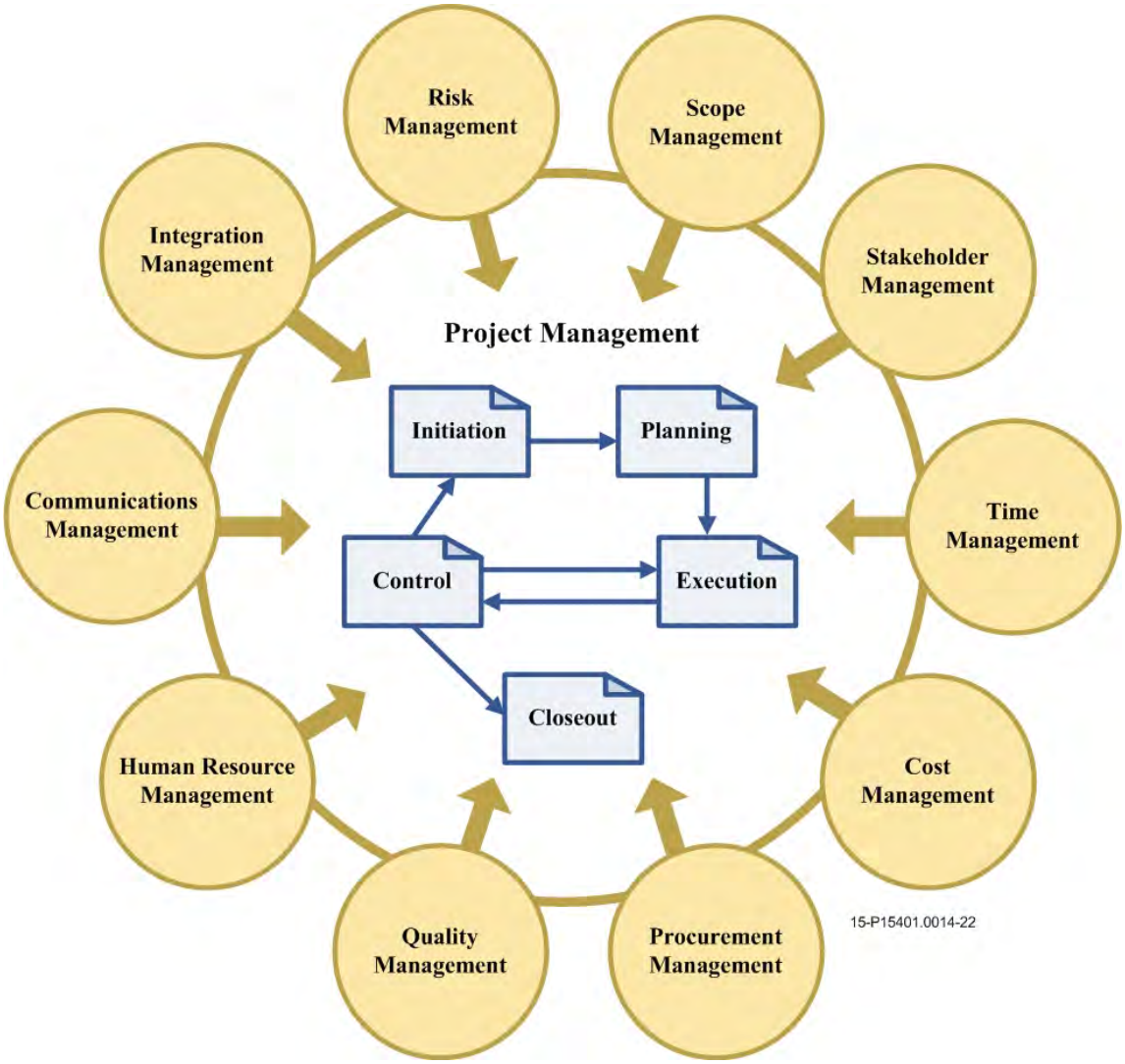


Exhibit 3.10.2-2: Project Management Lifecycle and Knowledge Areas. *MAXIMUS manages projects throughout each stage of the project lifecycle using a proven project management methodology for consistency and success.*

Our PMM breaks down every project into a lifecycle of tasks and activities from beginning to end. Our lifecycle approach helps MAXIMUS develop a plan that focuses on the right activities at the right time to increase the probability of success. It also enables components of our implementation approach to be added or removed based on the needs of the specific project. The project lifecycle defined within PMBOK® and used by MAXIMUS consists of five integrated process groups that follow the general chronology of a project. We apply specific processes from each to complete all aspects of the scope of work.

- **Initiation** – Defining the project and securing buy-in by appropriate stakeholders
- **Planning** – Detailing the tasks, resources, and schedule necessary to accomplish the project
- **Execution** – Carrying out the planned tasks
- **Control** – Managing the scope of the project as it is executed

- **Closeout** – Wrapping up the completed project and documenting lessons learned

Efficiency

The MAXIMUS team follows the guidelines of these PMBOK® integrated process groups to plan, execute, and control the tasks required to deliver the work products for the project and focus on the appropriate management processes as required by the project work plan. The MAXIMUS project management approach is composed of PMI-favored project management methods and best practices across all project phases. The methods provide a consistent framework for our projects, but they are not intended to form rigid project management procedures that must be strictly followed without consideration for project variations or State of Montana needs. In fact, one of the principal objectives in developing our project management methodology was to balance the "consistent framework" intent with the equally important intent to make the methodology customizable and scalable.

Within our PMBOK®-based project management approach, we apply the 10 PMBOK® knowledge areas to guide the implementation of our projects. Each knowledge area contains the processes that need to be accomplished within its discipline to achieve a successful project outcome. We work with the State to finalize each project management process and agree on the content and format of artifacts from each of our project management processes.

MAXIMUS uses an industry standard suite of tools and methods to facilitate Project Management. Below are some of the tools that we will use on the MPATH project. If any of these tools are not approved by Montana, MAXIMUS will submit the appropriate paperwork to get an exception or explore the use of a different tool that is State approved:

- **SharePoint** – This tool is used as a document repository that allows for collaboration between the State and MAXIMUS. SharePoint allows for the storage of documents as well as the tracking of action items, version history, and allows for storage of all meeting minutes.
- **Microsoft Project** – enables the integrated implementation plan to be defined and tracked with dependencies and a critical path
- **Microsoft Office** – MAXIMUS uses the Office Suite for the creation and delivery of deliverables with the use of Word, Excel, PowerPoint, and Outlook
- **Adobe Acrobat** – MAXIMUS uses Adobe Acrobat to convert deliverables into PDF format for final delivery
- **JIRA** – This tool is used for tracking issue reports and resolution, defect remediation, action items and changes. This tool is flexible enough to be used for recording and tracking many of the critical project management artifacts.
- **JAMA Contour** – This tool is used to manage the Requirements Traceability Matrix and confirmation of testing for each requirement.

3.10.2.1 Project Management

> 3.10.2.1 Project Management
>
> The Contractor shall submit a formal Project Management Plan and project schedule, along with other project planning documents. The Contractor must adhere to the Project Management Institute (PMI) or similar industry-standard project management standards and approach throughout the Contract term. The offer must describe their approach to meet each of the Project Management requirements defined in Attachment F, Requirements Matrix.

The most important project management principle we bring to the MPATH project is an emphasis on communication and collaboration with the Department and its other contractors. We strive to keep transparent, open channels of communication between our projects and clients. Our Project Manager, Juli Mattfeldt, a current resident of Helena, will be onsite and dedicated full time to the project. She will work closely with State staff on a daily basis to provide accurate communication, build collaboration with all team members, and lead the successful implementation of our solution. Ms. Mattfeldt is a certified Project Management Professional (PMP) and is experienced in establishing and enforcing Project Management Plans and implementing Provider Services systems. She led the implementation of our District of Columbia project and has current relevant experience as well as a long history of working on projects for the State of Montana.

In addition to our adherence to PMBOK® principles, we established our own set of best practices through our years of project transitions and implementations, and compiled them into Project Implementation and Project Management Manuals that supplement PMBOK® in guiding our projects to success. These manuals are based on our deep experience starting up and operating projects and contain well-defined policies and procedures covering both internal project management and corporate oversight requirements. Our experience has helped us be successful in a variety of landscapes and cultures. MAXIMUS reliance on PMBOK® principles and our own Project Implementation and Project Management Manuals will help the project operate in a disciplined, well-managed, and consistent manner, promoting the delivery of quality products and services in a timely and cost-effective fashion.

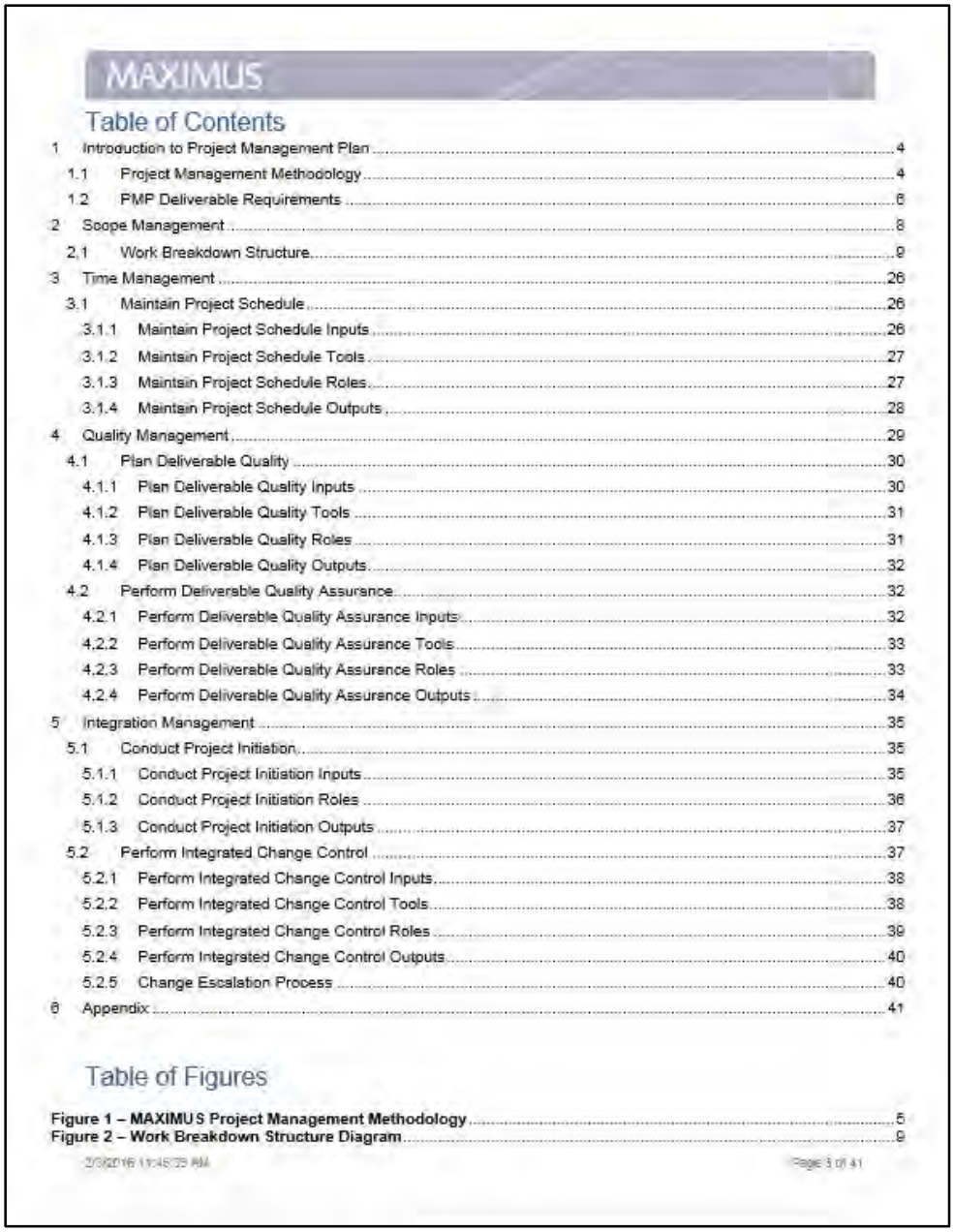
As a matter of course, MAXIMUS follows quality management standards established by the International Organization for Standardization (ISO 20000 and ISO 9001 standards) to define and document all functions as repeatable processes, decrease variability through business process improvement, and reduce the chances of human error. Our expertise in applying PMBOK® and ISO standards and methods, paired with our business process management (BPM) methods and tools, gives us the flexibility to manage and rapidly respond to changes as they occur during implementation. We look forward to bringing this innovative expertise to Montana and deliver project efficiencies that significantly improve Provider services.

To implement the Provider Services module, MAXIMUS will tailor our project management methodology based on the specific RFP requirements and the knowledge obtained on past projects to deliver a Project Management Plan that provides:

- Communication Plan
- Project Status Reporting Procedures
- Change Management Plan
- Work Breakdown Structure
- Staff Management Plan & Organizational Structure
- Quality Management Plan
- Risk Management Plan
- Issue Management Plan
- State-approved Deliverable Review Process
- Procedures and Tools for Retaining and Updating Project Documentation

The Project Management Plan will provide a comprehensive baseline of what needs to be achieved by the project, how it is to be achieved, who will be involved, how it will be reported and measured and how

information will be communicated with the project. The Department-approved Project Management plan will serve as a reference to guide decisions and clarifications on the project. As the project evolves, we will keep the Project Management Plan current with the latest relevant information as required. In the sub-sections that follow, we provide the details of how we plan and manage each of the key project management activities in the Project Management Plan. *Exhibit 3.10.2.1-1: Sample Project Management Plan Table of Contents* shows a snippet from the Implementation Plan we submitted for the District of Columbia.



MAXIMUS

Table of Contents

1 Introduction to Project Management Plan 4
1.1 Project Management Methodology 4
1.2 PMP Deliverable Requirements 6
2 Scope Management 8
2.1 Work Breakdown Structure 9
3 Time Management 26
3.1 Maintain Project Schedule 26
3.1.1 Maintain Project Schedule Inputs 26
3.1.2 Maintain Project Schedule Tools 27
3.1.3 Maintain Project Schedule Roles 27
3.1.4 Maintain Project Schedule Outputs 28
4 Quality Management 29
4.1 Plan Deliverable Quality 30
4.1.1 Plan Deliverable Quality Inputs 30
4.1.2 Plan Deliverable Quality Tools 31
4.1.3 Plan Deliverable Quality Roles 31
4.1.4 Plan Deliverable Quality Outputs 32
4.2 Perform Deliverable Quality Assurance 32
4.2.1 Perform Deliverable Quality Assurance Inputs 32
4.2.2 Perform Deliverable Quality Assurance Tools 33
4.2.3 Perform Deliverable Quality Assurance Roles 33
4.2.4 Perform Deliverable Quality Assurance Outputs 34
5 Integration Management 35
5.1 Conduct Project Initiation 35
5.1.1 Conduct Project Initiation Inputs 35
5.1.2 Conduct Project Initiation Roles 36
5.1.3 Conduct Project Initiation Outputs 37
5.2 Perform Integrated Change Control 37
5.2.1 Perform Integrated Change Control Inputs 38
5.2.2 Perform Integrated Change Control Tools 38
5.2.3 Perform Integrated Change Control Roles 39
5.2.4 Perform Integrated Change Control Outputs 40
5.2.5 Change Escalation Process 40
6 Appendix 41

Table of Figures

Figure 1 – MAXIMUS Project Management Methodology 5
Figure 2 – Work Breakdown Structure Diagram 9

Exhibit 3.10.2.1-1: Sample Project Management Plan Table of Contents. *MAXIMUS submits a Project Management Plan to DPHHS, which outlines our project management approach for successfully delivering the Provider Services solution. We tailor our previously created planning documents to meet the requirements of each State.*

3.10.2.1.1Communication Plan

MAXIMUS project management methodology enables a communication process where stakeholder needs are aligned with the work to be performed and where all parties involved agree on the desired results prior to beginning the work. We establish a process to achieve the complete communication lifecycle. We accomplish this by confirming that stakeholder needs are communicated to the performing project team, and the project team provides timely feedback to management. Management, in turn, communicates results and corrective action to the stakeholders, and the project team completing a fully integrated schedule of communication. MAXIMUS communication management approach consists of three key processes:

- Communication planning
- Performance reporting
- Administrative closeout

Communication throughout the project lifecycle is an integral part of the MAXIMUS project management methodology.

MAXIMUS begins the development of the communication plan by working with State staff to identify the project stakeholders, as well as their roles, responsibilities, and communication needs. The Communication Plan identifies those groups as well as others who are likely to be stakeholders in the project and will require information about the project. During project initiation, MAXIMUS finalizes the stakeholder identification based on discussions with State management and builds a matrix of communications needs for each stakeholder.

A primary communication vehicle on the project is the detailed project work plan. The detailed project work plan contains all activities required for successful project completion, including the appropriate dependencies between activities as well as the expected activity duration. By including all activities and their related dependencies, project leaders are assured that completion of the activities on the schedule will lead to a successful project implementation. The detailed project work plan contains the critical path marking the set of activities and durations that, if changed, will change the project schedule. We update the project schedule each week, so that our management team can assess progress and make updates to staffing or delivery to eliminate possible delays. By updating the detailed project work plan each week with actual progress on activities, the schedule will accurately reflect the current plan for completing the project.

The MAXIMUS Project Manager is responsible for communicating project status to all interested stakeholders. *Exhibit 3.10.2.1-2: Primary Communications Vehicles* shows the primary communication methods we use as a part of our overall communications plan.

Communication Vehicle	Purpose
Detailed project work plan	Control scope and activity, coordinate communication, and document responsibility
Schedule Review and Status Meetings	Monitor and control activity, communicate plans and results, support risk mitigation, and enforce accountability
Weekly Project Status Report	Monitor, control and report on the state requirements, and communicate project metrics
Monthly Project Status Report	Focus on schedule activity. Report on adherence to the plan, updates based on activity, and scheduled tasks
Executive Steering Committee Meeting	Provide direction and management, secure executive commitment, and resolve issues among internal or external stakeholders
Project Change Request	Integrated analysis, planning, and implementation of project changes including scope, schedule, and cost updates
Outreach Sessions	When Option B is selected, describes outreach materials and sessions planned for Providers **NOTE:** Outreach sessions/initiatives for Providers will primarily be for re-enrollment and revalidation
Web-based Outreach Initiatives	Describes the project's approach to providing web-based outreach initiatives to Providers

Exhibit 3.10.2.1-2: Primary Communication Vehicles. *MAXIMUS manages projects throughout each stage of the project lifecycle using a proven project management methodology for consistency and success.*

In addition to these formal communication methods, our focus on collaboration yields other types of less formal yet practical types of communications on the project. Other types of communications may include:

- Email
- Informal meetings
- Other ad hoc communications

These communications will likely represent the bulk of the information exchange that occurs on the project. However, MAXIMUS specifies the formal vehicles necessary to confirm we properly communicate critical management information so that all parties have the same understanding of discussions, issues, and approach. Our Project Manager monitors informal communications, and includes information in our more formal communication methods, when appropriate. *Exhibit 3.10.2.1-3: Sample Communication Management Plan* shows a snippet from the Implementation Plan we submitted for the District of Columbia.

1 Introduction to Project Communication Plan

MAXIMUS believes that consistent and effective communication is the cornerstone of a successful partnership with the District. Communications Management includes the processes required to ensure the timely and appropriate generation, collection, distribution, and storage of project information. It describes the mechanisms for communication between project members and the method(s) of distribution for different types of communications. The plan serves as a guide for communications throughout the life of the project and can be updated if and when requirements change. This plan is an extension of the Project Management Plan and is based on the processes described for Communications Management in the Project Management Institute's (PMI) Body of Knowledge (PMBOK). Table 1 describes the processes involved in Communications Management.

Table 1 - Communications Management Processes

Process	Description
Identify Stakeholders	The process of identifying all people or organizations impacted by the project, and documenting relevant information regarding their interests, involvement, and impact on project success.
Plan Communications	The process of determining the project stakeholder information needs and defining a communications approach.
Distribute Information	The process of making relevant information available to project stakeholders as planned.
Report Performance	The process of collecting and distributing performance information, including status reports, progress measurements, and forecasts.
Manage Stakeholder Expectations	The process of communicating and working with stakeholders to meet their needs and addressing issues as they occur.

This Project Communication Plan establishes the communications framework for the project. The plan defines the communications needs and expectations for the project, including:

- The information that will be communicated
- How the information will be communicated
- When or at what frequency the information will be communicated
- From whom the communication will originate and to whom the communication will be sent

1.1 Project Communication Plan Deliverable Requirements

The goal of this plan is to ensure communication requirements described in the contractual agreement between the District and MAXIMUS are adhered to and that there are clear guidelines for disseminating

Exhibit 3.10.2.1-3: Sample Communication Management Plan. *MAXIMUS submits a Communication Management Plan to DPHHS, which outlines our communication management approach for successfully delivering the Provider Services solution. We tailor our previously created planning documents to meet the requirements of each State.*

Project participants and stakeholders regularly receive consistent, accurate information about the project, which allows them to make informed decisions and closely monitor activities progress. MAXIMUS will produce a weekly project status reporting during the DDI phase of the MPATH project and during our post-implementation support period. The project status reports will be placed on the project's SharePoint repository to allow access for all required stakeholders. The weekly status report contains multiple sections that will provide the Department and other project stakeholders with an accurate summary of the current project status and directly align with our project management processes so they become an integrated component of our project delivery tasks.

This will include an up-to-date detailed project work plan and the status of any known project risks or issues.

3.10.2.1.2Project Status Reports and Meeting Procedures

MAXIMUS project status monitoring incorporates a consistent and proven process that provides our clients with the progress data they need to accurately assess the status of the project, understand project issues, address issues and risks, and resolve time critical action items. We use a weekly status report supported by a status meeting to keep focus on current project activities and identification of any issues that are impacting the plan. The MAXIMUS status report template uses dashboard indicators to give a high-level assessment of the project and then provides the details in the report to support those assessments. *Exhibit 3.10.2.1-4: Project Dashboard* shows the dashboard indicators and criteria used to assign the project health indicators. The MAXIMUS project status report template is structured, informative, and written at a level that is easy for business staff to quickly comprehend the progress to date, plans for the future, and staffing responsibilities and the decisions required to keep the project moving forward according to plan. During Project Initiation, we will work with DPHHS to confirm the project indicators are accurate and the level of data contained in the report is appropriate for the audience.

Project Health Check					
Status	**Schedule**	**Scope**	**Quality**	**Risk**	**Resources**
Green	X	X	X	X	X
Yellow					
Red					

Project Health Check Status Definitions			
Project Area	***Green (Controlled)***	***Yellow (Caution)***	***Red (Critical)***
Schedule	Critical Path Tasks and all deliverables have been completed or are estimated to be completed on schedule.	One or more Critical Path tasks or deliverables are at least one week behind schedule.	One or more Critical Path tasks or deliverables are at least two weeks behind schedule.
Scope	There are less than 2 active issues related to scope or less than 2 active change requests related to scope.	There are more than 2 active issues related to scope or more than 2 change requests related to scope.	There are more than 5 active issues related to scope or more than 5 change requests related to scope.
Quality	Quality processes defined in the PMP or other plans are being followed. No deliverables are unapproved due to quality issues.	Quality issues are developing, as deliverable reviews are taking longer than expected due to a significant volume of defects or comments.	One or more deliverables are currently unapproved due to quality issues.
Risk	There are less than 2 active risks without a mitigation plan.	There are 3 or more active risks without a mitigation plan.	There are 5 or more active risks without a mitigation plan.
Resources	Necessary resources are available as needed.	Resource availability issues are beginning to affect our ability to complete project tasks.	Resource availability is seriously affecting project performance and needs to be reviewed

Exhibit 3.10.2.1-4: Project Dashboard. *MAXIMUS will carefully manage and report the status of the MPATH project on a weekly basis using a formal written status report.*

An agenda and copy of both the weekly and monthly status reports and presentation materials will be delivered to DPHHS at least 24 hours prior to every meeting. Weekly status meetings are targeted to the project team members from MAXIMUS and DPHHS and address the day-to-day tasks and assignments. Monthly status meetings provide a high-level view of the project for senior management and other

stakeholders. MAXIMUS uses ReadyTalk™ for web conferencing and to record the meetings. ReadyTalk allows remote attendees to view and participate at project meetings. These recordings are used to create the minutes, which are submitted within 48 hours after the meeting for DPPHS review, editing, and approval.

MAXIMUS is meticulous about tracking the progress of the project. We require all project staff members to report progress against their individual assignments on a weekly basis so completion percentages can be applied to the project plan task and an accurate assessment of the project completion can be reported in relationship to the planned progress to date. This level of detail is necessary to provide accurate earned value and variance reporting of the project progress. The Project Management Plan will include tasks and/or sub-plans for other contractors and DPHHS responsibilities so a “big picture” view of all work to be completed and task dependencies across all organizations can be identified and tracked. We submit an updated and current Project Schedule as an electronic attachment with each monthly status report submission.

The weekly project status report is a comprehensive and detailed assessment of the project status that is the basis for the management team to discuss progress to date, issues that occur, and plan for the activities in the next reporting period. The status report provides a list of all tasks completed during the prior reporting period, all tasks that are past due, and tasks planned to start in the next reporting period. It is an important meeting because it provides current relevant information about the project.

The Deliverables table shows all product deliverables, their current status (planned, in progress, submitted, review, and approved), planned submission date, actual submission date, percent complete, approval date, payment amount (if applicable), invoice date, payment status and date.

Key staff changes are addressed through the change request process while non-key changes are reported in the staffing section of the status report and reflected in the Resource Matrix view of the project schedule. The status report also includes sections that show active issues, risks, outstanding action items, and pending decisions. We report the active Action Items, Risks, Issues, and Decision Registers weekly in the status report. Closed and inactive items are retained in the registers indefinitely for historical and reference purposes.

As the project progresses, we report additional metrics based on relevance. As an example, during the development phase, we report application component coding and unit testing progress at the component level. Similarly, we report test execution and defect remediation statistics in the status for all testing phases.

As required by the RFP, MAXIMUS will also conduct a monthly status meeting. This meeting will focus principally on the project schedule and contain a detailed review of the progress that occurred during the month, the plan for upcoming tasks, specific discussions about updates to the plan to alleviate issues, and updates made based on progress. We anticipate a collaborative setting where parties are prepared to contribute to solutions related to required plan updates, issues, or risk mitigation. Since we update the schedule weekly, we will produce an end of month update to support the discussions for this meeting. The monthly report provides virtually the same information that the weekly status reports provide, but at a higher level to allow DPHHS, IV&V, and State CIO management to quickly understand the progress of the project, risks and issues and make an accurate assessment of the project health. This report will also provide the information to support the State CIO’s Legislative Finance Committee reporting.

After implementation, the monthly status report includes an assessment of all Operations and Maintenance (O&M) SLA's and will show each target performance goal and MAXIMUS' compliance or deficiency. In the event there is a deficiency, MAXIMUS will provide an explanation of why the target was missed and an action plan for achieving the goal in the next reporting period.

We track and report System Enhancement Pool hours in a table similar to the one shown in *Exhibit 3.10.2.1-5: System Enhancement Pool Report*. This report includes a comprehensive view of the enhancements requested, approval status, estimated, actual and variance hours and implementation release plan.

System Enhancement Pool Report for the Base Contract Period								
4,000 Hours in Year 1 Contract								
Change Request Description	Submitted For Review	Status	Approved Date	Estimated Hours	Actual Hours	Estimate Variance	Target Release	Date Implemented
CR-01 EIN and SSN Changes	10/9/2016	Approved	10/19/2016	100	109	9	1.1.0	11/8/2016
CR-02 Contact Name for Addresses	10/22/2016	Approved	11/1/2016	52	56	4	1.1.1	11/21/2016
CR-03 New document upload	12/5/2016	Approved	12/15/2016	174	165	(9)	1.1.2	1/4/2017
CR-04 Address Changes	1/3/2017	Approved	1/13/2017	190	189	(1)	1.1.3	2/2/2017
CR-05 Group Affiliation Changes	1/25/2017	Approved	2/4/2017	185	203	18	1.1.4	2/24/2017
CR-06 Additional Agency Changes	4/29/2017	Approved	5/9/2017	79	78	(1)	1.1.5	5/29/2017
CR-07 Specialty Codes Change	6/10/2017	Pending	TBD	70	75		1.1.8	
Total Hours				**850**	**875**	**Hours Remaining**		**3,125**

Exhibit 3.10.2.1-5: System Enhancement Pool Report. *MAXIMUS will carefully manage and report the status of the enhancement pool hours on a weekly basis.*

3.10.2.1.3Change Management Plan & WBS

The primary tool we use for scope management is the Work Breakdown Structure (WBS). The WBS is a deliverable-based hierarchy of all activities required to complete the project. The WBS describes each planned activity in terms of the work to be performed and the general criteria required for completion. The WBS is a complete listing of all activities and deliverables expected on the project. It serves as the primary classification scheme for work performed on the project, and we discuss all change requests in terms of their impact on the WBS deliverables and activities. MAXIMUS will develop the WBS as part of the project initiation tasks for inclusion in Project Management Plan.

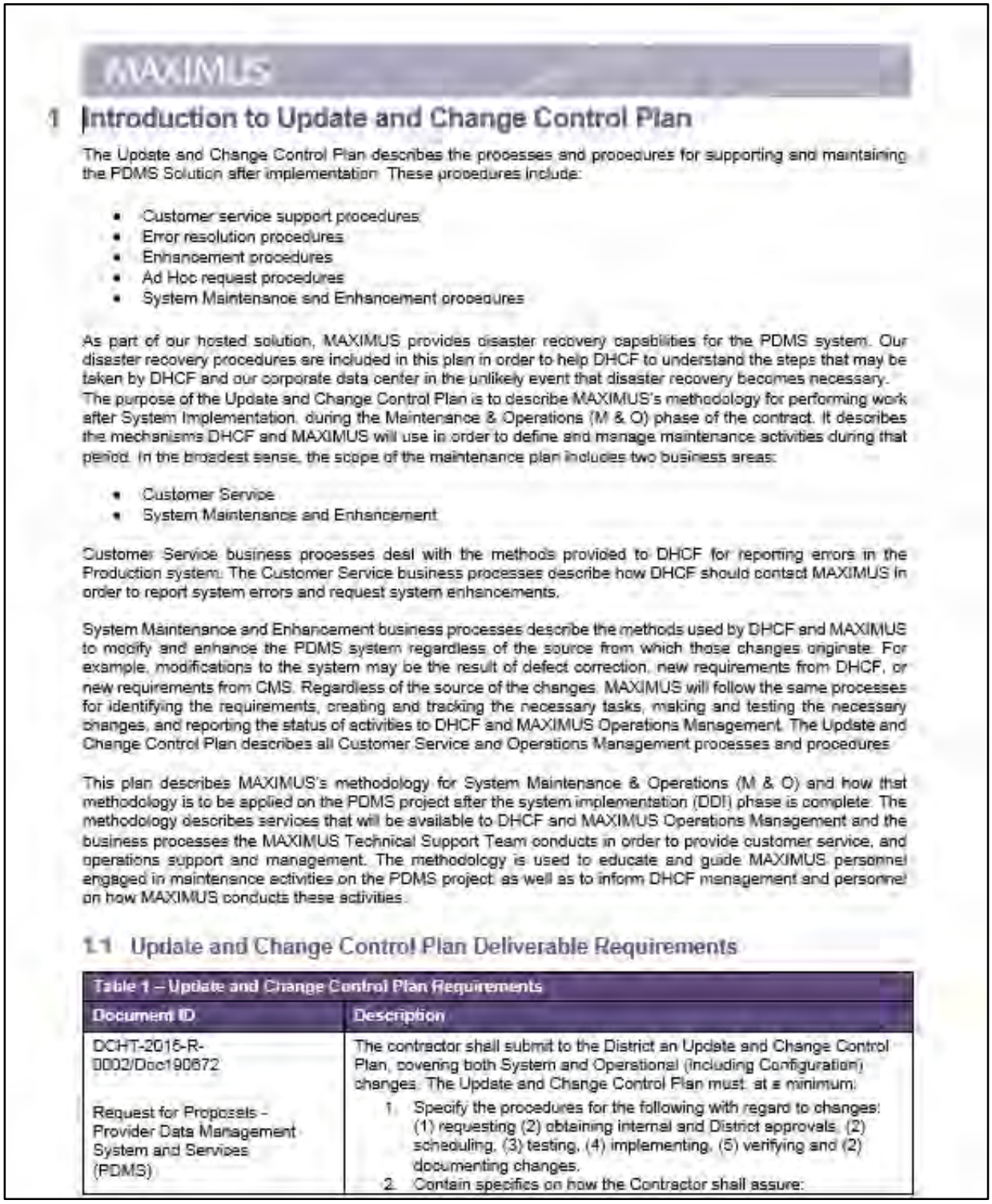
One of the risks inherent in a project of this size and scope is "scope creep"— a gradual, unintended increase in work that the parties believe needs to be performed to meet the project requirements. The MAXIMUS methodology of documenting the WBS and integrating it with the key process areas on the project is an active defense against scope creep, since the entire Project Management Plan is based on a common set of expectations from the very beginning. By definition, activities and deliverables contained in the WBS are "in scope" and those not in the WBS are "out of scope." Out-of-scope activities and deliverables require a change request before we can work on them because the project team is not authorized to expend time or resources on them otherwise.

To respond to and implement requested changes in the project time frames, we propose the following set of guidelines:

- Only the Department or MAXIMUS project management staff can request project changes

- Once a change request has been initiated, MAXIMUS will respond to the request and provide a written level of effort according to the service level agreements defined in the RFP
- The Department will respond to the MAXIMUS proposal either approving or denying the request
- The weekly status report will show all change requests along with their status
- We will define an escalation approach for changes that cannot be agreed to within the project.

Should any project stakeholder determine a change in requirements is necessary during any phase of the project, the WBS provides an excellent tool for quantifying and analyzing the appropriate changes necessary to meet the new requirements. Each change can be expressed in terms of its effect on the WBS, which can in turn be mapped to changes required in the deliverables, project schedule, cost estimate, and other key process areas of the project. *Exhibit 3.10.2.1-6: Sample Change Management Plan* shows a snippet from the Change Management Plan we submitted for the District of Columbia.



MAXIMUS

1 Introduction to Update and Change Control Plan

The Update and Change Control Plan describes the processes and procedures for supporting and maintaining the PDMS Solution after implementation. These procedures include:

- Customer service support procedures
- Error resolution procedures
- Enhancement procedures
- Ad Hoc request procedures
- System Maintenance and Enhancement procedures

As part of our hosted solution, MAXIMUS provides disaster recovery capabilities for the PDMS system. Our disaster recovery procedures are included in this plan in order to help DHCF to understand the steps that may be taken by DHCF and our corporate data center in the unlikely event that disaster recovery becomes necessary. The purpose of the Update and Change Control Plan is to describe MAXIMUS's methodology for performing work after System Implementation, during the Maintenance & Operations (M & O) phase of the contract. It describes the mechanisms DHCF and MAXIMUS will use in order to define and manage maintenance activities during that period. In the broadest sense, the scope of the maintenance plan includes two business areas:

- Customer Service
- System Maintenance and Enhancement

Customer Service business processes deal with the methods provided to DHCF for reporting errors in the Production system. The Customer Service business processes describe how DHCF should contact MAXIMUS in order to report system errors and request system enhancements.

System Maintenance and Enhancement business processes describe the methods used by DHCF and MAXIMUS to modify and enhance the PDMS system regardless of the source from which those changes originate. For example, modifications to the system may be the result of defect correction, new requirements from DHCF, or new requirements from CMS. Regardless of the source of the changes, MAXIMUS will follow the same processes for identifying the requirements, creating and tracking the necessary tasks, making and testing the necessary changes, and reporting the status of activities to DHCF and MAXIMUS Operations Management. The Update and Change Control Plan describes all Customer Service and Operations Management processes and procedures.

This plan describes MAXIMUS's methodology for System Maintenance & Operations (M & O) and how that methodology is to be applied on the PDMS project after the system implementation (DDI) phase is complete. The methodology describes services that will be available to DHCF and MAXIMUS Operations Management and the business processes the MAXIMUS Technical Support Team conducts in order to provide customer service, and operations support and management. The methodology is used to educate and guide MAXIMUS personnel engaged in maintenance activities on the PDMS project as well as to inform DHCF management and personnel on how MAXIMUS conducts these activities.

1.1 Update and Change Control Plan Deliverable Requirements

Table 1 – Update and Change Control Plan Requirements	
Document ID	**Description**
DCHT-2018-R-0002/Doc190672 Request for Proposals – Provider Data Management System and Services (PDMS)	The contractor shall submit to the District an Update and Change Control Plan, covering both System and Operational (including Configuration) changes. The Update and Change Control Plan must, at a minimum: 1. Specify the procedures for the following with regard to changes: (1) requesting (2) obtaining internal and District approvals, (2) scheduling, (3) testing, (4) implementing, (5) verifying and (2) documenting changes. 2. Contain specifics on how the Contractor shall assure:

Exhibit 3.10.2.1-6: Sample Change Management Plan. *MAXIMUS submits a Change Management Plan to DPHHS, which outlines our approach for successfully managing change on the Provider Services solution. We tailor our previously created planning documents to meet the requirements of each State.*

3.10.2.1.4Staffing Management Plan

We develop the WBS and detailed project work plan as tools to determine the right mix of people and skills needed for this project, as well as the timing and duration for personnel assignment. The WBS describes the project deliverables and their related activities. The detailed project work plan details the tasks required to perform each WBS activity and establishes the sequence in which staff must perform them. When placed on a timeline, this schedule allows management to determine the appropriate personnel for each task, aggregate and balance the activities of those personnel, and ultimately develop a project organization.

To staff our projects appropriately, we develop a staffing plan based on both the WBS and detailed project work plan. This plan contains the number of staff required for each task based upon the activities to be completed in the detailed project work plan and the timeline set forth by the client. This defines when staff will be required, what they will be doing, and what skill sets are necessary. This planning activity assigns resource requirements based on the detailed project work plan so resources can be assigned to complete the required tasks. This also allows us to continually review progress against the schedule and make adjustments as required to the number and make-up of personnel on the various project teams.

To estimate time and resources for a new project or any change requests that may be approved, we examine the type of work being performed and determine a comparable effort on previous projects. We review the hours spent, duration of tasks within the activity, and number and kind of resources required to complete the effort. Comparing the data for this activity to the one required by the RFP or change request, we adjust the numbers to reflect the scope of effort. We also take into consideration the skill level of resources dedicated to an activity in determining our estimate, considering standard productivity levels. Our resource planning for the MPATH project is based on our experience in performing three similar implementations for our Provider Services module. Combined with our sound project management resource planning best practices, we are confident in our resource allocation and estimates for the MPATH project.

As we assign resources to the scheduled tasks, we review the impact the assigned resources have on the overall schedule. We continue to derive, in this fashion, the number of resources necessary to complete each phase of the project in the required timeframe while allowing for maximum flexibility within the schedule's critical path to provide room for contingencies. We manage the project resources by repeating the same process we used for developing the initial project cost estimate and resource-staffing plan. We examine dependencies that exist between activities, subtasks, or phases within a task, and we confirm that no technical or human resource is over allocated or overburdened. This integrated approach to staffing and time estimating will give Montana confidence in our estimates for the scope of work we propose and in our ability to fulfill our obligations as the project is executed. Refer to *Section 3.10.5–Personnel*, for details regarding our organization structure and our assigned personnel that will be dedicated to the MPATH project.

Our detailed staff planning activities result in a Staffing Plan that is a component of our Project Management Plan. We will review and finalize the plan during project initiation. The Plan will:

- Identify the roles and responsibilities by resource type throughout all phases of the contract, including identifying key and non-key personnel as well as FTE allocation for all personnel.

- Identify Staffing Levels (estimated by resource type by phase for the duration of the project) to be reported in the Resource Allocation Matrix.
- Detail how the staffing levels shall achieve consistent, dependable service regardless of changes that may influence work volume.
- Detail differentiated by Proposer staff, subcontractor staff, if applicable, and State project staff.
- Identify total hours to be expended, per phase or effort, and for the entire project, by Proposer staff and by State project staff.
- Identify tools and processes used to screen available staff and fill positions.
- Define expectations regarding onsite time for contractor resources
- Include a process for temporarily and permanently replacing vacancies in key personnel and other manager/lead positions consistent with staffing SLAs.

Exhibit 3.10.2.1-7: Sample Staffing Plan shows a snippet from the Staffing Plan we submitted for the District of Columbia.

MAXIMUS

1 Introduction to Project Staffing Plan

Human Resources Management includes the processes that are used to acquire, organize, and manage Human Resources on a project. This section does not discuss how MAXIMUS acquires staff for the DDI phase of the project, and focuses mainly on the Human Resources already assigned to the project.

In the operations phase of the project, after DDI, we evaluate our workforce management approach and ongoing staffing requirements. This plan identifies how we will recruit and hire any necessary new project staff to augment our existing staff or reduce the size of the staff, depending upon the coming year's projected requirements for enrolling new Providers and revalidating the enrollment of existing Providers based on the schedule established by federal and District regulations. It also identifies any necessary changes to our management approach for overseeing staff in our District office as well as in the field.

Table 1 – Human Resources Management Processes

Process	Description
Maintain Staffing Plan	Maintaining the Staffing Plan is the process by which MAXIMUS estimates the staffing resources needed during each phase of the project.

1.1 Staffing Plan Deliverable Requirements

Table 2 - Project Staffing Plan Requirements

Document ID	Description
DCHT-2015-R-0002/Doc190672 Request for Proposals – Provider Data Management System and Services (PDMS) C.5.2.1.3	Deliver a Staffing Plan that describes the personnel resources required for the project. The Staffing Plan must, at a minimum: 1. Identify all Contractor staff, including all sub-contractors to be assigned (e.g., total number of persons, skill sets, and percentage of time to be spent on the project); 2. Identify District staff assignment needs (e.g., total number of persons, skill sets, and percentage of time needed on the project); and 3. Identify roles and responsibilities of all staff during all phases of the project.

The project is being performed on a fixed-price contract. Because the contract is fixed-price, the actual cost for resources that perform work on the project does not impact the cost to the District. However, as requested in the RFP, MAXIMUS has provided the Staffing Plan shown below. Table 3 identifies the primary human resources that MAXIMUS will be used on the project during the DDI phase. However, MAXIMUS may use additional short-term Human Resources on the project when a particular person has a specific skill or knowledge that is useful to helping complete the project.

Note: The staffing plan for the MAXIMUS Operations Staff post implementation is described in detail in the Operations Plan. Please refer to that document for the Staffing Plan for that phase of the project. Table 3 only describes the staffing plan for the DDI phase.

Exhibit 3.10.2.1-7: Sample Staffing Plan. *MAXIMUS submits a Staffing Plan to DPHHS, which outlines our approach for successfully staffing the Provider Services solution. We tailor our previously created planning documents to meet the requirements of each State.*

3.10.2.1.5 Quality Management Plan

Quality management consists of processes and activities to determine quality policies, objectives, and responsibilities that satisfy the project requirements set forth by the customer. To be effective, quality management must be embedded into the project delivery activities and time must be set aside to identify quality objectives and to monitor adherence to those objectives as deliverables are developed. MAXIMUS approaches quality management from planning, control, and assurance standpoints. These functions are part of the project management controls focused on preventing defects rather than on finding them after they occur. This is an important distinction between our approach and many other vendors because we believe that providing deliverables that meet our customer's requirements the first time is a key aspect of project success and customer satisfaction. In addition, this approach allows us to focus on the delivery activities rather than the correction of reviewed deliverables. This approach allows the project team to focus value added tasks geared toward project implementation. To make sure we adhere to the required quality requirements and the SLAs for the MPATH project, we have proposed a full-time Compliance Manager who will be committed to making sure that project deliverables are produced when scheduled and conform to quality requirements and SLAs for the project.

To achieve our quality objectives, we will work with the State to identify the appropriate process and product standards we will use to govern all activities on the project. This will begin during Project Initiation and result in our Quality Management plan, which will be a part of the overall Project Management Plan for the MPATH project. We develop quality metrics used to gauge the quality of work. We will include relevant information in our Project Status Report that reflects actual progress against the project's quality standards.

As MAXIMUS produces deliverables, the delivery staff reference specific quality checklists, developed during the definition of the deliverable, required for the deliverable to be considered complete. The entire team will be oriented to the defined quality metrics. All deliverables will have the same look and will be easy to review. This will allow the State reviewers to focus on the content rather than other items that diminish the quality of the products and add to the complexity of the review process. As we draft deliverables, we will follow up the work with a formal quality review and correction period prior to the submission of the deliverable to the State. This will provide a final check that the deliverable meets the requirements as specified and the scope of work proposed. *Exhibit 3.10.2.1-8: Sample Quality Management Plan* shows a snippet from the Quality Management Plan we submitted for the District of Columbia.

MAXIMUS

1 Deliverables Requirement

Table 2 - Operations Plan Requirements	
Document ID	**Description**
DCHT-2015-R-0002/Doc190672 Request for Proposals - Provider Data Management System and Services (PDMS) C.5.2.1.6.9	Plan shall define the content and format of the Quality Control and Assurance Report(s) that shall be produced during the Operational Phase including, at a minimum: 1. Quality Control and Assurance Issue Log 2. Quality Control and Assurance Operational Activities

1.1 Quality Control

Quality control is built into every step of our operations allowing us to monitor both efficiency and effectiveness of Provider services as they occur. It includes the processes built directly into our business operations that ensure all work is performed according to specifications. All project staff follows established guidelines and documented processes to help ensure that the completion of each required task or activity is consistent, comprehensive, and in compliance with the scope of the contract. Quality control is performed for each area of our operations including:

- PDM Call Center Quality Control: Quality control is built directly into the operational aspects of the contract so as to enable immediate remediation of any quality problems. Our Account Manager and Operations/Provider Relations Manager monitors Provider interactions with the Call Center on an ongoing basis, ensuring that calls are conducted with respect and efficiency.
- Provider Enrollment Quality Control: Processing Provider applications and revalidations in DecisionPoint involves multiple steps, where different workers may be responsible for different pieces of the enrollment process for a given Provider application. This enables us to have the worker performing a given function review and identify any quality problems with previous steps.
- Site Visit Quality Control: Site visits require sign-off by both the Site Visit Specialist and the Provider being reviewed. The site visit process includes a standardized checklist as a built-in mechanism for quality control. All items on the checklist must be completed before the visit can be considered complete. Further, our Operations/Provider Relations Manager spot checks the site visit checklists to ensure that they comply with project standards. Our Operations/Provider Relations Manager may also occasionally accompany the Site Visit Specialist on site visits as an additional means of ongoing quality control.

1.2 Quality Assurance

While quality control activities are conducted "in process" as various operational activities occur, our quality assurance reviews provide "after the fact", retrospective validation of compliance with standards and metrics. Quality assurance activities include:

- PDM Call Center Quality Assurance: Our QA/Training Analyst conducts silent, live monitoring of CSR calls for quality assurance and training purposes. The QA/Training Analyst uses a checklist to evaluate calls and assess each CSR's performance in delivering accurate and appropriate information to Providers. Call monitoring focuses on several areas, including authentication of Providers, program knowledge, customer service skills, ability to resolve help desk inquiries, and proper documentation of the call in DecisionPoint.
- Provider Enrollment Quality Assurance: Our QA/Training Analyst reviews a sample of processed applications to ensure accuracy, timeliness, and compliance with regulations. Real-time dashboards in DecisionPoint facilitate this review process by providing a snapshot of up-to-date information on all applications, by Provider type, along with aging data.

Exhibit 3.10.2.1-8: Sample Quality Management Plan. *MAXIMUS submits a Quality Management Plan to DPHHS, which outlines our approach for managing the quality of the Provider Services solution. We tailor our previously created planning documents to meet the requirements of each State.*

We will utilize our quality management processes across all aspects of the project. We clearly understand that high quality work equals client satisfaction and project success. The MAXIMUS team is committed to delivering high quality work products to the State; we will follow the defined quality processes to attain that goal. Our demonstrated history of success in Provider Services implementations has helped us focus on the right activities to keep the project on schedule, and delivery needed information to our customers.

3.10.2.1.6 Risk Management Plan

Risk Management is a critical component of successful project delivery. Accordingly, our project management methodology calls for the implementation of a set of activities that expose project risks and set forth a structure for mitigation. We examine assumptions, constraints and dependencies for hidden risks and harvest potential risk statements from previous projects' risk logs. In addition, we require all project team members to participate in the risk management processes to address all avenues for risk introduction.

To be effective, risk management must occur as a regular part of project delivery. We recommend that proactive risk identification be part of the daily work process and that it be performed at the initiative of all project members. As part of our Project Management Plan, MAXIMUS will develop a Risk Management Plan that will be used to document how risk management activities will be conducted on the project. Because risk management is key to project success, MAXIMUS has developed a standard Risk Management Plan format we use for all our projects. The outline of our standard Risk Management Plan is as follows:

- **Purpose:** In this opening section, we define risk management and state the purpose of a risk management plan, which is to describe the structured approach we will take to manage risk on a particular project.
- **Roles and Responsibilities:** Here we list project roles and describe the risk management responsibilities associated with those roles. Everyone has a role in managing project risk, and so this section will include MAXIMUS roles and responsibilities and those held by State staff members.
- **Risk Identification:** In this section, we define both how risks are proactively identified and the process project team members follow to document identified risks. One proactive method of identifying risks is to document team members' project assumptions and the constraints and dependencies under which the team members believe the project operates. We will maintain an inventory of these dynamic assumptions, constraints and dependencies as appendices to the risk management plan.
- **Risk Assessment:** The Risk Assessment section of the plan is where we describe how risks will be assigned impact rankings, probability coefficients and risk scores. MAXIMUS will validate the identification of the risk or risk related issues. We evaluate each risk for the failure modes of Quality, Technical, and Business and determine the adverse effects for each item.

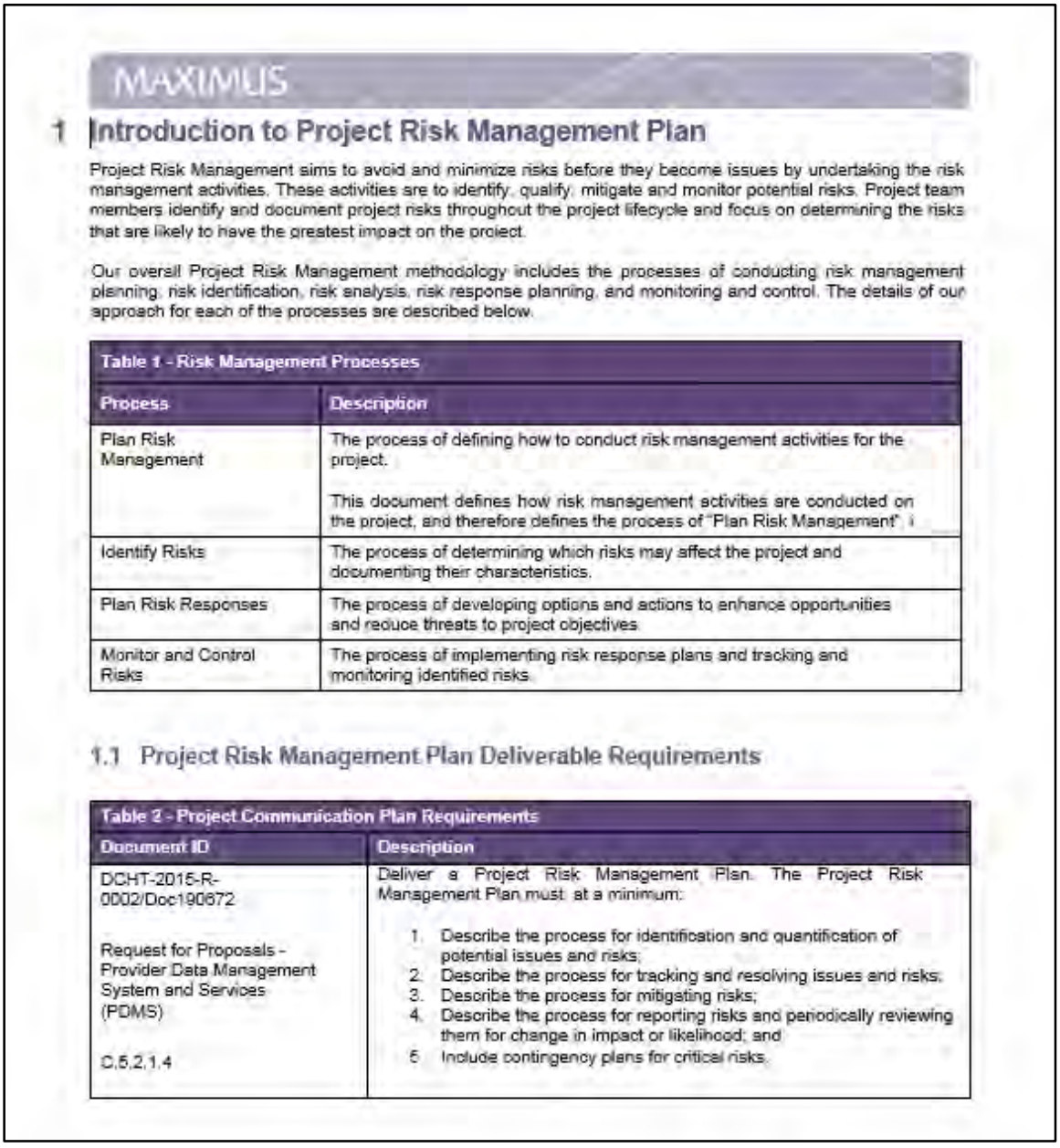
MAXIMUS will provide guidance and collaboration in risk analysis for each item so that the associated risks are fully analyzed. We rate the risk parameters for each risk scenario or event, as well as related adverse effects. For every risk scenario or event, MAXIMUS assigns a score indicating the likelihood of

occurrence, severity of the impact and probability for detection. We use a risk analysis matrix to analyze the rating of the Quality, Technical, and Business risks.

Our risk management approach is a team activity (conducted as a part of our regularly scheduled weekly status meeting). If there is insufficient information to assess the risk, the Project Manager is responsible for commissioning appropriate analysis and assigning resources necessary to perform risk assessment. Responses to risks may take one of several forms including:

- Avoiding the risk to prevent any damage to project outcomes
- Transferring the risk to another party
- Mitigating the potential effects of the risk on project outcomes and
- Accepting the risk in the event the impact of the risk occurring is relatively low or it is very unlikely to occur

MAXIMUS understands that risk management takes time and resources and the results of the effort must be beneficial to the project. We focus on real project risks that could occur based on the constraints and external factors that impact the project. During the project initiation activities, MAXIMUS will meet with the Department's management staff and jointly conduct risk assessment sessions to identify project risks and categorize them according to impact and probability. We capture the resulting information in the Project Risk Assessment, which documents and prioritizes risks according to their likelihood and severity. We then review the Project Risk Assessment with key State management staff to merge their assessments of overall program risk into the Project Risk Assessment. *Exhibit 3.10.2.1-9: Sample Risk Management Plan* shows a snippet from the Risk Management Plan we submitted for the District of Columbia.



MAXIMUS

1 Introduction to Project Risk Management Plan

Project Risk Management aims to avoid and minimize risks before they become issues by undertaking the risk management activities. These activities are to identify, qualify, mitigate and monitor potential risks. Project team members identify and document project risks throughout the project lifecycle and focus on determining the risks that are likely to have the greatest impact on the project.

Our overall Project Risk Management methodology includes the processes of conducting risk management planning, risk identification, risk analysis, risk response planning, and monitoring and control. The details of our approach for each of the processes are described below.

Table 1 - Risk Management Processes

Process	Description
Plan Risk Management	The process of defining how to conduct risk management activities for the project. This document defines how risk management activities are conducted on the project, and therefore defines the process of "Plan Risk Management".
Identify Risks	The process of determining which risks may affect the project and documenting their characteristics.
Plan Risk Responses	The process of developing options and actions to enhance opportunities and reduce threats to project objectives.
Monitor and Control Risks	The process of implementing risk response plans and tracking and monitoring identified risks.

1.1 Project Risk Management Plan Deliverable Requirements

Table 2 - Project Communication Plan Requirements

Document ID	Description
DCHT-2015-R-0002/Doc190672 Request for Proposals - Provider Data Management System and Services (PDMS) C.5.2.1.4	Deliver a Project Risk Management Plan. The Project Risk Management Plan must, at a minimum: 1. Describe the process for identification and quantification of potential issues and risks; 2. Describe the process for tracking and resolving issues and risks; 3. Describe the process for mitigating risks; 4. Describe the process for reporting risks and periodically reviewing them for change in impact or likelihood; and 5. Include contingency plans for critical risks.

Exhibit 3.10.2.1-9: Sample Risk Management Plan. *MAXIMUS submits a Risk Management Plan to DPHHS, which outlines our approach for managing risk on the Provider Services solution. We tailor our previously created planning documents to meet the requirements of each State.*

To enable continuous monitoring and management, those risks that are actively being managed through a risk management plan are included on the Project Status Report, along with any mitigation efforts agreed upon by the project team. Risk owners and responses are also included, if applicable. Project risks will be reviewed in scheduled project status meetings with appropriate staff from both DPHHS and MAXIMUS. This will enable project risks to be adequately managed throughout the project and that both the Department and MAXIMUS agree on how best to handle risks as they are identified and the project progresses.

3.10.2.1.7 Issue Management Plan

Issues, their causes, and their resolution are key project concerns and require a defined project management process to manage. Issues can cause conflicts among project resources and have potentially negative consequences for a project. Most issues that arise during a project are based on a lack of communication or a failure in the communication chain. MAXIMUS' goal is to minimize the number of project issues and potential disputes that can become barriers to project success by introducing processes that maintain efficient communications channels. We will work closely with the Department's management staff to identify the key communication mechanisms and adequately document them along with methods that allow any project staff member to voice their concerns about project or staffing items.

While we intend these processes to minimize the issues that surface on the project, we also understand that some project issues and/or disputes are unavoidable. We will implement a project infrastructure that allows for quick identification of issues, comprehensive issue tracking, and processes that require staff interaction/resolution as the first line of defense. Our intent by implementing these management controls is to avoid a long list of unresolved issues and having them escalate into incidents or full-fledged disputes. In addition, we want to avoid managing an issues list instead of the project schedule because in our experience when this occurs the project is a significant risk of failure. The relatively short duration of the project and the many interrelated activities require the implementation of fast and efficient resolution processes so that the detailed project work plan is not impacted.

If an issue should occur, we will resolve it as quickly and efficiently as possible. Any issues that can be resolved without escalation are put through the issues management process, which includes logging, prioritizing, and incident reporting, as appropriate. As issues are resolved, we track and cross-reference each resolution. The MAXIMUS project manager will maintain an issues log that tracks all identified project issues (including contractual issues) for resolution. For each issue, the project team will record the following information in the log:

- Issue Tracking Number
- Issue Description
- Issue Owner (may be blank for new issues)
- Actions/Updates
- Current Status
- Targeted Resolution Date

As soon as possible after documenting the issue, the MAXIMUS Project Manager will schedule a meeting with the State's Project Manager to discuss and resolve the incident in a mutually satisfactory manner. Within the weekly status report, we will list issues/problems identified during the reporting period and provide a status (e.g., in progress) regarding new and resolved issues. The Status meeting is an excellent place to air issues and have the team resolve them in a collaborative manner. In addition, a detailed issues report will provide details regarding all logged issues and will accompany the status report.

Issues that the MPATH Provider Services project management team cannot resolve will be escalated to the next level of management within the project organizational structure. MAXIMUS will work with the State to define this channel if the situation arises where the project team cannot resolve the issue. We will

continue to track these management issues in our issues log, and will show that we been escalated the issue for resolution.

3.10.2.1.8Deliverable Development and Approval Process

MAXIMUS understands that on-time and on-budget delivery of the Provider Services Solution will be based on the quality of the deliverables we submit. Submitting deliverables according to the project schedule is meaningless if the product delivered does not meet necessary standards for usability and compliance. We take quality very seriously and have constructed a deliverable production process to support the quality of our deliverables. As state above, we utilize a Compliance Manager to support the quality reviews and verify compliance with contract requirements.

We plan to submit all deliverables to DPHHS according to the project schedule. Depending on the size and complexity of the deliverables, we will include additional time for detailed walkthroughs and, when agreed to, a revision period so that we can incorporate updates from the walkthrough into the deliverable before it is submitted. In our past implementations, we have also broken large deliverables into logical smaller components that we submit as they are completed. For example, in our District of Columbia implementation, we broke the detailed system design into functional components that we submitted and reviewed with the customer. A final sign off was still required for the entire deliverable, but the smaller components being delivered in several submissions over time helped the review process and removed a major time constraint for the review of that deliverable.

We will work with DPHHS to review each deliverable and during the creation of the Deliverable Expectations Document (DED), we will identify the timeframes and review type for each deliverable. We will then update the project schedule to align with the deliverable development and review approach taking special care that we do not ultimately exceed the total time for the deliverable.

For planning purposes, the project schedule allows ten days for initial DPHHS review, five days for MAXIMUS revisions based on comments, and an additional three days for final approval of deliverables. MAXIMUS believes that our quality and compliance processes will enable us to gain approval after we have resolved questions from the first review so that no more than two (2) submissions will be required for any deliverable. MAXIMUS has a repository of project deliverable templates and actual deliverables from past projects we believe will give us an advantage on the Montana project.

Exhibit 3.10.2.1-11: MAXIMUS Deliverable Development and Approval process shows our approach to the creation, review, and approval of all deliverables. We will align our review and submission procedures with DPHHS requirements upon contract award. Short duration projects with numerous deliverables make it critical to put a formal deliverable review process in place. This will enable deliverables to be submitted as complete and fully compliant documents, that quality is a priority of the deliverable process, and deliverable review and approval is a fast and efficient process.

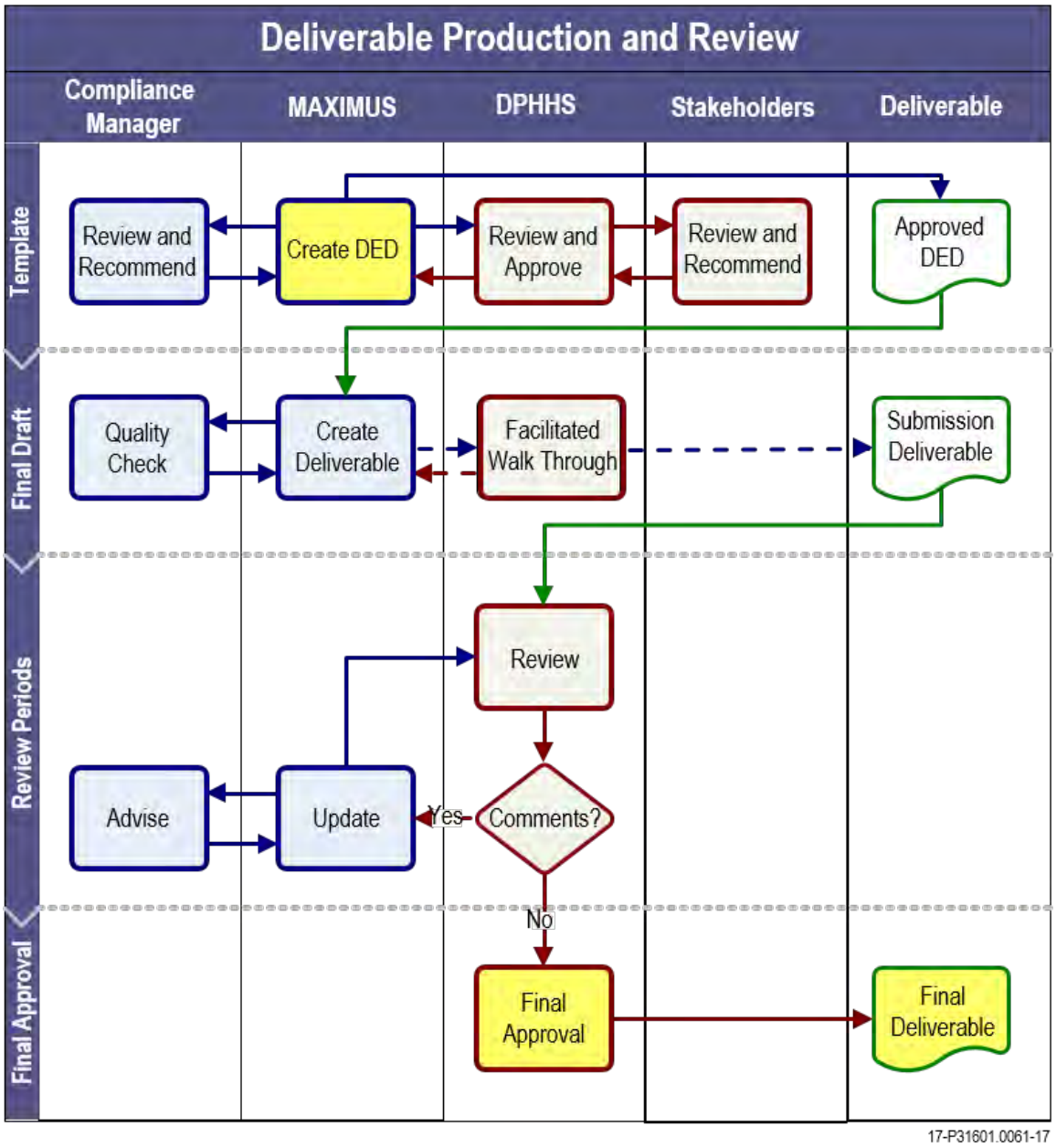


Exhibit 3.10.2.1-11: MAXIMUS Deliverable Development and Approval. *MAXIMUS follows a detailed process for developing and delivering required deliverables.*

The deliverable review process we typically follow includes:

- **Create Deliverable Expectation Document (DED)** – MAXIMUS will create a document that defines the approach, content, and approval criteria for each deliverable including an annotated table of contents.
- **Walkthrough and Approve DED** – MAXIMUS will walkthrough each DED with DPHHS to gain approval on the approach and expectations for each deliverable. We will identify and update the DED with comments from the walkthrough.

- **Deliverable Creation** – The assigned team members create the document according to the contractual scope of work.
- **Internal Reviews** – Appropriate team members are assigned to conduct a comprehensive review of the draft of a deliverable (or appropriate sections) for completeness and accuracy. Comments and changes will be incorporated into the deliverable draft by the author(s). The Compliance Manager reviews the deliverable with the team using the approved DED as a guide and verifies quality and adherence to the DED.
- **Final Updates** – Comments from the internal review are incorporated into the final deliverable.
- **Deliverable Submission** – The MAXIMUS Project Manager submits the deliverable to the Department for review and comment.
- **Deliverable Walkthrough** – Based on the requirements of the DED, the deliverable may need a walkthrough with specified DPHHS or partner vendor staff.
- **Department Review/Comments** – Upon receipt of a deliverable, the Department will log the deliverable and convene a panel to review the deliverable to determine their readiness for use and compliance with content requirements. If the material or document is determined to be non-compliant, the Department will send written notification to the MAXIMUS Program Manager outlining the reason(s) for the determination.
- **Department Comment Resolution** – The MAXIMUS team reviews comments provided by the Department and updates the deliverable appropriately documenting a specific response to each issue identified.
- **MAXIMUS Resolution Review** – The MAXIMUS Project Manager and the Compliance Manager review the resolved comments for accuracy and completeness and submits the deliverable to the Department for final approval.
- **Department Final Approval** – The Department verifies their comments were adequately addressed and approves the deliverable in writing.

The strict deliverable service level agreement coupled with the time constraints of the project necessitate that deliverables are developed correctly the first time and the review can be complete to meet the project schedule. For this to occur, MAXIMUS will use our Compliance Manager and a series of review steps to validate quality and content of each deliverable. For DPHHS, it is critical that during review all comments and concerns are captured during the initial review. Subsequent reviews will only check that MAXIMUS adequately handled the initial review points and new items will not be allowed. This approach keeps the teams focused on what is needed for a specific deliverable, aligns with the timeframes included in the project schedule, and closes the loop on the service level agreement that we are required to meet related to no more than two submissions of any deliverable.

3.10.2.1.9Project Oversight

MAXIMUS is frequently called upon to provide IV&V services and therefore, we fully appreciate both the importance of this role and criticality of IV&V and State's PMO having accurate and timely data as a basis to assess the health of the project and make recommendations to DPHHS. MAXIMUS has the capability to extract project schedule, development, testing and defect remediation statistics, performance data and other project related data into formats that allow independent analysis and assessment. This

information facilitates confidence in the progress reporting so all parties have accurate and verified information to support critical decisions such as readiness for implementation.

3.10.2.1.10 Project Documentation Repository

MAXIMUS will establish an internal Microsoft SharePoint repository to house all MPATH documentation to include deliverables, action items, issues, risks and decision registers, meeting minutes, presentations, design documents, and other project artifacts. The MAXIMUS repository will consist of subfolders for each project phase for project team members to locate easily and update the most current version of each document. SharePoint provides document versioning, backup, and recovery in the event a document becomes corrupted or accidentally overwritten.

Based on the State's direction, MAXIMUS will transfer all completed project documentation from the MAXIMUS internal SharePoint repository to the States and/or the Systems Integration Services collaboration site. This includes all project deliverables, status reports, technical and non-technical project artifacts, requirements matrix, business design documentation (process models, use cases, user stories, storyboards, detailed design documents, supplemental specifications, test cases, test scripts, test results, and user, system and training documentation. MAXIMUS recommends that DPHHS create a folder structure that mirrors the MAXIMUS repository in the collaboration site to facilitate management and retrieval of the documentation. The collaboration site will be the official source of record for all final versions of project documentation.

3.10.2.1.11 Project Initiation Kick-Off

MAXIMUS has managed the start-up of thousands of projects nationwide including three modular Provider management systems that were successfully implemented and are in production today. This knowledge translates to a MAXIMUS-led startup that reflects a proven organization and provides confidence that the planning and execution of the implementation tasks were completed with the highest degree of quality and according to schedule.

Upon contract award, MAXIMUS schedules a kick-off meeting with the State to review our project approach, gain commitment to a common objective, and gauge expectations of various stakeholder participants. We find the kick-off meeting to be essential in developing a common understanding of the methodology, schedule, and responsibilities of all parties. We use this opportunity to answer participant's questions, and discover and address any concerns, rumors, or confusion that project stakeholders have before proceeding with scheduled project activities. MAXIMUS provides an agenda to the State prior to the meeting to confirm that we address all meeting objectives. At this meeting, MAXIMUS will:

- Introduce project management staff to the State project staff and provide the State with an organizational chart
- Review and explain the project schedule
- Create a project contact list
- Confirm the schedule for project governance activities such as the format for status reports, the schedule for status meetings, and the deliverable review process
- Explain how the Requirements Traceability Matrix (RTM) provided in this proposal is maintained throughout the project

- Describe the processes to be used to validate the contract requirements with State staff
- Demonstrate how to access the project document repository
- Provider a demonstration of the MAXIMUS Provider Services base solution
- Review the Requirements Validation meeting schedule

We will also schedule a series of follow up meetings to review all project management artifacts and early deliverables so that the project begins in an efficient manner with all parties understanding the detailed schedule and activities that must occur to successfully complete Project Initiation. During the kick-off meeting, we provide a demonstration of the Provider Services base system. This demonstration is an important part of the agenda as it allows the State stakeholders and subject matter experts to visualize the system's ability to meet the functional requirements from the RFP. We transition from this demonstration in the kick-off meeting to then conducting the Requirements Validation gap analysis sessions that formally launches the DDI effort of the Provider Services implementation. In the sections that follow, we expand on our approach for completing all phases of the Provider Services module DDI, from Requirements Validation through Certification.

3.10.2.1.12 Project Management Requirements

The following table includes Attachment F Project Management Requirements, our summarized response to each requirement, and the section(s) in our proposal in which we provide our detailed response.

ID	Project Management Requirement	MAXIMUS Summarized Response
PMT01	The Contractor shall provide licenses as required by the Agency to allow users access to perform all necessary business functions.	MAXIMUS product licensing for our Solution includes access for all users that are authorized by the Agency to complete necessary business functions.
PMT02	The Contractor shall support the Department in all program governance activities as necessary.	MAXIMUS will provide the information necessary to support the Department in conducting all provider management governance activities.
PMT03	The Contractor shall be responsible for the capture and dissemination to the Department of agendas, meeting minutes and documentation necessary for successful execution of the project.	MAXIMUS provides agendas, meeting minutes, and any other documentation that is required to successfully execute the MPATH project. Refer to *Section 3.10.2.1.2–Project Status Reports and Meeting Procedures*.
PMT04	The Contractor shall participate in necessary meetings with the stakeholders and/or other Contractors.	MAXIMUS participates in all necessary meetings with the appropriate stakeholders and Contractors. Refer to *Section 3.10.2.1.2–Project Status Reports and Meeting Procedures.*
PMT05	The Contractor shall provide deliverables or documentation as defined in the Project Work Plan (PWP) and approved by the Department.	MAXIMUS provides all deliverables and documentation in accordance with the timelines defined in the State approved project work plan. Refer to *Section 3.10.2.1.8–Deliverable Development and Approval Process and Section 3.10.7–Project Deliverables and Documentation.*
PMT08	The Contractor shall support the State and its Contractor(s) in Independent Verification and Validation (IV&V) activities associated with the contract including CMS Certification(s).	MAXIMUS supports the State and its contractors with any IV&V activities associated with CMS Certification. This includes providing documentation, preparing Certification packages and attending meetings with CMS. MAXIMUS understands the importance that the IV&V contractor will bring to the project. We are confident that our proven project management and software development methodologies, combined with quality control procedures we have in place for our deliverables, will result in little or no concerns raised by the IV&V vendor during the MPATH project. We will work closely with the IV&V vendor to ensure they are educated on all aspects of our approach and ensure they get adequate status information throughout the project. Refer to *Section 3.10.2.1.9–Project Oversight.*
PMT09	The Contractor shall conduct a monthly status meeting to discuss project tasks and activities (e.g., deliverables, milestones, issues, risks, and SLAs).	MAXIMUS conducts a monthly status meeting with the Department to discuss project status, tasks, and activities. Refer to *Section 3.10.2.1.2–Project Status Reports and Meeting Procedures.*

ID	Project Management Requirement	MAXIMUS Summarized Response
PMT10	The Contractor shall conduct weekly meetings to discuss issues, risks, progress of current projects, solution changes, resource changes, and other areas specific to the scope of work.	MAXIMUS conducts a weekly status meeting to discuss the intricacies of the MPATH project. This meeting includes discussion of issues, progress, risks, solution changes, resource changes, and other areas specific to the scope of work. Refer to *Section 3.10.2.1.2–Project Status Reports and Meeting Procedures*.
PMT11	The Contractor must employ a project management approach that will satisfy the scope of work and incorporate all activities described in the RFP. The Contractor shall adjust the project management approach or project schedules, as necessary, to collaborate with the module vendors in order to incrementally build the enterprise platform.	MAXIMUS utilizes a project management approach that meets all the requirements defined in the RFP. Our project management approach is flexible enough to allow for adjustments to work with multiple vendors in an enterprise solution. Refer to *Section 3.10.2.1–Project Management*.
PMT12	The Contractor shall conduct a project initiation kick-off meeting with key stakeholders and the State's project team.	MAXIMUS conducts a project initiation kick-off meeting with all key stakeholders and the State's project team to ensure everyone understands how the project shall be executed from kick-off to implementation. Refer to *Section 3.10.2.1.11, Project Initiation Kick-Off.*
PMT13	The Contractor shall implement procedures and tools for tracking project action items, decisions, issues, risks and defects.	MAXIMUS implements processes and procedures for tracking action items, decisions, issues, risks, and defects. Refer to *Section 3.10.2.1.2–Project Status Reports and Meeting Procedures* and *Section 3.10.2.1.10–Project Documentation Repository.*
PMT14	The Contractor shall provide an electronic document repository for project documents and deliverables. The Contractor, Department staff and other contractors with the appropriate security level must have the ability to upload/attach new or revised versions of documents. The repository must perform version control and allow users to view all prior versions.	MAXIMUS provides SharePoint as an electronic document repository for project documents and deliverables. MAXIMUS provides access to appropriate users while employing appropriate security levels for each user. SharePoint is a robust tool that allows for versioning of documents. Refer to *Section 3.10.2.1.10–Project Documentation Repository.*
PMT15	The Contractor shall establish and utilize a deliverable review and acceptance process agreed upon by the Department that incorporates the following: a. Review cycles, which will be conducted and scaled to the size and complexity of the deliverables. b. Deliverables will need to reflect coordination with the overall modular program and will follow agreed upon change control processes. c. Informal reviews and walkthroughs of draft and final deliverables are encouraged. d. Queuing up excessive deliverables for simultaneous review is unacceptable to the Department.	MAXIMUS establishes a deliverable review process according to the requirements in the RFP. MAXIMUS delivers documents as they are completed to prevent submission of an excessive number of documents to the Department for simultaneous review. Each review cycle may differ in length depending on the complexity of the document and whether a walkthrough has been completed. Refer to *Section 3.10.2.1.8–Deliverable Development and Approval Process and Section 3.10.7–Project Deliverables and Documentation.*
PMT16	The Contractor shall provide deliverables that at a minimum meet the following quality standards: a. Provide accurate and comprehensive content, reflecting the specific requirements for the deliverable. b. Ensure appropriate technical level for the audience. c. Utilize correct grammar, spelling, and versioning. d. Ensure diagrams are clear, concise, and value added. e. Follow industry-related standards. f. Appropriately define and reference information.	MAXIMUS ensures that deliverables: a. reflect the specific deliverable requirements, b. are of the appropriate technical level for the audience, c. use correct grammar, spelling, and versioning d. contain clear, concise and value added diagrams, e. follow industry standards f. define and reference information We have proposed a Compliance Manager who will be committed to making sure that project deliverables are produced and conform to quality requirements and SLAs for the project. Refer to *Section 3.10.2.1.8–Deliverable Development and Approval Process and Section 3.10.7–Project Deliverables and Documentation.*

ID	Project Management Requirement	MAXIMUS Summarized Response
PMT17	The Contractor shall submit a monthly status report. The monthly status report must contain, at a minimum: a. A complete set of updated and current output from the Project Work Plan along with a copy of the corresponding Project schedule files in electronic version. b. A description of the overall completion status of the Project including schedule variations that report the earned value of the work completed, the planned value of the work completed, and the variance. c. Planned tasks and activities for the next month. d. The Deliverable status, with percentage of completion and time ahead or behind schedule for particular tasks. e. Identification of any staffing issues or changes in the Resource Allocation Matrix. f. An updated status on all issues being monitored. g. An updated status on all risks being monitored. h. Provide metrics necessary to support the State CIO's Legislative Finance Committee (LFC) reporting requirements. i. Provide testing status and metrics. j. Provide System enhancement hourly pool total hours used and total hours remaining. k. An updated status on all SLA being monitored.	MAXIMUS submits a monthly status report that contains, at a minimum: a. updated project work plan including a full electronic project schedule b. overall completion project status c. planned tasks and activities for the next month d. a listing of deliverables and their current completion status e. staffing issues or changes f. updated status on issues being monitored g. updated status on risks being monitored h. metrics that support the State CIO's Legislative Finance Committee reporting requirements i. testing status j. status of enhancement pool hours k. status on SLAs being monitored Refer to *Section 3.10.2.1.2–Project Status Reports and Meeting Procedures*.
PMT18	The Contractor shall develop and maintain a Project Management Plan (PMP): The purpose of the Project Management Plan is to provide a comprehensive baseline of what needs to be achieved by the project, how it is to be achieved, who will be involved, how it will be reported and measured and how information will be communicated with the project. It will serve as a reference for decision and clarifications. All relevant project plans including but not limited to the Communication Plan, Change Management Plan, Staffing Management Plan, Quality Management Plan, Risk Management Plan, Issue Management Plan and the Work Breakdown Structure are incorporated into the Project Management Plan. It is a living document that evolves as the project progresses and is updated with the latest relevant information as required. The Project Management Plan may be broken into separate documents, but all documents will be considered sections of the Project Management Plan.	MAXIMUS develops and maintains a Project Management Plan (PMP). All relevant project plans will be included in the PMP. This document will be a living document that evolves as the project progresses. Refer to *Section 3.10.2.1–Project Management, Section 3.10.2.1.1–Communication Plan, 3.10.2.1.4–Staffing Management Plan, Section 3.10.2.1.5–Quality Management Plan, Section 3.10.2.1.6–Risk Management Plan, Section 3.10.2.1.3–Change Management and WBS, Section 3.10.2.1.7–Issue Management Plan,* and *Section 3.10.2.18–Deliverable Development and Approval Process.*
PMT19	The Contractor shall develop and maintain a detailed Project Work Plan (PWP) and a Gantt Chart that is aligned with the scope of the work outlined in this RFP. The PWP must identify realistic person hours of effort for each task and identify planned completion dates for all deliverables and milestones. Additionally the PWP must include the elements necessary for the IMS include: start and end dates of major phases, key project milestones, integration points, cross module dependencies, and sufficient information to support the State CIO's Legislative Finance Committee (LFC) reporting requirements. The PWP must be continually refined and updated as the project progresses and will retain the baseline for comparative reporting.	MAXIMUS develops and maintains a project work plan (PWP) and a Gantt chart that aligns with the scope of work. The PWP is built with realistic person hours with start and completion dates for all deliverables and milestones. The information in the PWP also contains sufficient information to support the State CIO's LFC reporting requirements. The PWP is continually updated as the project progresses, but a baseline is maintained for comparative purposes. Refer to *Section 3.10.2.1.8–Deliverable Development and Approval Process, Section 3.10.2.1.2—Project Status Reports and Meeting Procedures, and Section 3.10.2.1.3-Change Management and WBS.*

ID	Project Management Requirement	MAXIMUS Summarized Response
PMT21	The Contractor shall coordinate with the Department and with the module vendors as required by the Department, to support the program-level change management process consistent with the Enterprise Change Management Plan.	The change management process is defined in the Project Management Plan deliverable and describes in detail how program-level changes will support, and be consistent with, the change management process in the Enterprise Change Management Plan. Refer to *Section 3.10.2.1.3-Change Management and WBS* for further details.
PMT25	The Contractor shall be required to work collaboratively with the Department and the System Integrator to provide schedule information to be included in the Integrated Master Schedule (IMS). Elements necessary for the IMS include; start and end dates of major phases, key project milestones, integration points, cross module dependencies, and sufficient information to support the State CIO's Legislative Finance Committee (LFC) reporting requirements.	MAXIMUS works collaboratively with the Department and the System Integrator to update the Integrated Master Schedule with the relevant information. Refer to *Section 3.10.2.1.3–Change Management and WBS* and *Section 3.10.2.1.2–Project Status Reports and Meeting Procedures.*
PMT27	The Contractor shall coordinate module deliverable and milestone walkthroughs and participate in other module walkthroughs as required by the Department.	MAXIMUS coordinates deliverable and milestone walkthroughs and participates in other module walkthroughs as required by the Department. Refer to *Section 3.10.2.1.8–Deliverable Development and Approval Process and Section 3.10.7–Project Deliverables and Documentation.*
PMT29	The Contractor shall submit a monthly System Enhancement Pool report that details tickets invoiced to the hourly pool and must include hours used and hours remaining for the Department's approval.	MAXIMUS submits a monthly system enhancement pool report that identifies the tickets invoiced and the hours used and hours remaining. Refer to *Section 3.10.2.1.2–Project Status Reports and Meeting Procedures*.
PMT31	The Contractor shall cooperate with the State's PMO and the IV&V contractor to give an accurate, honest reporting of the project status.	One of the most important project management principles we bring to the MPATH project is an emphasis on communication and collaboration with the Department and other key stakeholders. We strive to keep easy, open channels of communication between our projects and clients. MAXIMUS will fully cooperate with the State's PMO and IV&V contractor to give an accurate and honest status of the project. Refer to *Section 3.10.2.1.9–Project Oversight*.
PMT32	The Contractor shall contribute to the State's and/or the Systems Integration Services collaboration site, technical and non-technical project artifacts for the Contractor's module or module components including requirements, use cases, user stories, storyboards, system design documents, supplemental specifications, test cases, test scripts, test results, user, system and training documentation at the State's direction.	Based on the State's direction, MAXIMUS contributes to the State's and/or the Systems Integration Services collaboration site. This may include any of the project's technical and non-technical artifacts. Refer to *Section 3.10.2.1.10–Project Documentation Repository*.

3.10.2.2 System Development Methodology

> 3.10.2.2 System Development Methodology
>
> The Contractor will be expected to follow an industry-standard systems development methodology for the initial implementation of the proposed solution and throughout the Contract term. The Offeror must propose a System Development Methodology approach that achieves the expected outcomes of the SDLC-based activities stated below.

All aspects of systems and software development, particularly designing, testing, and configuration, are governed by our System Development Methodology (SDM). Our approach confirms that the State's defined deliverables, tracking, and monitoring functions are in line with those requested by the RFP. In this section of our proposal, we provide an overview of our SDM, and describe how it is used to support the successful delivery of the MPATH Provider Services module.

While all aspects of the MPATH project are important, the tasks and activities related to modifying and configuring the software for use in the State of Montana are necessary for the overall success of the project. The requirements — system design, configuration, testing, and implementation — are a set of

complex tasks with a number of activities occurring simultaneously. It is important that a solid plan for execution be put in place before the project team begins work. MAXIMUS is proposing a realistic and carefully crafted schedule with configurations and enhancements that are clearly defined, approved, and fully tested, and that all RFP requirements are satisfied. *Exhibit 3.10.2.2-1 Project Phases* shows the sequential steps from Requirements Validation through Implementation that will result in the completion of the MAXIMUS Provider Services solution.

Exhibit 3.10.2.2-1: Project Phases. *MAXIMUS SDM follows a clearly defined SDLC that results in confirmation of quality and completeness through every step of the project.*

Our approach focuses on the tasks necessary for MAXIMUS to configure or enhance our base system to deliver all anticipated functionality and to support the defined requirements for the system. We focus the bulk of our design and implementation effort on addressing the requirements gaps between our proven system and the contract requirements. We have found that approach works well when the base system meets the majority of the business requirements and the focus is on identifying configuration updates to align with a state's specific business processes and required workflows. We utilized this approach in Tennessee, Nebraska, and the District of Columbia. This means we can spend more time to design and make system changes to meet the unique requirements of Montana providers and DPHHS and focus on items such as the MMIS interface that require customization for Montana. Our approach enables the business staff to quickly see the results of the gap analysis and requirements activities and to work closely with State business staff to understand how the gaps should best be filled.

3.10.2.2.1 Integrated Planning Effort

Best Practice

MAXIMUS utilizes a process-based approach for undertaking projects. We build a comprehensive, integrated Project Work Plan that includes all work required by all parties to successfully implement the Provider Services module. We work closely with DPHHS, the legacy MMIS vendor, the system integrator vendor, and other module contractors to craft an integrated project schedule that fully identifies tasks, estimated timelines, responsibilities and interdependencies of every organization. Creation of this integrated plan helps each partner understand the tasks and schedule that has to be met for the project.

Placing emphasis on the execution of an integrated plan for the entire solution allows MAXIMUS to implement the full solution into production within our proposed twelve-month timeframe. This timeline and schedule gives the State sufficient time to communicate needs to Stakeholders, complete operational readiness reviews and translates into a successful implementation.

The MAXIMUS plan includes configuration and implementation of our hosting solution. Our approach unifies hardware, software, and communications protocols through web services to deliver information to our staff members, State workers, and Providers at their desks. Integrating these different components requires leading edge tools and technical support to provide seamless views of program and customer data. We use the combination of User Acceptance Testing and Operational Readiness testing, which will begin approximately eight weeks before go-live, as the mechanisms to provide a final review and

approval of the overall MPATH solution. We also begin system testing early and invite the State to participate in data conversion test reviews, data integration testing and in parallel testing if desired. The intent is to provide adequate time for the State to understand the impacts of a modular implementation on the operating teams and to feel comfortable that all of the required functionality has been implemented correctly.

3.10.2.2.2 Incremental Design, Development and Testing

MAXIMUS closely adheres to the PMI Project Management Body of Knowledge (PMBOK®) Guide and Standards in our application software delivery methodology, project schedule, and associated project deliverables. This methodology is a formalized approach to project execution that is governed by a proven set of written procedures that serve as the guide for all project staff activities.

We utilize Agile Scrum based daily standup meetings, team oriented design, development, testing, and user experience confirmation. However, we do not adhere to the sprint based deployment approach. We have found that four-week sprints are difficult on large complex software development projects due to the degree of complexity and integration required to adequately test and verify each sprint. Rather we use an incremental approach based on logical work units that progressively adds functionality in a logical sequence. An incremental approach results in business oriented, sequential delivery of fully integrated and complete user facing functionality that can be shown to end users early so that course corrections can be made with minimal impact to the overall schedule.

We also incrementally create the Waterfall based design documentation that our State customers require for confirmation of requirements and approval of major project milestones. Incremental delivery of design and other deliverable documentation prevents the customer from having to wade through thousands of pages of information to try to determine compliance with contract requirements. In addition, major groups of functions can be approved allowing the configuration team to begin work while other aspects of the solution are being designed. We have found that when one large design document is submitted, the time the review team needs to thoroughly review frequently exceeds the time allotted in the project schedule and also frequently results in key requirements and design decisions being missed. Contract deliverables are compiled at timelines mandated in the contract to satisfy State requirements for invoice and payment approval.

For the MPATH Provider Services project, we propose six incremental deliveries of the MPATH application components. Four tracks are specific to the base functionality while the other two enable MAXIMUS to integrate Option A and Option B functions into the overall system implementation plan. Provider Management Services systems are unique in that both the functionality and the workload to implement them can be divided into logical and discrete business functions that are also very similar in size and complexity. Incremental development has many advantages. It breaks the system up into manageable pieces, allows testing to occur sooner, and provides users with early opportunity to view and work with the application. Early user involvement identifies design discrepancies and allows for correction without impact to the project end date. *Exhibit 3.10.2.2-2: Incremental Delivery* provides a graphical depiction of the incremental design, development, and testing efforts. Each increment culminates with a user experience checkpoint that confirms that the user's expectations during design have been achieved. If there are discrepancies in expectations, the methodology allows for revisions to each increment prior to and during integration testing.

CONFIDENTIAL

We have designed our implementation plan around the requirements for the base Provider Services module. However, we have also carefully planned how we would integrate the system changes required for Option A and B. Our approach is to use the functions within a completed track to build upon for the additional functions required for Options A and B. As can be seen, we begin designing the enhancements necessary for the additional provider self-service functions included in Option A after we have completed the provider facing components of the base. Similarly, we begin design work to integrate the CRM functions for Option B after we have configured the enrollment and screening requirements. Aligning the work in this fashion enables us to maximize the policy and business staff support already present for the base solution as well as extending the testing infrastructure and staff to complete a full system review.

Experience

Our plan is designed to allow a state to choose the base system only, either option or both options with the same overall schedule.

As shown in *Exhibit 3.10.2.2-2*, we begin work on the MMIS Interfaces and Conversion very early in the project. In our experience, there is a significant amount of work and coordination required with DPHHS, the MMIS Vendor, and the System Integrator to design, implement, and test these components of the Provider Services solution. As a result, our methodology separates Interfaces and Conversion analysis,

CONFIDENTIAL

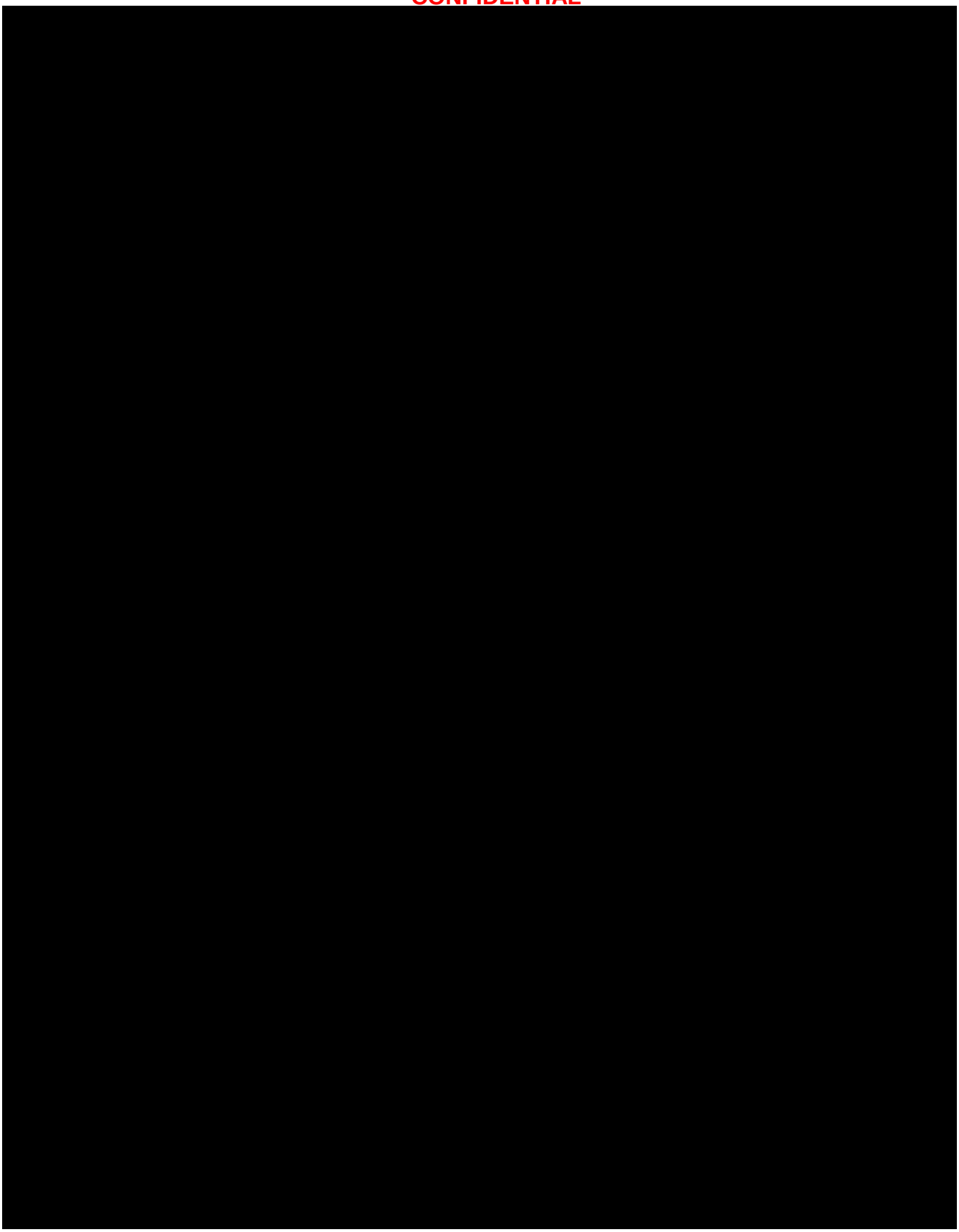
CONFIDENTIAL

design, development, and testing into separate threads that ultimately are completed in synch with the user interface application components. We also start System testing after the main components of the online solution are finished so we can integrate converted data and interface data early in the system testing process to maximize the number of test cycles that can be run for each. This approach leads to a complete solution that is functionally ready for Integration, System, and User Acceptance Testing while still allowing important ancillary functions such as correspondence management and reporting to be included in the overall processes as they are complete.

Each Track shown in *Exhibit 3.10.2.2-2* above consists of design, configuration/build, testing, and user experience confirmation tasks. Based on our experience, we separate the DDI into these Tracks to make sure that once full System Testing begins, we have placed proper focus on the key functionality of the system well in advance of conducting the full system test. *Exhibit 3.10.2.2-3: Development Tracks* provides a description of each of our Development Tracks and provides the reasoning behind the sequencing of each Track.

CONFIDENTIAL

CONFIDENTIAL



CONFIDENTIAL

During Project Initiation, MAXIMUS schedules and conducts a Project Kick-Off meeting with key MPATH stakeholders and the State's project team. The kick-off meeting consists of several agenda items, including a review of the six proposed development tracks described in *Exhibit 3.10.2.2-3*. During the kick-off meeting, we also provide a brief demonstration of the Provider Services base system. This demonstration is an important part of the agenda as it allows the State stakeholders and subject matter experts to visualize the system's ability to meet the functional requirements from the RFP and how they align with the development tracks. We transition from this demonstration in the kick-off meeting to then conducting the Requirements Validation gap analysis sessions that formally launches the DDI effort of the Provider Services implementation. In the sections that follow, we expand on our approach for completing all phases of the Provider Services module DDI, from Requirements Validation through Certification.

3.10.2.3 Requirements Management

> 3.10.2.3 Requirements Management
>
> The Contractor must work with the DPHHS MPATH Team to confirm the Contractor's understanding of the RFP requirements and to reconcile the RFP requirements for the scope of work against the proposed solution. The Offeror must describe their approach to meet each of the detailed Requirements Management requirements defined in Attachment F, Requirements Matrix.

MAXIMUS understands the importance of confirming the system and business requirements before moving onto design and development. Changes to the MAXIMUS Provider Services base system based on RFP requirements represent new or changed functionality that affects the State as well as the Provider community. It is critical that the project team has an accurate understanding of these requirements. Discussions and agreements form the basis for the final set of system and business requirements that lead the design and development efforts. *Exhibit 3.10.2.3-1: Requirements Validation* shows the key tasks completed during the Requirements Validation phase of the MPATH project.

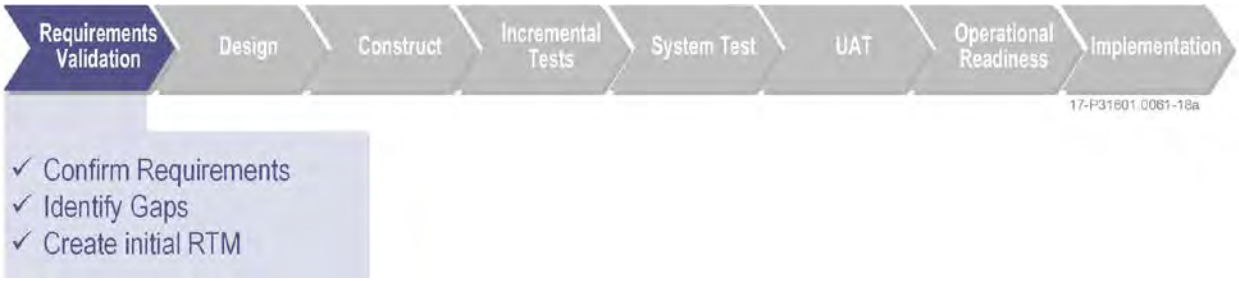


Exhibit 3.10.2.3-1: Requirements Validation. *During Requirements Validation, MAXIMUS conducts review sessions with the Department to validate and confirm the intent of all requirements in the RFP.*

Compliance

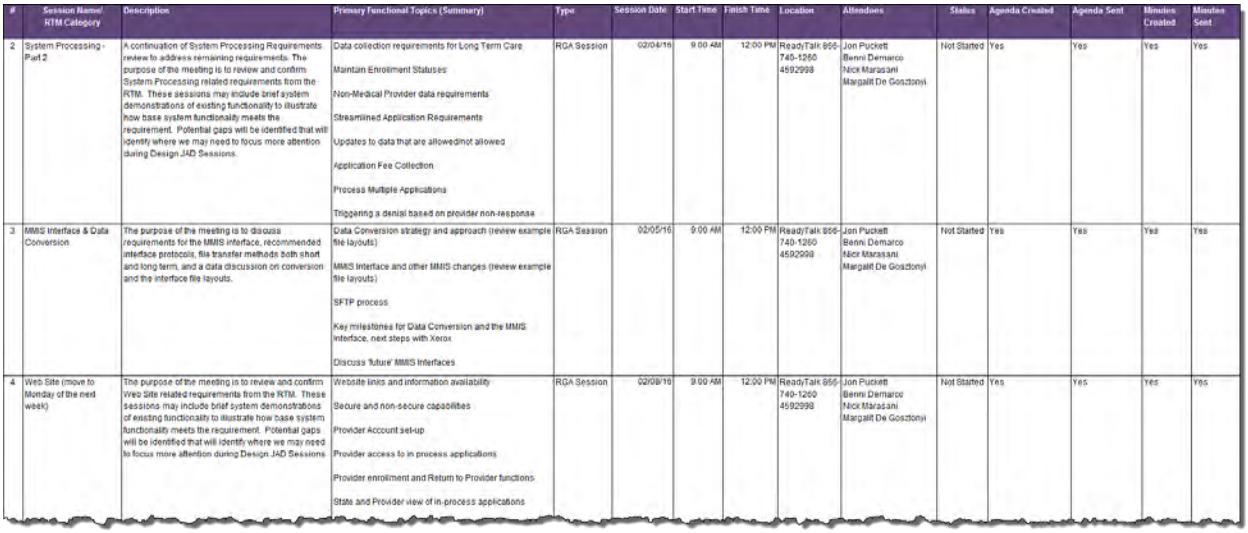
Our solution already meets a large percentage of the functionality requested for the Provider Services solution, given its compliance with CMS and ACA-requirements. We may also address additional requirements, but we cannot confirm that until we meet with DPHHS to demonstrate the capabilities existing within our base Provider Services solution. We can accomplish many of the remaining requirements through configuration updates rather than software coding changes. We anticipate the majority of coding changes will involve implementation of the MMIS interface and possibly due to the implementation of additional verification sources that are not available in our other implementations.

Our highly configurable solution allows us to perform efficient maintenance, and allows our support staff to focus attention primarily on system enhancements and improvements, as requested by DPHHS. Conducting the Requirements Gap Analysis (RGA) sessions are a core component of the MAXIMUS SDM. MAXIMUS uses the RGA approach to validate project requirements against existing application components to quickly and easily determine functionality gaps. Our RGA approach relies on facilitated work sessions where our Business Analysts present the functionality of the base system and describe how we meet each requirement as presented in our proposal. DPHHS subject matter experts communicate whether they believe the system meets the RFP requirements or if modifications may be necessary.

All RFP requirements are initially loaded into Jama's Contour requirements management tool. For a description of this tool, please visit the "Jama Contour / What is Jama?" web page at the following link: https://www.jamasoftware.com/platform/. When we capture additional details about each requirement as subordinate requirements, requirements decomposition occurs. We map these subordinate, detailed requirements to application components to provide traceability. We have found RGA enables a collaborative approach that allows the project teams to make decisions and resolve functionality gaps in a quick and cooperative manner. This approach also allows the state user community to see the Provider Services system functionality firsthand and early in the project so they become familiar with the system and understand how it functions. The feedback enables MAXIMUS to confirm the number of changes and validate the System Design and Configuration planning efforts. We use this knowledge for all subsequent phases and as the basis for a detailed understanding of our system and operational solution.

The RGA addresses security requirements and defining user roles. We will focus at least one RGA session on a review of existing Provider Services base system user roles and accounts and defining the different user roles and associated system access authority levels. During the system level security requirements discussion, MAXIMUS shares our approach for security vulnerability scans and data encryption to protect the application and data from unauthorized access.

Requirements Validation begins with a series of joint gap analysis sessions that include participation by state business and technical staff and the MAXIMUS project team. We organize these sessions around specific system functions required to administer the program. In preparation for the RGA sessions, MAXIMUS analyzes the Appendix F requirements and prepares a complete session schedule that we submit to the Department. *Exhibit 3.10.2.3-2: Requirements Validation Session Schedule* shows an excerpt from the RGA sessions we scheduled during our District of Columbia project.



#	Session Name/ RTM Category	Description	Primary Functional Topics (Summary)	Type	Session Date	Start Time	Finish Time	Location	Attendees	Status	Agenda Created	Agenda Sent	Minutes Created	Minutes Sent
2	System Processing - Part 2	A continuation of System Processing Requirements review to address remaining requirements. The purpose of the meeting is to review and confirm System Processing related requirements from the RTM. These sessions may include brief system demonstrations of existing functionality to illustrate how base system functionality meets the requirement. Potential gaps will be identified that will identify where we may need to focus more attention during Design JAD Sessions.	Data collection requirements for Long Term Care Maintain Enrollment Statuses Non-Medical Provider data requirements Streamlined Application Requirements Updates to data that are allowed/not allowed Application Fee Collection Process Multiple Applications Triggering a denial based on provider non-response	RGA Session	02/04/16	9:00 AM	12:00 PM	ReadyTalk 866-740-1260 4592998	Jon Puckett Benni Demarco Nick Marasani Margalit De Goszdonyi	Not Started	Yes	Yes	Yes	Yes
3	MMIS Interface & Data Conversion	The purpose of the meeting is to discuss requirements for the MMIS interface, recommended interface protocols, file transfer methods both short and long term, and a data discussion on conversion and the interface file layouts.	Data Conversion strategy and approach (review example file layouts) MMIS Interface and other MMIS changes (review example file layouts) SFTP process Key milestones for Data Conversion and the MMIS Interface, next steps with Xerox Discuss 'future' MMIS Interfaces	RGA Session	02/05/16	9:00 AM	12:00 PM	ReadyTalk 866-740-1260 4592998	Jon Puckett Benni Demarco Nick Marasani Margalit De Goszdonyi	Not Started	Yes	Yes	Yes	Yes
4	Web Site (move to Monday of the next week)	The purpose of the meeting is to review and confirm Web Site related requirements from the RTM. These sessions may include brief system demonstrations of existing functionality to illustrate how base system functionality meets the requirement. Potential gaps will be identified that will identify where we may need to focus more attention during Design JAD Sessions.	Website links and information availability Secure and non-secure capabilities Provider Account set-up Provider access to in process applications Provider enrollment and Return to Provider functions State and Provider view of in-process applications	RGA Session	02/08/16	9:00 AM	12:00 PM	ReadyTalk 866-740-1260 4592998	Jon Puckett Benni Demarco Nick Marasani Margalit De Goszdonyi	Not Started	Yes	Yes	Yes	Yes

Exhibit 3.10.2.3-2: Requirements Validation Session Schedule. *MAXIMUS analyzes the RFP requirements, organizes them into functional/technical categories, and prepares a schedule that lists all sessions required for Requirements Validation.*

During each RGA Session, MAXIMUS provides a walkthrough of each system function in conjunction with a demonstration of the system that illustrates the system capabilities. The demonstration allows users to understand how the Provider, Operations, and state users interact with the system. We also review infrastructure, processing, performance, and non-functional requirements to confirm each we have met each requirement. *Exhibit 3.10.2.3-3: Requirements Review Process* shows our approach to completing Requirements Validation by assessing the MAXIMUS base product against the RFP requirements.

Exhibit 3.10.2.3-3: Requirements Review Process. *MAXIMUS conducts a series of Requirements Gap Analysis sessions with participation from state business and technical staff to confirm system requirements. We use a variety of inputs, staff, standards, and tools to create the deliverables required by the RFP.*

Best Practice

The walkthroughs result in the identification of functionality matches and gaps. MAXIMUS Business Analysts capture high-level descriptions of the modifications necessary by functional and/or technical areas. We identify requirement gaps as such in the requirements management tool, Jama Contour, and we create placeholders for application to record the need for additional application components until the designs for the new components are complete. This is where we map the decomposed requirements to high-level test scenarios or use cases that will

eventually become test scripts. *Exhibit 3.10.2.3-4: RTM Gap Analysis* shows a snippet of the RTM we created on our District of Columbia implementation during the Requirements Validation phase.

PDMS Requirements Validation Phase Requirements Traceability Matrix (RTM)						
Area	Requirement ID	Description	Functional vs. Non-Functional	RGA Session	Gap	RTM Session Notes and Initial Gap Analysis
System Processing	C.5.3.2.5	Edit to prevent duplicate provider enrollment during an add transaction.	Functional	1	No	Requirement validated. The base PDMS solution prevents a duplicate from being added to the system based on the Provider's NPI, Zip Code, Zip Code Extension, and Taxonomy Code. The rule was confirmed to be the same for DC. All DC Providers are required to have an NPI including Waiver Providers and Medicaid in Schools. Providers must submit a full application for each of their practice locations. Providers wanting to practice at the same location but with a different Provider Type are also required to submit a full application. Thus, the NPI/Zip/Taxonomy rule can be applied across all DC Providers. Analysis will need to be done during data conversion to identify if duplicate providers may exist on the MMIS per this rule and a decision reached on how to deal with them.
System Processing	C.5.3.2.6	Identify and report any duplicate provider numbers, license or certification numbers, SSN, or FEIN numbers on the provider master file.	Functional	1	No	Requirement validated. The system will prevent duplicate providers from being entered per the NPI/Zip Code/Taxonomy rule. Requirement clarified during RTM Session: the system will have the capability of producing an ad hoc report for any providers that may have been entered/converted using a duplicate SSN/FEIN, duplicate license number, or duplicate certification number.
System Processing	C.5.3.2.7	Accept and store any and all Medicare Universal Provider Identification Numbers (UPIN) and the National Provider Identifiers (NPI), and any previous Medicaid Provider ID numbers (PID).	Functional	1	Yes	Requirement validated. The system will store Medicare Numbers and NPI numbers for providers. Storing previous Medicaid ID Numbers will not be required on PDMS. The provider will maintain their same Medicaid ID throughout their existence on the PDMS. Only 1 NPI can exist for the Provider using the same Medicaid ID. If the provider is newly enrolling and initially enters an incorrect NPI, they will have the ability to update their NPI prior to their application being approved. Providers that are previouslay approved (have a Medicaid ID from the MMIS) that wish to change their NPI will need to contact the MAXIMUS help desk. Authorized MAXIMUS users will have the ability to update the Provider's NPI and other provider identifiers, based on the provider's request. The gap here is to change the system to allow an authorized MAXIMUS user to directly update key identifiers (including NPI) for the Provider.
System Processing	C.5.3.2.8	Monitor provider enrollment to ensure that each provider/provider type combination only has one provider number.	Functional	1	No	Requirement validated. The system will enforce that a provider can only have 1 provider type. But the provider can have additional specialties and taxonomies for that same provider type.

Exhibit 3.10.2.3-4: RTM Gap Analysis. *The RGA sessions result in updates to the RTM where we identify and document potential gaps that need to be further analyzed during System Design.*

The gap analysis documents are the basis for System Design documents that we ultimately create during the Design Phase. The RTM provides for traceability of all specified system changes and forms the basis for the development of test cases to be used during system, integration, and user acceptance testing. If there is a disagreement about how a system function meets a requirement, we will table it and refer it to project management for agreement. This allows the sessions to move quickly and to avoid getting bogged down in details that must be resolved at the management level. We will document each item that meets this criterion and include a description of the issue.

We use the detailed Provider Services solution RTM as a checklist to confirm that we have met every requirement and each requirement is based on the following key activities:

- MAXIMUS updates the RTM throughout the implementation phases as changes occur
- The RTM contains all MITA items that are pertinent to the development effort
- The RTM contains all MECT checklist items that are pertinent to this project
- MAXIMUS obtains State confirmation and approval on our proposed means of addressing each RTM requirement prior to beginning System Design
- Identification of all system stakeholders and users and their access needs
- Identification of all interfaces to all systems, both internal and external to the State
- Descriptions of the system environments (that is, development, testing, model office, production), their intended use, intended user(s), and which environment(s) the State uses for testing, reviewing MAXIMUS testing, and production

We finalize and submit the RTM to the State for review and approval at the end of the Requirements Validation phase. However, our technical team swiftly transitions into conducting further analysis and

preparing for the System Design phase as/when major functional sections of the RTM are completed. We conduct this analysis in parallel with completing the RTM to be sure we are well prepared to begin the System Design phase.

Requirements Management Requirements

The following table includes Attachment F Requirements Management Requirements and our summarized response to each requirement.

ID	Requirements Management Requirement	MAXIMUS Summarized Response
RQM01	During the requirements validation sessions, the Contractor must demonstrate a fully functioning solution that has been initially configured based on the Contractor's understanding of the requirements described in the RFP and publicly available policy documents, manuals, and fee schedules.	Conducting the Requirements Gap Analysis (RGA) sessions are a core component of the MAXIMUS SDM. MAXIMUS uses the RGA approach to validate project requirements against existing application components to quickly and easily determine functionality gaps. Our RGA approach relies on facilitated work sessions where our Business Analysts present the functionality of the base system and describe how we meet each requirement as presented in our proposal.
RQM02	The Contractor shall work with the Department to confirm the Contractor's understanding of the requirements and to clarify and/or elaborate requirements where necessary to achieve desired business outcomes.	MAXIMUS meets with the Department to confirm the requirements and to clarify any d to achieve desired business outcomes. Refer to the narrative in this section for more details on the full requirements validation process.
RQM03	The Contractor shall document any gaps between the initially configured solution and the business requirements in the requirements management tool. Gaps must show bi-directional traceability with applicable business requirement(s), design, test cases, test results, MECT criteria and certification artifacts.	MAXIMUS documents any gaps between the initially configured solution and the business requirements documented in the requirements management tool. Gaps are shown with bi-directional traceability to requirements, design, test, etc.
RQM04	The Contractor shall, during requirement validation, provide designated Department staff access to a fully functioning environment to become familiar with the solution.	MAXIMUS provides the State with access to a fully functioning system to get familiar with the solution.
RQM05	The Contractor shall utilize project control tools to formally track all requirements and related design, configuration testing, and certification artifacts. The Contractor's requirements management tool shall ensure approved changes to requirements are linked back the approved change request.	MAXIMUS utilizes project control tools to track all requirements, design, configuration, testing, and certification artifacts. MAXIMUS' requirements management tool links approved changes to requirements.
RQM06	The Contractor shall develop, maintain and submit a Requirements Traceability Matrix (RTM) to track detailed requirements and their realization throughout all project phases. This should include how the requirement is realized (e.g., configuration, custom development, base functionality). All revisions must be reviewed and approved by the State.	MAXIMUS uses JAMA Contour to develop and maintain an RTM and requirement changes throughout the project. JAMA Contour allows State staff to inspect and approve all revisions. The process for constructing and finalizing the RTM is described in this section.
RQM07	The Contractor's requirements management tool shall have the ability to manage requirements traceability by module(s), MITA business area, MITA business process and MECT checklists.	JAMA Contour allows us to manage the requirements traceability by module so that items can be reported by MITA business area, MITA business process, and MECT checklists.

3.10.2.4 Design Configuration, and Build

> 3.10.2.4 Design Configuration, and Build
>
> The Contractor shall undertake activities to resolve gaps between the RFP requirements and the proposed solution. Once designs have been approved by DPHHS, the Contractor shall configure and/or customize the solution based on the desired business outcomes. The Offeror must describe their approach to meet each of the Detailed Design, Configuration, and Build requirements defined in Attachment F, Requirements Matrix.

As part of our SDM, MAXIMUS uses a system design and development process that aligns with Agile/SCRUM practices, but is much more focused on completion of functional packages than four-week

sprints. We use an incremental build methodology based upon iterative configuration. By "iterative configuration," we mean that requirements and software evolve through collaboration between State subject matter experts, MAXIMUS Business Analysts, and the development team. We present results of the development effort to the user community as soon as they are complete, rather than at the end of the entire configuration phase. Our configuration approach follows a structured, repeatable development cycle, with each development stream producing independent functional components we promote through configuration and testing as we identify system gaps. *Exhibit 3.10.2.4-1: Incremental Implementation Approach* reflects the approach MAXIMUS will use to design, configure, and implement our Provider Services module for the State.

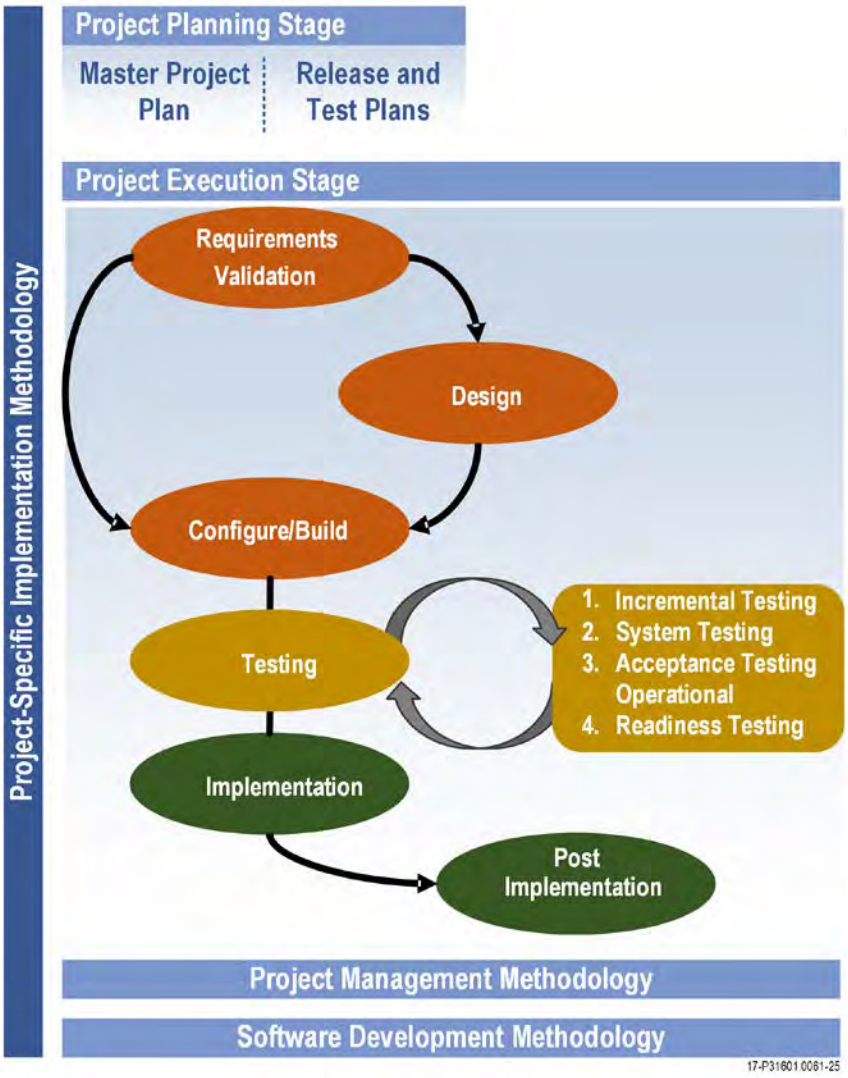


Exhibit 3.10.2.4-1: Incremental Implementation Approach. *Our implementation methodology allows us to complete configuration, testing, and implementation within our proposed project timeframe. MAXIMUS uses an iterative development approach that results in the required documentation creation, but allows expedited configuration activities leading to early testing and confirmation by the Department.*

In this section of our proposal, we describe how we take the results of the Requirements Gap Analysis (RGA) to design, configure, and build the Provider Services module to meet all of the State RFP requirements.

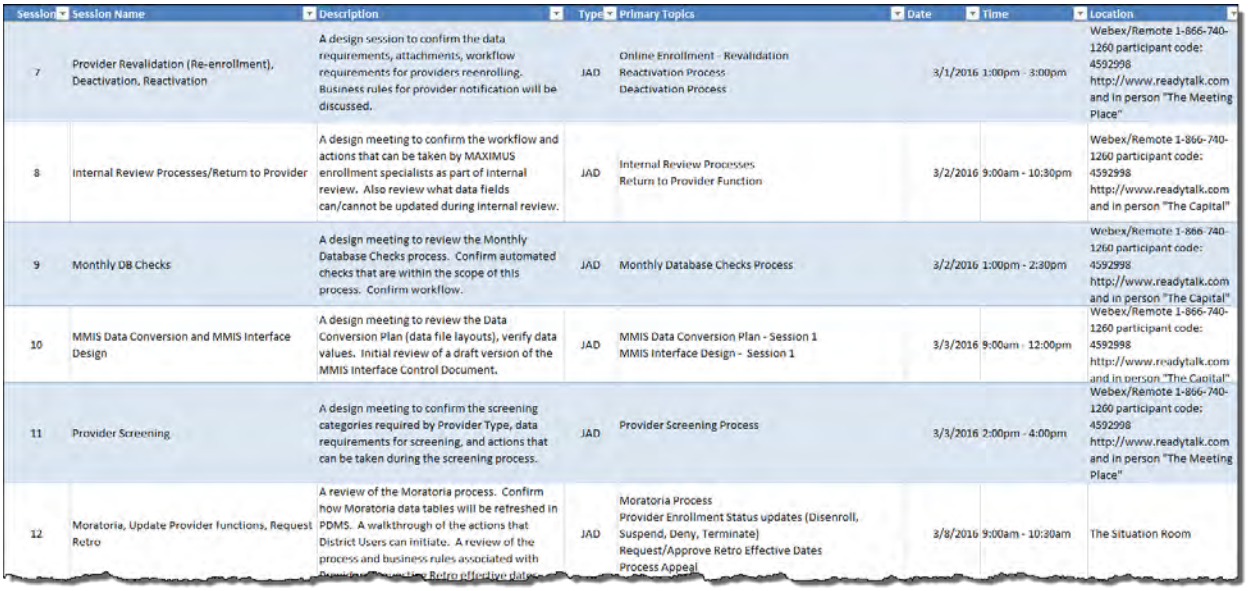
3.10.2.4.1Design Phase

In advance of the Design Phase, MAXIMUS creates and submits the Application Configuration and Maintenance Plan to the Department. This plan will conform to the requirements for requirement DOC04 in Appendix F. The key sections of the plan will provide details on our approach for the Design Phase and will include a schedule of our planned design iterations. Please refer to *Section 3.10.2.2.2–Incremental Design, Development and Testing* for further details regarding our proposed design iterations for the project.

Using the Application Configuration and Maintenance Plan as a guide, MAXIMUS takes the inputs gathered from the RGA process, conducts Design Sessions with DPHHS subject matter experts, and incrementally creates the System Design Documentation (SDD) packages that the State uses to confirm the Provider Services module configuration. Our technical team uses the SDD as the guide for developing new or modifying existing interfaces and other custom functionality changes. *Exhibit 3.10.2.4-2: Design Phase* shows the key activities and deliverables we complete during the Design Phase of the project.

Exhibit 3.10.2.4-2: Design Phase. *MAXIMUS will conduct a series of Design Sessions with the Department and other external agencies to review system configuration items to confirm that we adequately address all of the State's requirements. We incrementally create SDD packages to document the results of the Design Sessions and submit these to DPHHS for approval. These outputs are integral components of our software development methodology.*

A significant amount of preparation takes place prior to each Design Session. MAXIMUS Business Analysts further decompose the requirements contained in the RTM and organize the requirements into functional categories and workflows. We examine the gaps exposed during Requirements Validation and analyze their potential impact to the system. We prepare test providers in the test environment to demonstrate existing system functionality to the Department, allowing subject matter experts to visualize the workflow and the current business rules being enforced in the base system. We examine the initial data conversion files received from the MMIS vendor to understand the current data requirements for Providers, and to examine the reference data that is currently in place in the MMIS. We review the current paper enrollment forms in use by the State and determine if there are any potential data gaps as compared to what the base system currently captures. We formulate a Design Session schedule and submit the schedule to the Department so that DPHHS can plan accordingly and allocate the necessary resources. *Exhibit 3.10.2.4-3: Design Session Schedule* provides a snippet of the schedule we prepared for our District of Columbia Provider Services project.



Session	Session Name	Description	Type	Primary Topics	Date	Time	Location
7	Provider Revalidation (Re-enrollment), Deactivation, Reactivation	A design session to confirm the data requirements, attachments, workflow requirements for providers reenrolling. Business rules for provider notification will be discussed.	JAD	Online Enrollment - Revalidation Reactivation Process Deactivation Process	3/1/2016	1:00pm - 3:00pm	Webex/Remote 1-866-740-1260 participant code: 4592998 http://www.readytalk.com and in person "The Meeting Place"
8	Internal Review Processes/Return to Provider	A design meeting to confirm the workflow and actions that can be taken by MAXIMUS enrollment specialists as part of internal review. Also review what data fields can/cannot be updated during internal review.	JAD	Internal Review Processes Return to Provider Function	3/2/2016	9:00am - 10:30pm	Webex/Remote 1-866-740-1260 participant code: 4592998 http://www.readytalk.com and in person "The Capital"
9	Monthly DB Checks	A design meeting to review the Monthly Database Checks process. Confirm automated checks that are within the scope of this process. Confirm workflow.	JAD	Monthly Database Checks Process	3/2/2016	1:00pm - 2:30pm	Webex/Remote 1-866-740-1260 participant code: 4592998 http://www.readytalk.com and in person "The Capital"
10	MMIS Data Conversion and MMIS Interface Design	A design meeting to review the Data Conversion Plan (data file layouts), verify data values. Initial review of a draft version of the MMIS Interface Control Document.	JAD	MMIS Data Conversion Plan - Session 1 MMIS Interface Design - Session 1	3/3/2016	9:00am - 12:00pm	Webex/Remote 1-866-740-1260 participant code: 4592998 http://www.readytalk.com and in person "The Capital"
11	Provider Screening	A design meeting to confirm the screening categories required by Provider Type, data requirements for screening, and actions that can be taken during the screening process.	JAD	Provider Screening Process	3/3/2016	2:00pm - 4:00pm	Webex/Remote 1-866-740-1260 participant code: 4592998 http://www.readytalk.com and in person "The Meeting Place"
12	Moratoria, Update Provider Functions, Request Retro	A review of the Moratoria process. Confirm how Moratoria data tables will be refreshed in PDMS. A walkthrough of the actions that District Users can initiate. A review of the process and business rules associated with Requesting/Approving Retro effective dates	JAD	Moratoria Process Provider Enrollment Status updates (Disenroll, Suspend, Deny, Terminate) Request/Approve Retro Effective Dates Process Appeal	3/8/2016	9:00am - 10:30am	The Situation Room

Exhibit 3.10.2.4-3: Design Session Schedule. *MAXIMUS prepares and submits a Design Session schedule to the Department so that DPHHS leadership can plan for and allocate resources to attend the Design Sessions.*

MAXIMUS submits a Design Session agenda to the Department (and other stakeholders, as required) in advance of conducting each session. Specific topics, questions, assumptions, etc. are outlined in the agenda, which the Business Analyst uses to facilitate the session. During the Design Sessions, MAXIMUS Business Analysts lead a discussion on the questions and assumptions that must be confirmed to establish the direction to take on the configuration of the base system to meet Department requirements. We demonstrate the current functionality in the base system as it relates to the Design Session topic being discussed. We focus on the identified gaps and collaborate with the Department to offer potential alternatives and options to avoid having to make any customizations to the base system. Decisions that cannot be made during these sessions are documented as action items for the Department to address in a future Design Session. At the conclusion of each Design Session, we prepare and submit meeting minutes to the Department for review.

Web Portal Design

MAXIMUS facilitates Design Sessions with the State that focus on mapping the data fields from existing State Medicaid enrollment and application forms to their corresponding data fields in the base system. This exercise tells us where there may be State specific differences in the editing and processing of data fields as defined in the base solution. *Exhibit 3.10.2.4-4: Enrollment Form Data Mapping* provides an excerpt from the data mapping spreadsheet we use for as part of our SDM.

MC19 Section	MC19 Field	DECISIONPoint Field	DECISIONPoint Screen	Section	Notes
Section A - General Information	A.1 Check Type of Enrollment Request: ☐ a. New Provider Number	Begin Enrollment	Provider Home Page	My Actions	Action
Section A - General Information	A.1 Check Type of Enrollment Request: ☐ b. New FTIN Number	Begin Enrollment	Provider Home Page	My Actions	Action
Section A - General Information	A.1 Check Type of Enrollment Request: ☐ c. Provider Renewal	Revalidation	Provider Home Page	My Actions	Action
Section A - General Information	A.1 Check Type of Enrollment Request: ☐ d. Add Member to Provider Group	Revalidation	Provider Home Page	My Actions	Action
Section A - General Information	A.1 Check Type of Enrollment Request: ☐ e. Update Expired Provider Number	Ownership Change	Provider Home Page	My Actions	Only if we convert inactive providers
Section A - General Information	1. Check Type of Enrollment Request: ☐ f. Current provider number (if b, c, d, or e is checked) _____	Add Affiliate	Provider Home Page		

Exhibit 3.10.2.4-4: Enrollment Form Data Mapping. *MAXIMUS produces a data mapping spreadsheet to facilitate sessions with State business users and to identify any required configuration changes to web portal enrollment screens or data model.*

This analysis identifies the necessary configuration changes to existing web portal screens as well as to the data model. This exercise also offers reassurance to the State's business team that the resulting Provider Services solution addresses all required fields from the State's enrollment forms, and that we understand the business rules for processing each field. Conversely, we also map the base system's screens to the State's enrollment forms, which allows us to easily identify where there are field discrepancies between our base system and DPHHS requirements. DPHHS may choose to keep the base system attributes that are not identified in the DPHHS requirements, or opt to remove these fields from the web portal screens for the MPATH solution. We also confirm edit and code table values, such as provider types, taxonomy codes, and specialties, so the technical team can make the configuration changes to the code tables and business rules engine. We identify the source for each edit and code table, and define how each table will initially be populated prior to testing. We also define data governance rules so we fully understand who will be responsible for providing updates and how frequently the updates must be performed.

Interface Design

MAXIMUS works with the Systems Integrator and the Department to design the required interfaces for the MPATH project. A key artifact of the design documentation is the Interface Control Document, which includes specifications for each interface specified in the contract. MAXIMUS has produced interface documentation for our Provider-facing web portal implementations in Tennessee, Nebraska, and the District of Columbia. We have a large library of application components that validate incoming data and format outbound provider data. These pre-built routines will aid design and development for all required interfaces.

MAXIMUS works closely with the Systems Integrator and the Department to design efficient and effective data exchanges. Interface approaches include application programming interfaces, open services under a service-oriented architecture (SOA), shared standards-based data stores, and other means as proposed during analysis. Once all parties agree to the best solution for the Provider Services module and the Trading Partner, the formatting, editing, and

validation rules, data exchange frequency, error reporting, and data correction procedures are defined in the Interface Control Document. Early analysis and automation of the data exchanges and error processing reduces reliance on the Trading Partners during the post-implementation support period. Designing automated and flexible exchanges saves time and mitigates the impact of changes to the interfaces after implementation.

Based on our experience, we anticipate the majority of the design focus will be on the MMIS interface because of the complexity and the amount of business rule configuration and data editing that will be required. MAXIMUS designed our base system with flexible data exchange formats to allow integration with other systems.

Our experience has shown that linking MMIS Provider application data to all the corresponding Provider data in the base Provider Services system is challenging and requires time-consuming analysis to make sure that data being sent to and from the MMIS is free of errors and will trigger the intended business actions and communications in both systems. We have pre-built functionality that notifies the sender when errors occur and suspends any transactions that do not pass system edits and validations. Similarly, we correct and reprocess any transactions rejected by trading partner systems. Careful analysis and extensive testing are required prior to implementation.

All three of our existing modular provider implementations require different technical approaches to implement the MMIS interface. In Tennessee, we use web services supported by shared trigger tables. In Nebraska, we interface with two systems that contain data for different provider types using flat files. These flat file exchanges contain the data and error processing information necessary for hands free updates to both systems. In the District of Columbia, we use a variable length flat file structure that aligns closely with the MMIS data model. Previous experience with a variety of MMIS interface exchange approaches and pre-built functionality supports our ability to quickly and effectively integrate with the Montana MMIS application. Our team spent a great deal of time identifying how we can best cross-reference the normalized data in our data model to the MMIS and other interfaces, and this experience will fast track the requirements confirmation, design, development, testing, and implementation of the MPATH interfaces implementation.

The interface Design Sessions we conduct on the MPATH project lead to the creation and submission of the Interface Control Documents, which we package with the System Design Document and submit to the State for review and approval. *Exhibit 3.10.2.4-5: Sample MMIS Interface Design* is an example of an Interface Control Document that specifies the characteristic and validation rules for each data field.

Mnemonic	Title	Description	Size	Valid Value Reference/Fomatting
MAX-TRANS-ID	Transaction ID	A unique transaction identifier generated by PDMS.	PIC 9(10).	
MAX-ACTION	Transaction Type	The Type of Transaction being processed.	PIC X(2).	AP - Add Provider – The transaction is adding a new Provider/Group that does not currently exist in the MMIS. UP - Update Provider – The transaction is updating information for a Provider/Group that already exists in the MMIS. AM - Add Group Member – The transaction is adding a new Group Member (Affiliation) to an existing Provider group in the MMIS. UM - Update Group Member – The transaction is updating information for a Group Member (Affiliation) that already exists in the MMIS.
MAX-PDMS-ID	MAXIMUS Provider ID	The unique ID assigned to the Provider in PDMS	PIC 9(10).	The MAXIMUS PDMS number will be padded with zeors on the left.
P-ID	Provider ID	A unique number that the system assigns to the provider for MMIS claims processing.	PIC X(9).	
P-RA-MEDM-CD	Provider RA Medium Code	This code indicates the medium that the provider receives remittance advices from the State.	PIC X(1).	Number:1621 Provider RA Medium Code--This code indicates the medium that the provider receives remittance advices from the State.
P-LOCN-CD	Provider Location Code	NOT USED BY DC-- This code indicates whether the provider's practice location is in-state, out-of-state or on the	PIC X(1).	Number:0190 Provider Location Code
P-RA-SORT-SEQ-CD	Prov RA Sort Sequence Cd	This code indicates how the remittance advice is sorted before it is sent to the provider.	PIC X(1).	Number:0178 Prov RA Sort Sequence Cd--This code indicates how the remittance advice is sorted before it is sent to the provider.
P-RA-PRT-SUSP-CD	Prov RA Print Suspense Cd	This code indicates if suspended claims should be printed on the remittance advice.	PIC X(1).	Number:0179 Prov RA Print Suspense Cd--This code indicates if suspended claims should be printed on the remittance advice.
P-PRACT-TY-CD	Provider Practice Type Code	This code indicates the type of practice that the provider belongs to.	PIC X(1).	Number:0203 Provider Practice Type Code--This code indicates the type of practice that the provider belongs to.
P-INDIV-GRP-CD	Prov Individual Group Code	This code tells if the provider represents a group or an individual or both	PIC X(1).	Number:0205 Prov Individual Group Code--This code tells if the provider represents a group or an individual or both.

Exhibit 3.10.02.4-5: Sample MMIS Interface Design. *This sample design shows a small subsection of the interface design document for our Provider Services implementation in the District of Columbia.*

Our flexible interface design and expert staff are capable of supporting all interface data transfer integration and associated business rules for Provider data updates. The existing interfaces incorporate checks and balances to make sure data transfers between the Provider Services Module and various Trading Partners are successful. In addition, the interface designs include exception handling to allow MAXIMUS and State authorized users to process any errors encountered in the interface.

System Design Document

The System Design Document (SDD) describes the changes needed to the system to address system gaps identified during the requirements review process. The SDD includes documentation of the design areas, as shown in *Exhibit 3.10.2.4-6: SDD Deliverable Content.*

SDD Section	Content Description
Component Description	General description of the Component including purpose, basic functionality, and business areas supported
Use Cases	A list of use cases that are handled by the component
Screen Designs	This section contains screen design documentation, which includes: ▪ Mapping of data fields to all inquiry, display, or input screens ▪ Mapping of data presented to a user via a window to that data's source table and column ▪ Required data fields, field edits, and special processing rules
MPATH Schema/ Database Design	This section provides a listing and brief description of each MPATH table, including its structure.

SDD Section	Content Description
MPATH Architecture	The architecture section provides an architectural schematic of the overall MPATH solution, along with a description of each architectural component.
Configuration Rules	This section contains a definition of all rules to be controlled by the rules-based solution.
Job Streams	Identifies inputs and outputs, control, job stream flow, work flow, error and recovery procedures, and operating procedures
Network Schematic	Diagram with all network components and technical security control
Edits	List of all edits for the input data and the corresponding error messages
Interface Control Documents	This section contains an identification of major interfaces (internal as well as external) files and processing architecture. It will contain an Interface Control Document (ICD) for each interface as developed in coordination with DPHHS and the external partner.
Reports	This section contains a listing and brief description (purpose, frequency) of reports to be produced, including fields on the report and any calculations completed in the report.
MPATH Detailed RTM	The DSD version of the RTM is extended to include: ▪ A cross-reference of the requirements to system components, where relevant ▪ A decomposition of requirements where additional detail has been provided

Exhibit 3.10.2.4-6: SDD Deliverable Content. *MAXIMUS produces all required System Design Documentation for the State by updating our existing design documentation from our base Provider Services solution.*

Efficiency

Our base solution is already bundled with extensive design documentation. For the MPATH implementation, we leverage this documentation largely as is, including our screen designs and logical/physical data model documentation. The investment we made in our product design documentation during our previous implementations saves time during the Development Phase, and through re-use, improves the quality of the design documentation. We modify existing documentation and produce new documentation when required. During the Design Sessions, our Business Analysts demonstrate the system functionality, decompose the requirements reviewed, and update the specifications to reflect any necessary changes. Each of the four application design packages, the Interface Control Documents, and the conversion design package are incrementally delivered to DPHHS for review and approval as they are completed. The development team begins configuration and development immediately following approval. Our proposed incremental approach enables DPHHS to understand and approve the component designs in manageable volumes. In our experience, this approach speeds time to delivery, while at the same time allowing for requisite quality in the resulting software product.

MAXIMUS delivers each SDD package to the State for review and approval, and then stores the design documentation in our SharePoint project repository, which is accessible by the State. *Exhibit 3.10.2.4-7: Design Document Repository* provides an example of the types of design documentation we currently produce and maintain for our base product implementations.

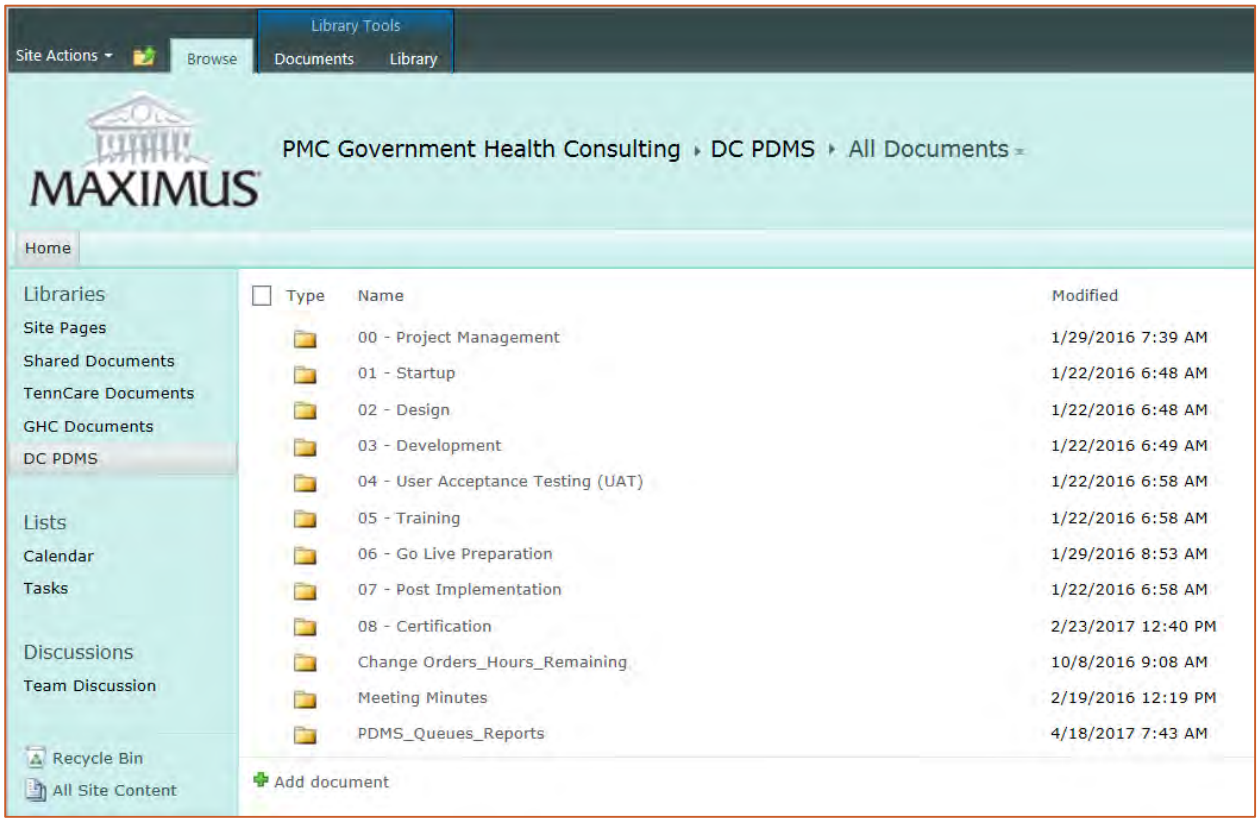


Exhibit 3.10.2.4-7: Design Document Repository. *MAXIMUS produces all required design documentation and stores them on a project repository approved by the State, which is accessible via the Internet.*

3.10.2.4.2Construction Phase

MAXIMUS will configure or enhance our base system to deliver all anticipated functionality and to support the defined requirements for the system. We make sure that we have executed all unit tests on each software component and that they function according to the approved specifications. We group the components together to conduct integration and system testing activities to confirm proper operation of the system. Our iterative approach enables the Department to quickly see the results of the requirement gaps and facilitates spending more time on testing rather than deliverables and documentation. We have found our approach works well when the base system meets the majority of the business requirements and the focus is on identifying configuration updates to align with a state's specific business processes and required workflows. We utilized this approach in Tennessee, Nebraska, and the District of Columbia. *Exhibit 3.10.2.4-8: MPATH Construction Phase* illustrates the key tasks and milestones that need to be completed during this phase.

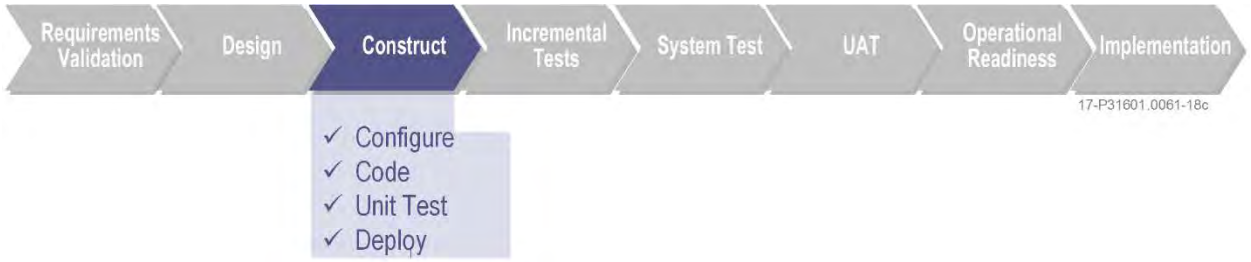


Exhibit 3.10.2.4-8: MPATH Construction Phase. *MAXIMUS makes configuration changes and develops new functionality to fill requirement gaps. We conduct Unit testing of each application component and Integration testing of functionally related components prior to Incremental testing and User Experience Confirmation.*

Our configuration and build approach uses a repeatable cycle, with each development package producing independent but complete functional components that are promoted from design through development, testing, and user experience confirmation. This approach benefits the user community in that users are able to view functionality early on in the project and provide value-added feedback to the MAXIMUS Business Analysts and development team. We found in our existing projects that when business users are able to review the system and confirm how business processes should be performed, fewer changes are requested during User Acceptance Testing.

Our development team uses the System Design documentation to configure and update the base solution to meet the requirements of DPHHS and the needs of the Provider community. We always find ways to tailor our system and services solution to the needs of our customer's stakeholders. We have found that increased self-service and engagement with the program works best for Providers. We will make changes to the application configuration and modify the Corticon business rules engine to reflect how business is conducted in Montana.

Expertise

The configuration of the system is a set of tasks with a number of activities occurring simultaneously. MAXIMUS constructs, modifies, or configures the software components required to support the Provider Services module installation for the State. MAXIMUS Business Analysts use the existing Montana application documentation and instructions to make an initial assessment of the changes necessary to code tables and business rules. We review and confirm these changes in Design Sessions with DPHHS Subject Matter Experts (SMEs). For configuration items that may be new to DPHHS, such as a new system workflow, our Business Analysts provide structured walkthroughs of the workflows with the State's SMEs. We explain how workflows are changed through configuration modifications in our system and then identify where changes are required. Starting with the base system flows allows DPHHS to leverage the lessons learned from our other project implementations as a basis for defining the solution. We document changes and our developers update the application as required based on the specifications. These specifications cover the full range of value changes from State code tables to the modification of workflow actions that trigger notifications and interface transactions.

By using our Open Interface Framework, we configure the MMIS and other required interfaces to the unique requirements of MPATH. This provides a quick and effective integration with the MMIS and other external partners while limiting the impact of changes in the Provider Services base system. Other configuration activities include updates to the underlying data structures for risk profiling and configuration of the workflows that support the screening and enrollment processes including any State

review and approval processes. In conjunction with the configuration work, MAXIMUS builds any new application components to address functionality gaps that cannot be made strictly through system configurations.

3.10.2.4.3Design, Configuration and Build Requirements

The following table includes Attachment F Design, Configuration and Build Requirements, our summarized response to each requirement, and the section(s) in our proposal in which we provide our detailed response.

ID	Design, Configuration and Build Requirement	MAXIMUS Summarized Response
DCB01	The Contractor's solution shall accommodate customer preferences for communications by electronic inbox, written correspondence, email, text, and phone.	The MAXIMUS Provider Services solution allows providers to choose their communication preference including electronic inbox, written correspondence, email, text, and phone. MAXIMUS views this requirement more as a functional requirement than a methodology related requirement. We will categorize this requirement as such during Gap Analysis and Design to be sure it receives proper focus.
DCB02	The Contractor shall develop and submit a design session schedule, agendas, and minutes for review by the Department.	MAXIMUS develops and submits a design session schedule, agenda, and minutes for review by the Department. We submit agendas at least 24 hours prior to each meeting and submit minutes within 48 hours after the conclusion of each meeting. Refer to *Section 3.10.2.4.1–Design Phase* for more information.
DCB03	The Contractor shall conduct collaborative design sessions to address all gaps identified during requirements validation.	MAXIMUS conducts design sessions to address all gaps identified during the requirements gap analysis. MAXIMUS reviews all of the requirements in the RTM and confirms that the existing functionality meets the needs of the requirement or that the gap is identified and a solution is determined. Refer to *Section 3.10.2.4.1–Design Phase* for more information.
DCB04	The Contractor shall, in the design sessions, recommend solutions for each configuration gap, as defined in requirements validation, that will produce the desired business outcomes. If a gap cannot be addressed via configuration, the Department may consider making policy changes before approving customizations to the solution.	MAXIMUS recommends solutions for each configuration gap as they are identified in the requirements gap analysis. If a gap cannot be addressed via configuration, MAXIMUS works with the Department to find alternative solutions.
DCB05	The Contractor shall demonstrate completed functionality frequently as the solution is configured/built, using a fully functioning environment.	MAXIMUS incrementally demonstrates a fully functional system as the system is configured/built. MAXIMUS breaks the system into 4 phases plus interfaces and conversion for design, development, and testing so the Department can see more of the system sooner. Refer to *Section 3.10.2.4.2-Construction Phase* for more information.
DCB06	The Contractor shall migrate completed releases promptly through various testing levels all the way to User Acceptance Testing (UAT).	MAXIMUS migrates releases through all levels of testing on the way to UAT. Each release is unit tested by developers, system tested and regression tested by system testers, and integration tested prior to being released for UAT. Refer to *Section 3.10.2.4.2–Construction Phase* for more information.
DCB07	The Contractor shall provide the design for online help approach and documentation, as appropriate.	MAXIMUS provides a design for online help and documentation.
DCB08	The Contractor shall work with the Systems Integrator and the Department to establish required interfaces as defined in the detailed scope of work.	MAXIMUS works with the Systems Integrator and the Department to establish required interfaces and to develop the associated designs. We will write separate design documents for these interfaces so that they can be designed with and reviewed by the appropriate parties. Refer to *Section 3.10.2.4.1–Design Phase subsection Interface Design* for more information.
DCB09	The Contractor shall provide office space for Contractor staff and meeting rooms as necessary to support the scope of work and contractual obligations.	MAXIMUS provides office space for any contractor staff as well as meeting rooms to support the contractual obligations.

ID	Design, Configuration and Build Requirement	MAXIMUS Summarized Response
DCB11	The Contractor shall develop auditing and general controls to ensure the effective use of the technical architecture and data in meeting requirements.	MAXIMUS develops auditing and controls to verify the effective use of the technical architecture and data in the process of meeting the RFP requirements.
DCB12	The Contractor must provide all technology and equipment for contractor staff necessary to support and complete the scope of work and the contractual obligations.	MAXIMUS provides all technology and equipment for our staff to complete the contract obligations.
DCB13	The Contractor shall be responsible for operating and maintaining any software needed to support all module components and project tools in use by the Contractor.	MAXIMUS verifies that all software needed to support module components and project tools are maintained and are operating as expected.
DCB14	The Contractor's solution shall have the ability to print a properly formatted representation of the entire screen (including sections not displayed without scrolling) and associated data in the application.	MAXIMUS allows the user to take a screen print of their screen to obtain an entire screen display. MAXIMUS also allows the client to generate a PDF of their application for printing. . MAXIMUS views this requirement more as a functional requirement than a methodology related requirement. We will categorize this requirement as such during Gap Analysis and Design to be sure it receives proper focus.
DCB15	The Contractor shall provide recommendations for simplified business rules and business processes to the Department.	MAXIMUS works with the Department to simplify business rules and processes. MAXIMUS has these discussions with the Department during the requirements gap analysis and throughout design and development.
DCB18	The Contractor shall configure, support and maintain all components of the solution in a manner that reflects performance expectations described in this RFP.	The MAXIMUS solution meets or exceeds all performance expectations outlined in the RFP.
DCB19	The Contractor's solution shall be free of any software components that are the result of legacy code transformation.	The MAXIMUS solution does not contain any legacy code components.
DCB20	The Contractor's solution shall provide Web based content that is supported by standard web browsers and are mobile and tablet compatible.	The website is hosted on the IIS web server and is accessible via standard web browsers. We use JQuery and AngularJS lightweight JavaScript frameworks to help make the website responsive. We also use BootStrap to make the website user friendly and to provide a consistent look and feel. These different frameworks allow the website to be browser agonistic. We follow a methodical and high impact approach to cross browser testing and high-risk browser testing for browsers that are used by 95 percent of the United States Chrome, IE, Safari, Firefox, and Opera.
DCB21	The Contractor's solution shall allow the Department to edit and change any static text in the application and correspondence templates. All static text must be approved by the Department.	The MAXIMUS solution allows the Department to edit and change any static text in the application and correspondence templates. MAXIMUS confirms that the State has approved all changes. MAXIMUS views this requirement more as a functional requirement than a methodology related requirement. We will categorize this requirement as such during Gap Analysis and Design to be sure it receives proper focus.

3.10.2.5 Data Conversion, Cleansing and Migration

3.10.2.5 Data Conversion, Cleansing and Migration

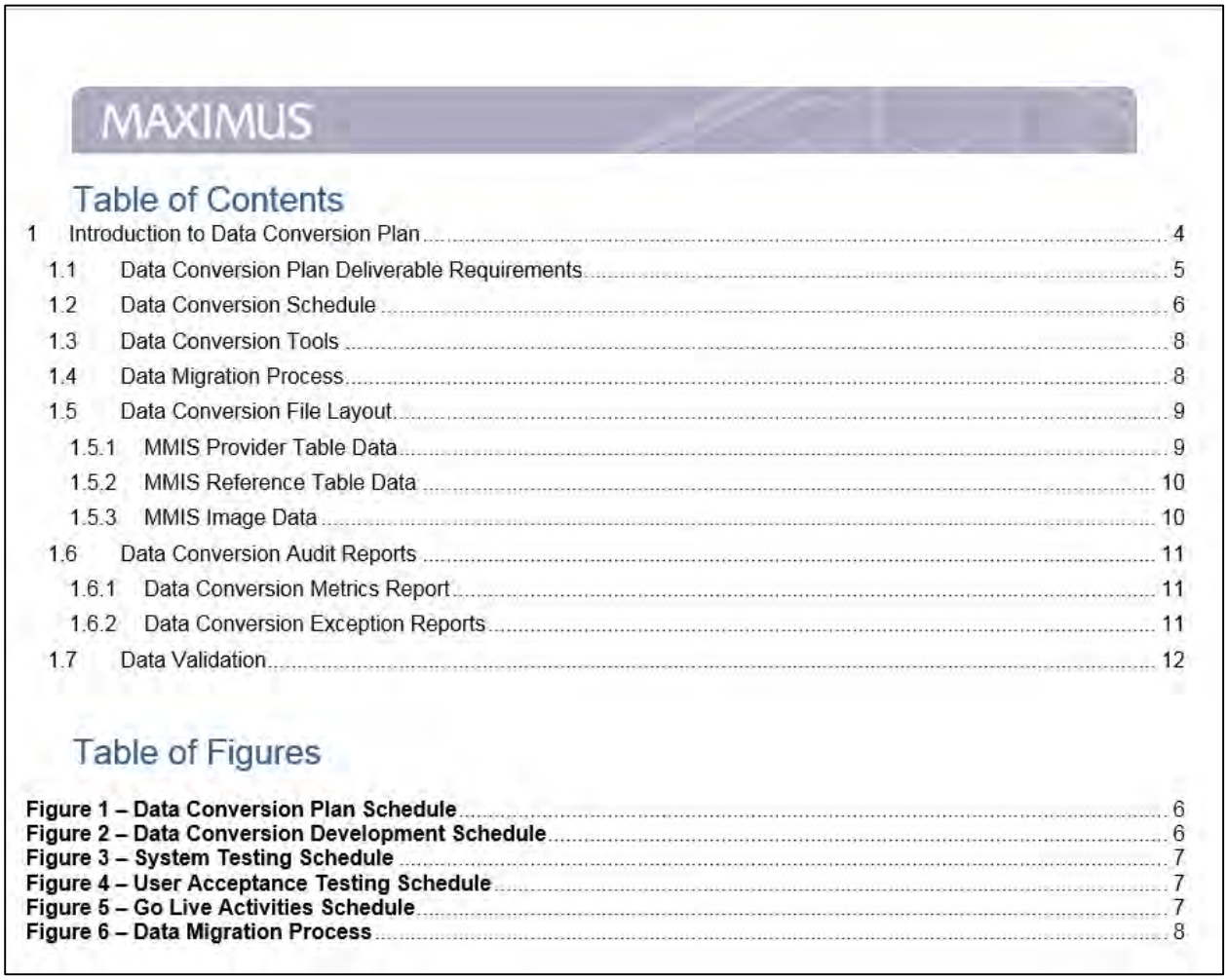
Data conversion, cleansing, and migration activities required to support the scope of work contained in this RFP include planning, identifying and analyzing conversion specifications, testing, execution and coordination of all data and file conversion, migration and data cleansing processes.

Data conversion often encounters risks and issues related to the complexities in defining the relationship between source and target data structures, differences in the data required for processing between legacy and new systems and the historical changes to processing requirements and valid codes that may result in data inconsistencies and missing data conditions. The Offeror must describe their approach to meet each of the detailed data conversion, cleansing and migration requirements defined in Attachment F, Requirements Matrix.

Our approach for data conversion is to engage DPHHS and the MMIS vendor early in the design process, with the intent of obtaining data specifications and test data from the source systems as early in the design process as possible. We propose to execute a number of conversion test loads using production data so we are able to progressively identify and resolve data anomalies, elaborate our conversion design, and assess the impact of data changes on the functional processing in the Provider Services system. Using production data helps identify rare and unique data scenarios and gaps in the initial conversion analysis. Identification of these challenges early in testing allows us to apply edits and transformations prior to the data load, which reduces the impact of the corrections if they were to be needed post-implementation.

3.10.2.5.1 Data Conversion Planning

MAXIMUS will create, submit, and maintain a Data Management, Conversion, and Migration Plan for the MPATH project that will meet the State's documentation requirements as outlined in Appendix F - Requirement DOC03. During Requirements Validation, MAXIMUS will conduct meetings with the Department to validate and confirm the conversion related requirements for the MPATH project. This will also include at least one meeting with the State and the MMIS vendor to discuss and agree upon the types of extract files that will be submitted from the MMIS legacy system, the general format of those files (e.g., pipe-delimited, fixed length, etc.) and the method of transfer. Other important requirements that need to be verified include the potential need to convert data from any source system other than the MMIS and the amount of Provider data history that needs to be converted. Based on our initial meetings and the validation of the conversion requirements, MAXIMUS will create and submit the Data Management, Conversion, and Migration Plan. *Exhibit 3.10.2.5-1: Sample Data Conversion Plan* shows the outline of our data conversion deliverable for our Provider Services implementation in the District of Columbia.



MAXIMUS

Table of Contents

1 Introduction to Data Conversion Plan 4
1.1 Data Conversion Plan Deliverable Requirements 5
1.2 Data Conversion Schedule 6
1.3 Data Conversion Tools 8
1.4 Data Migration Process 8
1.5 Data Conversion File Layout 9
1.5.1 MMIS Provider Table Data 9
1.5.2 MMIS Reference Table Data 10
1.5.3 MMIS Image Data 10
1.6 Data Conversion Audit Reports 11
1.6.1 Data Conversion Metrics Report 11
1.6.2 Data Conversion Exception Reports 11
1.7 Data Validation 12

Table of Figures

Figure 1 – Data Conversion Plan Schedule 6
Figure 2 – Data Conversion Development Schedule 6
Figure 3 – System Testing Schedule 7
Figure 4 – User Acceptance Testing Schedule 7
Figure 5 – Go Live Activities Schedule 7
Figure 6 – Data Migration Process 8

Exhibit 3.10.2.5-1: Sample Data Conversion Plan. *MAXIMUS will use planning documentation from previous projects and create the Data Conversion Plan to meet the requirements of the State.*

Our plan is shaped on best practices and lessons learned specifically for the migration of data from a legacy MMIS into a modular Provider Services database. We believe our approach for the MPATH project can reduce risk for the Department and the MMIS vendor by leveraging the existing extract and load procedures from our recent implementation for the District of Columbia. The District's MMIS is supported by the same vendor as Montana's, and we would assume the source MMIS database would be similar in each installation. During the initial conversion meetings with the State and MMIS vendor, we will review the conversion process we used for the District and determine if we can reuse that project's extract procedures for the Montana implementation.

3.10.2.5.2Data Conversion Approach

Our approach to conversion is based on a proven methodology and consists of several steps. We take the test data files from the source systems, stage them, and load them into our secure conversion data test environment. We conduct an initial data analysis in the staging tables to determine where potential data cleansing activities may need to occur. We also test the user interface against the converted data to make

CONFIDENTIAL

sure the user interface is capable of displaying and updating the converted data. We follow a basic process of Extract, Transform, and Load (ETL), with measures taken to safeguard data quality and validation throughout the design, development, and implementation cycle. Our data conversion approach is comprised of four primary steps:

- **Step 1** – Extraction and Analysis
- **Step 2** – Cleansing
- **Step 3** – Transformation
- **Step 4** – Data Loading

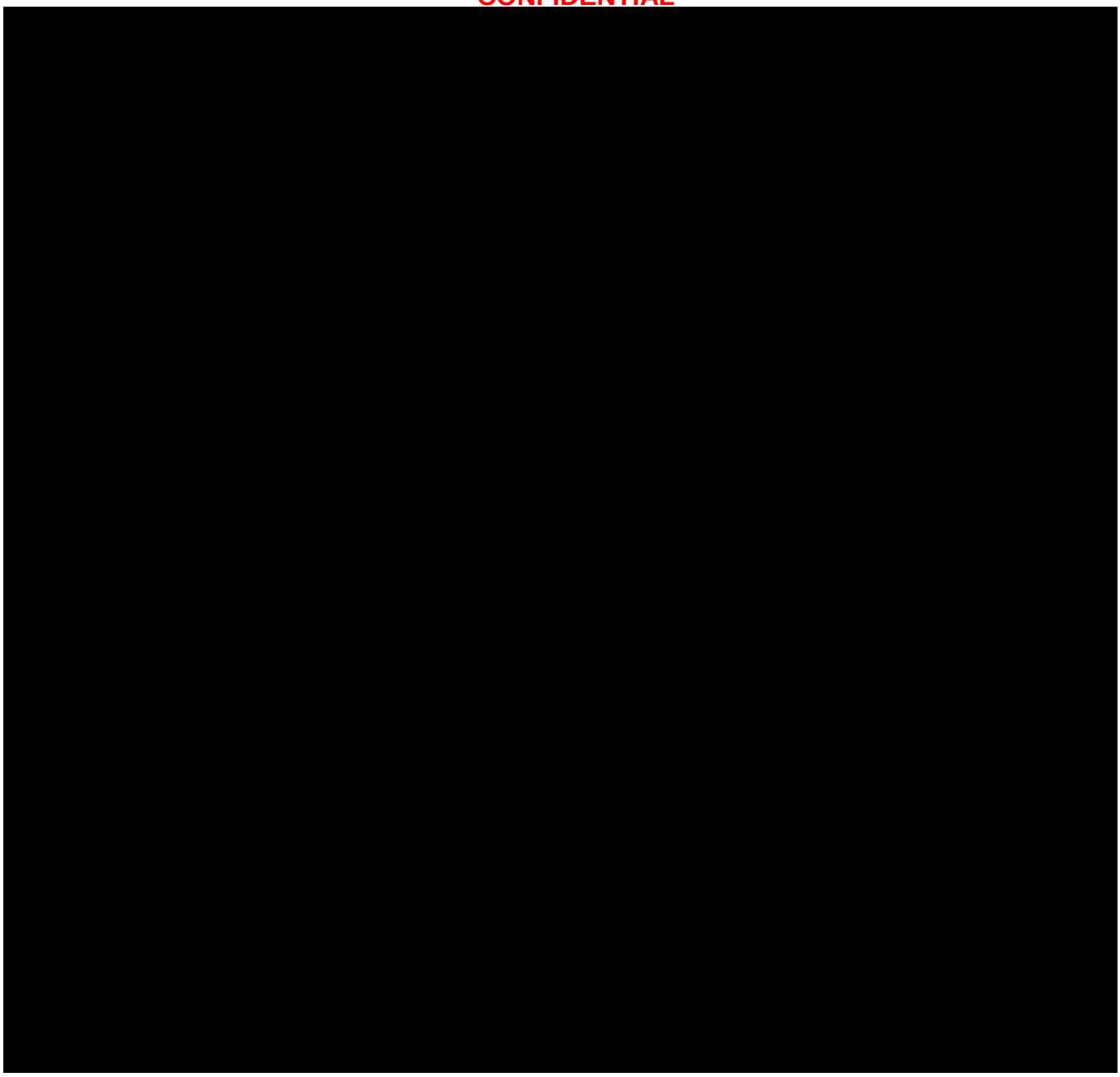
We repeat Steps 1 through 3 until all data issues are resolved. We then load and test the data in business test scenarios, such as re-enrollment and provider data updates. We repeat the conversion load process as many times as needed prior to implementation. Each iteration represents a trial conversion pass, with a final, full production conversion load at go-live.

We produce data mapping documentation for our all system implementations. We understand the importance of performing due diligence to disposition the data elements required to support the conversion process. This includes a source-to-target data mapping, as well as a target-to-source data mapping. The target-to-source data mapping is especially important, as this is when we identify the need for default values necessary to fill required data in the target database that may not be available within the

[redacted]

CONFIDENTIAL

CONFIDENTIAL



MAXIMUS conducts data conversion meetings to review the existing system and begins the mapping exercise between the provider data sources and our solution early in the project. Based on our experience, we recommend that data conversion requirements analysis start immediately following the project initiation so that we can use converted data during integration, system, and user acceptance testing. Once data mapping has occurred, we document data gaps, data purification, and data transformation needs in the conversion analysis document. We carefully identify the source of each data element and any special editing that must occur. We also discuss MMIS data requirements and business rules to make sure Medicaid Payment processing is not negatively impacted by data sent from the Provider Services module.

At the conclusion of the conversion analysis sessions, MAXIMUS presents the conversion analysis document and data mapping grids to the State, and works collaboratively to make updates and corrections

to finalize the conversion requirements. We will submit the data mapping documentation as one of the packages within the overall System Design Document deliverable, which we discuss in further detail in *Section 3.10.2.4, Design Configuration, and Build*. We provide the application development team with the documentation so they can account for any missing data or data anomalies that require special handling in the web-based components of the system. MAXIMUS has found that regularly scheduled and frequent meetings are critical to keep conversion analysis, design, and development from delaying System Testing. We also propose that a dedicated team of MAXIMUS, DPHHS, and MMIS vendor staff should be assigned to four weeks of conversion data analysis work sessions to resolve all conversion issues in a timely manner. Our team will hold follow-up work sessions as necessary to resolve any issues that arise during testing.

The Provider update/revalidation process alleviates many of the data cleansing issues. However, some data issues may need to be resolved at the source systems. We attempt to identify data issues and agree on a resolution as soon as possible to allow the MMIS vendor as much time as possible to correct the data so that these issues do not impact the implementation date. Additional corrections may require input from Providers, business operations, or other project stakeholders. The online Provider Services application notifies Providers which data values require correction during their initial update or revalidation. This approach allows conversion and loading of the data from the MMIS, even if some of the required data fields are missing or incorrect. The application sends updates made by Providers back to the MMIS via the MMIS interface to test that the systems are in sync.

In our design and development of the data conversion process, we consider the following key items:

- **Data conversion to pre-populate web forms for existing Providers –** As existing Providers revalidate, it is easier for them to start with the existing data from the MMIS. Using the MMIS data eases the transition from paper to electronic applications, while reducing the data entry burden on the Providers**.**
- **Data cleanup as a part of enrollment and revalidation –** We find that as existing Providers are processed, data anomalies related to practice locations and group affiliations may need to be corrected and the corrections automatically sent back to the MMIS.
- **Cross-referencing normalized data to MMIS data –** We track Providers uniquely, and information about related Providers (e.g., affiliates) is stored as relationships. We resolve missing relationships, key identifiers, and other data discrepancies in the staging tables prior to loading. In some cases, this means ‘plugging in” a temporary value that will pass our solution’s data integrity checks until the data can be corrected by the Provider. Examples of this type of information might be missing or invalid SSNs, License Numbers, Effective Dates, etc.

3.10.2.5.3Conversion of Electronic Documents/Images

In our very recent District of Columbia implementation, we gained extensive, practical experience in converting imaged documentation from an MMIS legacy system. We worked closely with the District and the District’s MMIS vendor to design an efficient process for converting the images into our target system image repository. *Exhibit 3.10.2.5-3: Converting Electronic Documents* shows an excerpt from our Data Management, Conversion, and Migration Plan submitted on our District of Columbia project. As shown in *Exhibit 3.10.2.5-3*, our approach in the District required us to receive two separate file submissions from the MMIS.

1.5.3 MMIS Image Data

The MMIS image data will be provided by Xerox in two files. The images themselves will be provided in a single compressed file (.zip). The second file will be an index that identifies and describes all the images in the compressed file. The index will be a pipe delimited text file in the structure described in the Table 8.

Table 8 - MMIS Image Data
Describes the table and data elements that will be provided by Xerox for image conversion.

Data Element	Description
Medicaid ID	The unique Medicaid ID of the Provider in the MMIS.
Document Type	A code identifying the type of document being converted. This value will match one of the Provider Attachment Type Codes (reference table number 0173).
File Name	The physical name of the image file.
Uploaded Date	The day upon which the file was scanned or uploaded into the MMIS or some approximate date.

Exhibit 3.10.2.5-3: Converting Electronic Documents. *MAXIMUS has experience in converting electronic documents from the legacy MMIS into a modular Provider Services solution. We bring this experience to the State and shape an approach that meets the requirements of the MPATH project.*

To efficiently accomplish the conversion of the electronic documents, the MMIS vendor sent us an initial (very large) file submission, and then periodically sent us delta files (only new images) from that point forward. This allowed us to build our converted image repository incrementally, and the final load at the final implementation conversion was largely routine. We recommend taking a similar approach for the Montana implementation.

End users of the Provider Services system are able to view the converted images through the Provider Services web portal. Providers are only able to view images for their account, while internal users are able to view the images for all converted Providers. We created a separate document section that is displayed on each screen in the system so a user can always conveniently open and review all electronic documents from the legacy MMIS. *Exhibit 3.10.2.5-4: Converting Electronic Documents* provides a snippet of a screen where we show these converted images to users through the Provider Services user interface. As shown in the screenshot in *Exhibit 3.10.2.5-4*, users are able to see all converted images, and have the ability to open and view each image from the Provider Services web portal.

CONFIDENTIAL

3.10.2.5.4Conversion Reports

MAXIMUS produces conversion audit reports and conversion exception reports to document and analyze the results of each conversion load. An exception report is generated for each conversion table each time a conversion run is executed. Each exception report will identify the MMIS Provider table from which data is being converted, and detailed information about the exception that the application encountered during processing. We will confirm the design and layout of these reports with the Department during our initial Conversion requirements meetings and adjust them, if required, to meet any of the unique needs for the MPATH Provider Services conversion. *Exhibit 3.10.2.5-5: Conversion Reports* is an excerpt from our conversion design document from our recent implementation in the District of Columbia.

MAXIMUS

1.6 Data Conversion Audit Reports

1.6.1 Data Conversion Metrics Report

The metrics report will be generated each time a conversion run is executed. The metrics report will identify each MMIS table from which data is being converted and provide counts related to the number of transactions processed. Table 9 describes the primary data elements on the report and an example of the report is provided as an attachment to this deliverable.

Table 9 – Data Conversion Metrics Report
Describes the data elements that will appear on the report

Data Element	Description
Table Name	The name of the table from which the transactions are being processed. This is the physical table name as specified in the MMIS Provider Table Data workbook. For example, PADDRSTB in the Provider Address Table.
Table Description	The description of the table from the MMIS Provider Table Data workbook. For example, the description PADDRSTB is Provider Address Table.
Transactions Received	The total number of records (transactions) in the table.
Transactions Processed	The number of records (transactions) in the table that were successfully processed.
Transactions Not Processed	The number of records (transactions) in the table that were not processed. In other words, the number of transactions for which there are exceptions.

1.6.2 Data Conversion Exception Reports

An exception report will be generated for each conversion table each time a conversion run is executed. Each exception report will identify the MMIS Provider table from which data is being converted and detailed information about the exception that was encountered during processing. Table 10 describes the primary data elements on the report and an example of a report for Addresses (PADDRSTB Exceptions) is provided in an attachment to this deliverable.

Table 10 – Data Conversion Metrics Report
Describes the data elements that will appear on the report

Data Element	Description
Table Name	The name of the table from which the transactions are being processed. This is the physical table name as specified in the MMIS Provider Table Data workbook. For example, PADDRSTB in the Provider Address Table.
Exception Reason	A text explanation for why the record (transaction) could not be processed.
Exception Action	If applicable, an action that needs to be taken to resolve the exception. This data element may signify no action (the transaction based on defined rules does not need to be converted), an action to be taken by MAXIMUS, or an action to be taken by DHCF/Xerox.
(Details…)	The report will contain the detailed data elements from the associated MMIS Data Table. At least one of these data elements will be sufficient to identify the specific transaction that was not processed (e.g. P-SYS-ID).

Exhibit 3.10.2.5-5: Conversion Reports. *We package our conversion process with existing audit reports that we will bring to the MPATH project and tailor, if required, to meet any of the unique needs of the Department.*

3.10.2.5.5Data Conversion, Cleansing and Migration Requirements

The following table includes Attachment F Data Conversion, Cleansing and Migration Requirements, our summarized response to each requirement, and the section(s) in our proposal in which we provide our detailed response.

ID	Data Conversion, Cleansing and Migration Requirement	MAXIMUS Summarized Response
DC01	The Contractor shall convert all member and provider data history for any member or provider that has been active within the past three years and three (3) years of all applicable operational data from the State's legacy systems. The Department may require additional data to be converted on an exception basis to support ongoing business needs (e.g., TPL recovery, SURS recovery and drug rebate). The Contractor shall produce comparative reports for all converted data. Any data quality issues will be addressed by the State within each source system.	MAXIMUS will convert provider data for all providers that have been active within the past three years and three years of all applicable operational data from the State's legacy systems. During conversion design, we will work with the Department to determine if there is any additional data that we may need to convert on an exception basis. We package our conversion load process with audit reports that we produce for each conversion run. We submit these reports to the Department and to the source agency (MMIS) for review, and use them as input for potential data quality issues that may need to be addressed for the next conversion iteration. Refer to *Section 3.10.2.5.1 Data Conversion Planning, Section 3.10.2.5.2–Data Conversion Approach* and *Section 3.10.2.5.4–Conversion Reports*.
DC02	The Contractor shall provide authorized Department or other designated staff access to an environment to validate converted data and provide support for the data validation effort.	Live conversion data is loaded into both our System Test and UAT test databases. The Department will have access to the project's UAT database. Department staff will be able to view the converted providers through the Provider Services user interface and MAXIMUS will produce reports that will assist Department users with the review.
DC03	The Contractor shall work with the State to identify the data elements from existing legacy systems that will or will not be converted to the Contractor's solution. The Contractor shall work with the State to achieve desired business outcomes without familiar data elements.	MAXIMUS will work collaboratively with the Department to determine which data elements will be converted from the existing legacy system(s). We believe we will bring tremendous value to the State when facilitating these types of decisions. We have been required to do full data conversion in all 3 of our modular implementations. As a result, we have accumulated a long list of lessons learned and best practices for data conversion. We will share these experiences with the State to help assist with this effort, but will be sure to implement the conversion solution to meet the expectations and needs of the State. Refer to *Section 3.10.2.5.2–Data Conversion Approach*.
DC04	The Contractor shall work with the State to identify data elements or fields in the Contractor's solution that are not available to be converted from the legacy system, and whether the conversion programs should fill them with default or initial values.	The data mapping exercise that we will go through with the State will expose these types of gaps. These gaps in data mapping serve as the agenda items for the collaborative conversion design meetings. We will work with the State to assist with which fields can be defaulted or set to initial values. We have experienced the need to do this extensively in other States and already have pre-built routines to handle defaulting data fields. Refer to *Section 3.10.2.5.2–Data Conversion Approach*.
DC05	The Contractor must perform one or more trial conversions as necessary, before final conversion of the data, and present the results to the State.	Our approach to data conversion calls for multiple iterations and trial conversion runs. In our most recent District of Columbia implementation, we conducted six trial conversions prior to running the full production load. For each trial run, we produce reports and share the results and analysis with the State. For each iteration, the data is loaded and tested in business test scenarios such as re-enrollment and provider data updates. We repeat the conversion load process as many times as needed prior to implementation. Each iteration represents a trial conversion pass, with a final, full production conversion load at go-live. Refer to *Section 3.10.2.5.2–Data Conversion Approach*.
DC06	The Contractor shall produce the reports necessary to demonstrate adequate checks and balances within the data conversion process.	We package our conversion load routines with audit and data quality reports. We generate these reports for each trial conversion run and share them with the State and the MMIS vendor. Refer to the 'Conversion Reports' sub-section for further details on how we implement this functionality for the Department. Refer to *Section 3.10.2.5.4–Conversion Reports*.

ID	Data Conversion, Cleansing and Migration Requirement	MAXIMUS Summarized Response
DC08	The Contractor shall convert electronic documents identified by the Department in a format approved by the Department.	MAXIMUS will convert all electronic documents from the source system image repository for providers that will be converted to the Provider Services database. In our District of Columbia implementation, we converted images from the source MMIS image repository. To accomplish this, we worked closely with the District and the District's MMIS vendor (Conduent) to define the set of files that would be required to conduct the conversion. Refer to the 'Conversion of Electronic Documents/Image's sub-section for further details on our approach for converted electronic images. Refer to *Section 3.10.2.5.3—Conversion of Electronic Documents/Images*.
DC09	The Contractor shall provide convenient access to electronic documents from systems being replaced.	End users of the Provider Services system are then able to view the converted images through the Provider Services web portal. Providers are only able to view images for their account, while internal users are able to view the images for all converted Providers. We created a separate document section that is displayed on each screen in the system so a user can always conveniently open and review all electronic documents from the legacy MMIS. Refer to the 'Conversion of Electronic Documents/Image's sub-section for further details on our approach for converted electronic images. Refer to *Section 3.10.2.5.3–Conversion of Electronic Documents/Images*.

3.10.2.6 Testing

> 3.10.2.6 Testing
>
> Testing is a critical component for successful implementation of any system configuration/development effort, therefore, in depth, process driven, fully documented testing processes are required for all implementations and configuration changes within the Montana Healthcare Programs enterprise. The testing activities shall include planning, managing and executing a comprehensive testing effort to include unit, system, regression, parallel, integration and UAT.
>
> Prior to implementing a new release, the Contractor is responsible for ensuring that all required tests are performed and evidence that each component meets or exceeds all relevant functional, technical, security, and performance requirements is provided. The Offeror must describe their approach to meet each of the detailed testing requirements defined in Attachment F, Requirements Matrix.

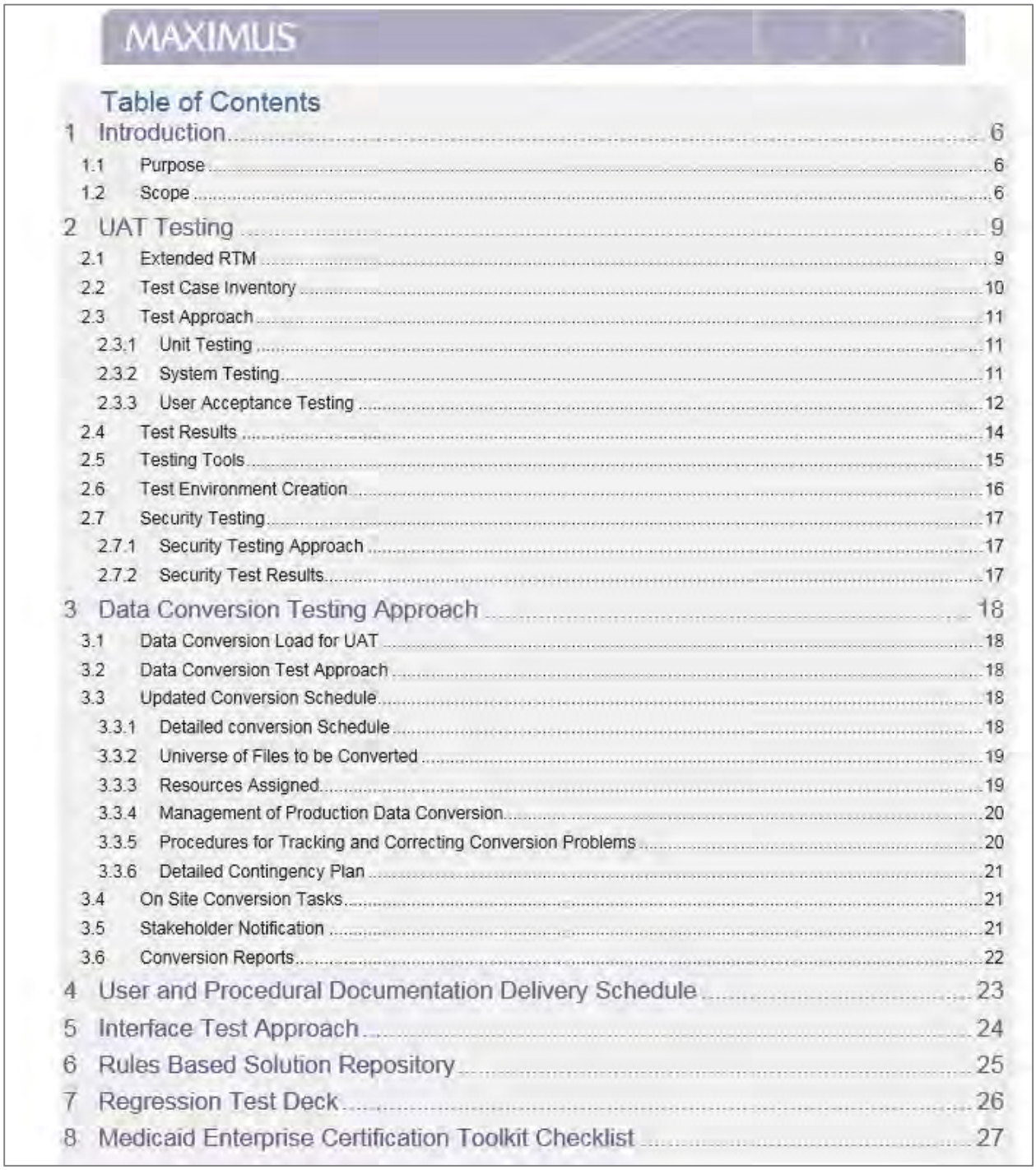
Testing is a critical aspect of the system implementation and the ability for the system to support the administration of the MPATH Provider Services module. MAXIMUS uses test planning to validate that the system meets the requirements specified by the contract and scope of work agreed to by the Department and MAXIMUS. Testing requires a systematic approach to validating features and functionality, as well as finding, documenting, correcting, and re-testing defects. To confirm that the system is adequately tested and ready for implementation, MAXIMUS conducts the following testing:

- Incremental Unit Testing
- System Integration Testing
- User Acceptance Testing
- Regression Testing
- Parallel Testing
- Performance Testing

Test scenarios will cover all aspects of the screening and enrollment process to verify that the system and its components are operationally ready to support the post-implementation business processes. As defects are uncovered and reported, our development staff review the submitted documentation and determine which components require remediation. We assign defects to the development staff responsible for the

remediation of the software or data correction based on the priority rating of the defect. Our staff performs regression testing in a mutually agreed upon fashion, based on the potential impact of the software changes.

We create and submit two primary test planning deliverables to the Department; these will shape the testing activities for the MPATH project. First, the Master Test Plan will describe our plan for conducting all testing activities and the types of testing that will be performed on the project. *Exhibit 3.10.2.6-1: Sample Master Test Plan* shows the table of contents from our test planning deliverable in the District of Columbia Provider Services implementation.



MAXIMUS

Table of Contents

1 Introduction 6
1.1 Purpose 6
1.2 Scope 6
2 UAT Testing 9
2.1 Extended RTM 9
2.2 Test Case Inventory 10
2.3 Test Approach 11
2.3.1 Unit Testing 11
2.3.2 System Testing 11
2.3.3 User Acceptance Testing 12
2.4 Test Results 14
2.5 Testing Tools 15
2.6 Test Environment Creation 16
2.7 Security Testing 17
2.7.1 Security Testing Approach 17
2.7.2 Security Test Results 17
3 Data Conversion Testing Approach 18
3.1 Data Conversion Load for UAT 18
3.2 Data Conversion Test Approach 18
3.3 Updated Conversion Schedule 18
3.3.1 Detailed conversion Schedule 18
3.3.2 Universe of Files to be Converted 19
3.3.3 Resources Assigned 19
3.3.4 Management of Production Data Conversion 20
3.3.5 Procedures for Tracking and Correcting Conversion Problems 20
3.3.6 Detailed Contingency Plan 21
3.4 On Site Conversion Tasks 21
3.5 Stakeholder Notification 21
3.6 Conversion Reports 22
4 User and Procedural Documentation Delivery Schedule 23
5 Interface Test Approach 24
6 Rules Based Solution Repository 25
7 Regression Test Deck 26
8 Medicaid Enterprise Certification Toolkit Checklist 27

Exhibit 3.10.2.6-1: Sample Master Test Plan. *MAXIMUS submits the Master Test Plan to the Department; this plan details the testing approach for all required levels of testing. We leverage deliverables from previous projects and shape them to meet any of the unique testing needs for the MPATH project.*

MAXIMUS will produce the Master Test Plan to contain the required level of detail as specified in Attachment F requirement DOC26 – Master Test Plan. The Master Test Plan will reassure the Department

that the proper test planning has occurred and that the appropriate level of resources is allocated to perform the required testing. We describe our detailed testing approach in the subsections below.

3.10.2.6.1 Incremental Unit Testing

The MAXIMUS team performs Incremental Testing for each functional package. As our developers complete the configuration and enhancement efforts and successfully unit test, they deploy the new functionality via system builds to the System Testing environment. MAXIMUS testers incrementally perform tests following use case scenarios created during the design phase for the functional package. We perform both positive and negative test cases that verify that the system functions have been implemented correctly and the system behaves as expected. We test all data entry field edits, correlation edits, workflow navigation, user messages and business rules following predefined test scenarios with expected outcomes. *Exhibit 3.10.2.6-2: Incremental Testing* shows the sequence of these tasks within our SDM and the primary activities that we will perform during Incremental Testing.

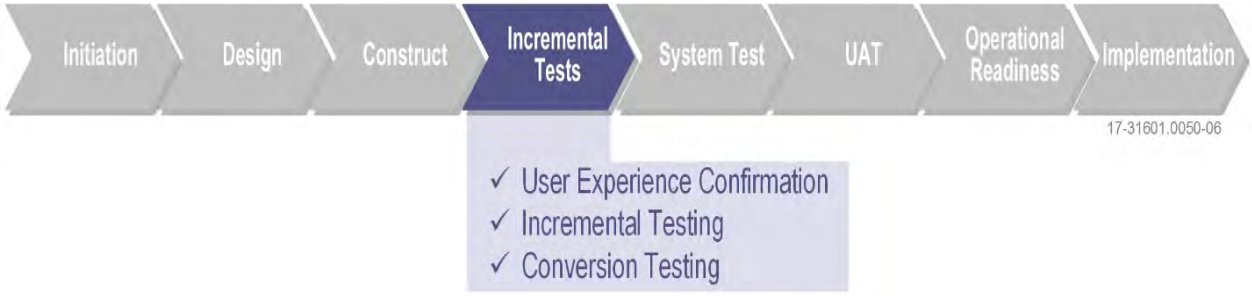


Exhibit 3.10.2.6-2: Incremental Testing. *Incremental testing tests functionally related components, conversion, and interfaces independently.*

Exhibit 3.10.2.6-3: User Interface Checklist Test provides an example of a User Interface Component checklist test script. Checklist tests are the first tests performed on each application component following deployment to the System Testing environment. These low-level tests verify the documented design changes were completed correctly prior to conducting more extensive user storyboard based testing. We use the Checklist in conjunction with the associated user interface design document to conduct the test and record the results. We use similar templates for reports and notices.

User Interface Information

Web Page Name	<enter the component being tested>
Developer	<enter the name of the developer>
Specification Name	<enter the related specification name>
Functional Analyst	<enter design analyst name>

Test Results

Test Conducted	Cycle	Description	Results / Defects	Tester
MM/DD/YYYY	1.0	First Attempt	<pass/defect>	<enter test analyst name>

Additional Components (Pop-ups) Tested

Component Name	Comment
	<explain how testing was accomplished if dependent component was not available or not fully functioning>

Testing Dependencies

Dependency	Comment
<explain what, if any actions must be performed prior to execution of the test>	Additional comments & instructions

Exhibit 3.10.2.6-3: User Interface Checklist Test. *We use checklists tests in conjunction with test cases and design documents to verify the changes.*

User Interface Test Conditions

Test Description	Positive	Negative	N/A	Additional Comments
Layout (view/report) Correct	☐		☐	
Protected Fields	☐		☐	
Required Fields	☐		☐	
Picklist Values	☐	☐	☐	
Primary Edits	☐	☐	☐	
Complex Edits	☐	☐	☐	
Error Messages	☐		☐	
Hyperlinks	☐		☐	
Data Retrieval/Display Formatting	☐		☐	
Special Filtering/Sorting	☐		☐	
Calculations	☐		☐	
Database Updates	☐		☐	
Actions Generated?	☐		☐	
Correspondence Generated?	☐		☐	
Audit Trail Created?	☐		☐	

Exhibit 3.10.2.6-3: User Interface Checklist Test (continued). *We use checklists tests in conjunction with test cases and design documents to verify the changes.*

The last step in Incremental Testing is the User Experience Confirmation. During this activity, MAXIMUS business analysts execute use cases created during the Design phase to demonstrate the functionality and workflow of the new components. These orchestrated walkthroughs of the workflows and each component within the increment give the DPHHS stakeholders an early opportunity to see the system changes and confirm that the system is meeting their expectations. Although the system is not fully tested at this point, the benefits of an early preview of the application are obvious. In the event that we identify minor changes or omissions in the design, we can frequently accommodate the modifications without impact to the planned implementation date.

3.10.2.6.2 System Integration Testing

System Integration Testing occurs when we have assembled all the incrementally tested functionality and tested it end-to-end. System Integration Testing includes a full data conversion load and exchanges of interface test files with external partners. Our testing methodology adheres to industry best practices for testing, such as those of the PMI PMBOK® guide and the Institute of Electrical and Electronic Engineers

(IEEE) standard for software verification and validation. We create test scenarios that simulate provider initiated account registration, application entry and submission, application review, provider screening, and state review and approval for a large variety of different provider types. We map Jama Contour Requirements to Application Components and Test scripts to provide confirmation that we have addressed the requirement in the software inventory, and that each application component has been tested to verify that the component achieves the requirement. Prior to starting the System Integration Testing, we execute a full conversion data load with current data from all the data sources. We run revalidation, reenrollment, and provider initiated update test cases using the converted provider data. *Exhibit 3.10.2.6-4: System Testing* illustrates the activities that need to be completed and the sequence of these tasks within our SDM.

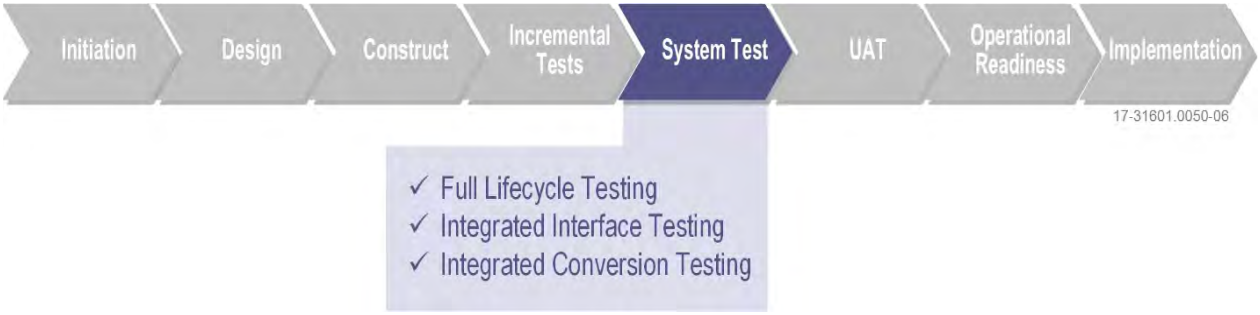


Exhibit 3.10.2.6-4: System Testing. *This test phase assembles all of the incrementally tested application components to support the business lifecycle based testing.*

We document our System Integration Testing approach in the System Test Plan that we submit in advance of the System Integration Testing phase. The System Test Plan will conform to the requirements as set forth in Attachment F requirement DOC28 – System Test Plan. An important attachment to the System Test Plan will be the Test Script Inventory, which will provide the Department with a complete inventory of the end-to-end system tests we plan to execute on the project. This inventory in turn serves as valuable input into the User Acceptance Testing phase. MAXIMUS plans and tracks System Integration Testing using the Test Script Inventory contained in Jama Contour. The inventory of tests includes new provider applications for all provider types, re-enrollment and revalidation tests, interface tests, batch processing tests, reports tests, security role tests, and conversion data tests. *Exhibit 3.10.2.6-5: New Provider Applications Test Inventory* is an example of the test inventory of New Provider Application Tests. The tests include the workflow steps and an indicator as a means to track progress of test execution at each step in the workflow. These step results are then rolled up to provide an overall assessment of System Integration Test progress.

Scenario #	N001	N002	N003	N004	N005	N006	N007	N008
Priority	1	1	1	1	1	1	1	2
Provider ID	Assigned	Assigned	Assigned	Assigned	Assigned	Assigned	Assigned	Assigned
Enrollment Form	Non-Inst	Non-Inst	Non-Inst	Non-Inst	Non-Inst	Non-Inst	Non-Inst	ASARS
Application Type	Standard	Standard	Standard	Standard	Standard	Standard	Standard	Standard
Outcome	Approve	Deny	Approve	Deny	Approve	Deny	Deny	Approve
Provider Category	Individual	Group	Individual	Group	Individual	Group	Individual	Facility
Provider Type	Nurse Practioner	Nurse Practioner	Dentist	Dentist	Optometrist	Optometrist	Podiatrist	Clinic, Adlt Subst Abuse
Taxonomy	207Q00000X	363L00000X	1223G0001X	1223G0001X	207W00000X	152WV0400X	213ES0103X	Input
ZIP5-ZIP4	20024-2612	20002-6445	20001-2000	20002-2001	20003-2002	20021-2004	Input	Input
NPI	1003062381	1003065665	1003063009	1003062522	1003063165	1003063199	1003065749	1003060096
Test Case #	N001-1	N002-1	N003-1	N004-1	N005-1	N006-1	N007-1	N008-1
Test Date	8/30/2016	8/30/2016	08/19/216	8/19/2016	8/19/2016	8/19/2016	8/30/2016	8/30/2016
Workflow Steps	**Pass**	**Pass**	**Pass**	**Pass**	**Pass**	**Pass**	**Pass**	**Pass**
Provider Management Home	P	P	P	P	P	P	P	P
Create User Account	P	P	P	P	P	P	P	P
Create User Account - Enter Provider Info	P	P	P	P	P	P	P	P
Create User Account - Create User ID & Password	P	P	P	P	P	P	P	P
User Account Activation	P	P	P	P	P	P	P	P
Provider Management Home	P	P	P	P	P	P	P	P
Identification Screen	P	P	P	P	P	P	P	P
Identification - Provider Information	P	P	P	P	P	P	P	P
Identification - USMLE/ECFMG (Citizenship)	P	N/A	P	N/A	P	N/A	P	N/A
Identification - Primary Contact Information	P	P	P	P	P	P	P	P
Licenses and Classifications	P	P	P	P	P	P	P	P
L&C - Specialties & Additional Specialties	P	P	P	N/A	P	N/A	P	P
L&C - Taxonomy - Primary/Secondary Taxonomy	P	P	P	P	P	P	P	P
L&C - Professional Licenses	P	P	P	P	P	P	P	P

Exhibit 3.10.2.6-5: New Provider Applications Test Inventory. *MAXIMUS uses the test script inventory to track progress and completeness of System Integration Testing.*

A plan and schedule for interface testing is developed in conjunction with the Trading Partners and interface file exchanges occur throughout the System Integration Testing Phase until all parties are satisfied that the interfaces are working properly.

System Integration Testing truly tests and confirms all aspects of the system. We execute test scenarios with both positive and negative tests to verify access and update capabilities for every security role. We also test document uploads and retrieval. All reports are executed and verified for accuracy against the conversion load counts. All provider notifications that we generate are checked against the specifications documents to make certain provider communications are timely and accurate. Once System Integration Testing has successfully completed and DPHHS has approved the results, MAXIMUS will move to User Acceptance Testing where DPHHS and external vendors perform testing.

3.10.2.6.3User Acceptance Testing

Immediately following the System Integration Testing, User Acceptance Testing commences. User Acceptance Testing (UAT) is the final system focused test before we proceed to operational readiness testing. MAXIMUS recognizes the importance of technical and functional support for UAT. We address the UAT stage within our project plan, and we will coordinate with the Department to identify the users who will participate in the scheduled testing. In addition, we will clearly define the desired outcomes with Department input and approval to confirm that we are meeting expectations for Provider Services system functionality.

MAXIMUS brings extensive experience to the State in our efforts to facilitate a successful UAT for MPATH. MAXIMUS has successfully implemented three major modular provider system implementations for Tennessee, Nebraska, and District of Columbia. Our clients validated the system functionality during each project's UAT phase. All of these projects involved Provider-facing web portals, electronic registration, internal workflow, and interfaces to the State's MMIS. *Exhibit 3.10.2.6-6: User Acceptance Testing* illustrates the activities that need to be completed and the sequence of these tasks within our SDM.

Exhibit 3.10.2.6-6: User Acceptance Testing. *User Acceptance Testing is the project phase that DPHHS and their External Partners execute their test scenarios to verify MPATH is working as expected.*

UAT allows users to see the entire system so they can review and accept system components prior to production implementation. It is also during this phase that the Department can take extra time to test how the Provider screening and enrollment business processes work within the context of the fully functional system. MAXIMUS will validate the full system and hosting infrastructure, as well as fail-over and recovery in the event of a disaster, is fully implemented for UAT. If required, the Department will have online access to test database tables and files to allow the State to independently prepare test data, run tests, and review test results.

MAXIMUS does not simply turn the system over to our client with the expectation that UAT goes well unassisted. We work closely with the State Test Lead to develop a plan that supports the available State staffing and timeline for UAT. Our business and test analysts are available to answer questions, provide suggestions, and assist when problems are encountered. UAT planning starts with a predefined set of test scenarios from System Integration Testing that DPHHS can use for tracking and monitoring their assignments and progress. We anticipate these test artifacts will be shared with the Systems Integrator Vendor and that updates will be made to reflect how DPHHS and their external partners want to conduct UAT.

As part of our approach for MPATH deployment, we will conduct interface and operations testing to confirm the solution is capable of supporting the policies set forth by DPHHS. Test scenarios will cover all aspects of the screening and enrollment process to prove that the system and its components are operationally ready to support the operational activities required post-implementation. We place particular emphasis on testing the MMIS interface, as well as the initial data conversion load of provider data from the MMIS. In the absence of the ESB, the interface testing for the initial implementation of the Provider Services solution will consist of a flat file exchange via SFTP with the MMIS vendor. We plan for and submit numerous file exchanges with the MMIS. *Exhibit 3.10.2.6-7: Sample MMIS Interface File Submission* provides an example of the contents of one of the interface test files we sent to the MMIS during User Acceptance Testing on our District of Columbia project.

Tue 10/18/2016 11:19 PM

UAT Interface File #8 High Volume Test

To

Cc

You replied to this message on 10/19/2016 6:26 AM.

All,

We have uploaded the eighth UAT Interface file to the MAXIMUS Xchange MoveIt directory, "Health Services/DC PDMS/MMIS/Test/From MAX."

The file name is: DC_TEST_MMIS_PROV_OUT_20161018.txt
It contains 126 Add Provider and 10 Update Provider Transactions from UAT. This is the high volume test file. It also contains the two Tax ID change transactions that Diane requested, one with an FEIN change, the second with an SSN change.

It is ready to download and process.

Please advise us when the response file is available.

John

John Walz
Senior Project Manager,
Program Modernization Consulting

Exhibit 3.10.2.6-7: Sample MMIS Interface File Submission. *We plan for and submit numerous test files to the MMIS during UAT.*

The testing that occurs leading up to each test interface file submission is well scripted. We recommend that the actual users that will be involved in the Provider enrollment and screening business processes participate as the users during UAT. In this model, a group of testers need to function as the Provider community to simulate the submission of enrollments, revalidations, and updates from the Provider Services web portal. The group of users involved from an operations standpoint will depend on the choice the Department makes regarding Option B Services. If the State chooses to procure the Option B Services from MAXIMUS, then the MAXIMUS operations team will assume the role of conducting provider reviews and screening during UAT. If the State does not opt for Option B, the incumbent vendor currently supporting Provider Services operations should assume these roles.

In addition to providing UAT support, the MAXIMUS team continues testing throughout the UAT period to deliver the best possible product. We hold weekly meetings to discuss and resolve any issues that the State and MAXIMUS testers encounter. Our suggested sequence of testing starts with simple scenarios and gradually incorporates more and more complex real world production tests that include document generation, converted data, interfaces and batch processing. We suggest DPHHS focus their initial testing on the common, or 80 percent scenarios, that are most likely and most critical to be processed correctly in the first 90 days following implementation. This approach allows the testers to become comfortable with how the system works and to confirm that the system correctly processes the lion's share of the workload. Less frequent, rare, and complex scenarios should be tested after the common scenarios are proven. Our Test Team is available to assist DPHHS testers with logging defects and retesting after we correct the defects. Our approach for UAT includes:

- Support for MAXIMUS and State user testing designed to demonstrate the system software supports the functional requirements for the system
- Tasks that provide a mechanism to verify system performance is acceptable

- Validation that the system infrastructure is implemented and that it operates as required for production

MAXIMUS will track the execution of UAT test cases and test results. Failed tests with Critical or High defects will result in a failure of the test execution. We log issue reports for all suspected defects in our JIRA tracking system. *Exhibit 3.10.2.6-8: Sample UAT Test Case Inventory* shows the MAXIMUS Test Case inventory that we will bring to the project as a starting point for UAT.

UAT Week	Test Case Category	Test Case Information	Priority
1	New Application	Non-Institutional, Individual, Physician MD, Approval	1
		Non-Institutional, Individual, Physician MD, Denial	1
		Non-Institutional, Group, Physician MD, Approval	1
		Non-Institutional, Group, Physician MD, Denial	1
		Non-Institutional, Group, Physician Group Practice, Approval	1
		Non-Institutional, Group, Physician Group Practice, Denial	1
		Non-Institutional, Individual, Doctor of Osteopathy, Approval	1
		Non-Institutional, Individual, Doctor of Osteopathy, Denial	1
		Non-Institutional, Group, Doctor of Osteopathy, Approval	1
		Non-Institutional, Group, Doctor of Osteopathy, Denial	1
	Interfaces	MMIS Interface Outbound	1
		MMIS Interface Inbound	1
2	Reenrollment	Non-Institutional, Individual, Physician, Approval	1
		Non-Institutional, Individual, Physician, Denial	1
		Non-Institutional, Group, Physician, Approval	1
		Non-Institutional, Group, Physician, Denial	1
		Non-Institutional, Group, Physician Group Practice, Approval	1
		Non-Institutional, Group, Physician Group Practice, Denial	1
		Non-Institutional, Group, Doctor of Osteopathy, Denial	1
		Non-Institutional, Individual, Podiatrist, Approval	1
		Non-Institutional, Individual, Podiatrist, Denial	1
		Non-Institutional, Group, Podiatrist, Approval	1
		Institutional, Facility/Institution, Clinic, Youth Alc/Subst Abuse, Denial	1
	Interfaces	MMIS Interface Outbound	1
		MMIS Interface Inbound	1
	Reports	RP-027 - Count of Service Provider Agreements Received	2
		RP-028 - Count of Servicer Provider Agreements Received (Revalidation)	2
		RP-029 - Count of Service Provider Agreements Outstanding (New Registration/Revalidation)	2
3	New Application	Streamlined, Individual, Physician MD, Approval	3
		Streamlined, Individual, Physician MD, Denial	3
		Streamlined, Individual, Doctor of Osteopathy, Approval	3
		Streamlined, Individual, Doctor of Osteopathy, Denial	3

Exhibit 3.10.2.6-8: Sample UAT Test Case Inventory. *MAXIMUS brings extensive experience in conducting UAT testing for modular implementations. We will leverage our existing test inventories for the MPATH project.*

As we correct defects, we will coordinate with DPHHS and the rest of the UAT Test Team to plan system releases. Once we implement a release into the UAT environment, we publish release notes that specify the defect fixes included in each build. We find that weekly builds work best, but allow for more frequent builds if necessary. During the weekly status meetings, we discuss adjustments to the build schedule and can make changes based on test progress and the backlog of defects.

3.10.2.6.4Regression Testing

Regression testing occurs continuously throughout the testing effort. It is important that regression testing occurs with each build to verify that previous functionality is still working as expected. MAXIMUS develops a "test deck" of test scenarios from the tests that passed during system testing. This subset of test scenarios are the highest priority and/or highest risk scenarios from system testing. The selected test scenarios depend upon the results of the system testing effort. Regression testing occurs at every level of testing and in every environment to verify that builds that migrate into production are clean and do not cause any unforeseen issues with current system functionality. *Exhibit 3.10.2.6-9: Sample Regression Test Deck* is an excerpt from one of the set of regression test decks used to test a change request in the District of Columbia.

Regression Test Case #	R-1	Regression Test Case #	R-2	Regression Test Case #	R-3	Regression Test Case #	R-4	Regression Test Case #	R-5
Application Type	Standard	Application Type	Streamlined	Application Type	Streamlined	Application Type	EPD Waiver	Application Type	Standard
Provider Category	Individual	Provider Category	Individual	Provider Category	Individual	Provider Category	Facility/Institution	Provider Category	Facility/Institution
Provider Type	Dentist	Provider Type	Physician MD	Provider Type	Physician MD	Provider Type	EPD Waiver	Provider Type	Home Health Agency
NPI		NPI		NPI		NPI		NPI	
Medicaid ID		Medicaid ID		Medicaid ID		Medicaid ID		Medicaid ID	
Test Type	*New Application*	Test Type	*New Application*	Test Type	*Re-enrollment*	Test Type	*New Application*	Test Type	*New Application*

Regression Test Case #	R-6	Regression Test Case #	R-7	Regression Test Case #	R-8	Regression Test Case #	R-9	Regression Test Case #	R-10
Application Type	Standard	Application Type	Streamlined	Application Type	Streamlined	Application Type	ADHP 1915(i)	Application Type	Crossover/QMB
Provider Category	Individual	Provider Category	Individual	Provider Category	Individual	Provider Category	Facility/Institution	Provider Category	Group
Provider Type	Podiatrist	Provider Type	Optometrist	Provider Type	Nurse Midwives	Provider Type	Adult Day Health 1915(i)	Provider Type	Dentist, Group Practice
NPI		NPI		NPI		NPI		NPI	
Medicaid ID		Medicaid ID		Medicaid ID		Medicaid ID		Medicaid ID	
Test Type	*New Application/Return to Provider*	Test Type	*Provider Update*	Test Type	*Operator Update*	Test Type	*New Application/Deny*	Test Type	*New Application*

Exhibit 3.10.2.6-9: Sample Regression Test Deck. *MAXIMUS brings extensive experience in conducting regression testing throughout implementations. We will leverage our existing regression test decks for the MPATH project.*

Automated testing is widely used in our development process during our system test phase. Our automated testing tool of choice is Selenium. Selenium is a free (open source) automated testing suite for web applications. Our automated testing approach begins with requiring that the testers record every manual test script execution. There are several reasons for doing this. First, the test tool documents every step in the test execution. This provides the development team a very accurate documentation trail of the actions taken by the tester which is valuable in debugging defects. If the test execution is processed without errors, we store the recorded test script in the Regression test repository.

The suite of successful test scripts are re-executed after every new build is released and the test database has been refreshed. Re-execution of the test scripts that had previously executed without errors verifies that previously working functionality has not been broken. Another use of the automated test tool is in setting up user accounts and registering Providers in the test environments. We use the Selenium test tool to automate these repetitive user interface tasks by creating input parameters that can be populated by data in spreadsheets such as MS Excel. This allows for a very quick population of a large number of user accounts and Provider applications. This methodology allows for a refresh of the test database and very

quick re-population of test environment with clean data. During the design phase, we identify the use cases that will benefit from testing through automation. The testers create the automated test scripts during System Testing.

3.10.2.6.5Parallel Testing

MAXIMUS will support a parallel test with the Department and the MMIS vendor during UAT, as required. We will document our recommended approach for conducting the parallel test in the Master Test Plan and work with the Department to reach agreement on an approach that satisfies the needs for the Provider Services module. We understand the importance to perform parallel testing with the existing production MMIS system to verify that the new system is providing the same results as the existing system.

This parallel testing is done with existing production cases. Test cases for provider enrollments, revalidations, and updates will be conducted in the Provider Services module UAT environment and the MMIS interface file will be generated and sent to the MMIS. On the MMIS side, there will need to be two environments established. First, users will need to data enter the same providers into the legacy MMIS through to approval and completion. The backend claims processing procedures should then be run to process claims against these providers. In a separate environment, the MMIS will need to process the interface file sent from the UAT Provider Services module, loading the new and updated providers into the system. The backend claims processing procedures can then be run against the providers in this environment, allowing for a comparison of results between the new process and the old process. We document any differences in JIRA and assign them to the responsible party. Defects identified that require changes on the Provider Services module will be corrected based on their priority.

3.10.2.6.6Performance Testing

MAXIMUS proposes to devote at least one test cycle to conducting a performance test of the Provider Services module. We will document our approach for conducting the performance test in the Master Test Plan and work with the Department to reach agreement on an approach that satisfies the performance testing need for the module.

To conduct the performance test for the Provider Services module, we use the RADVIEW WebLOAD performance testing tool. RADVIEW WebLOAD is a load testing and performance testing tool designed to stress test web applications. We use the regression test scripts created from the Selenium automated test tool as the test bed for conducting the performance test. Refer to *Section 3.10.2.6.4, Regression Testing* for further details on our use of the Selenium test tool. These same test scripts are used during Performance Testing. The RADVIEW WebLOAD web and mobile load testing software uses the Selenium test scripts in the simulation of thousands of concurrent users. These tests make it possible to test large loads and identify performance problems within an application well before implementing the system in production.

WebLOAD provides analysis data on how the application behaves under the load. WebLOAD monitors and incorporates statistics from the various components of the system being tested: servers, application server, database, network, load-balancer, firewall, etc., and can also monitor the End User Experience and Service Level Agreement (SLA) compliance in production environments. Any performance testing

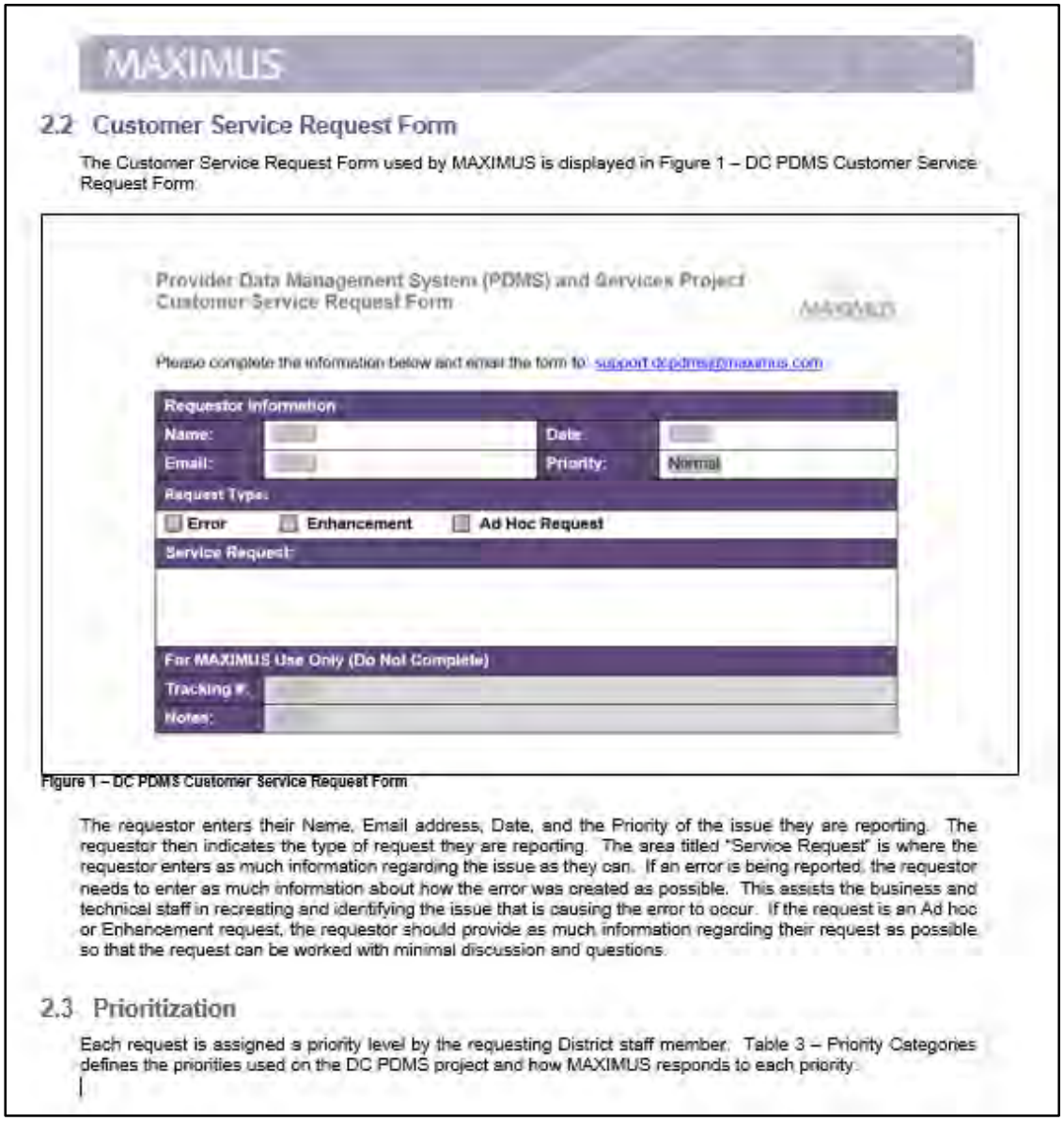
defects identified that require changes to the Provider Services module will be logged into JIRA and corrected based on their priority.

3.10.2.6.7 Defect Management

Throughout testing, it is important for MAXIMUS and the State to work together to submit, monitor, prioritize, and resolve defects that are found as testers complete their work on test scenarios. MAXIMUS develops and maintains a Defect Management Plan that describes the process of submitting, monitoring, and resolving defects. The plan includes at a minimum:

- The approach and tools utilized to assign, identify, prioritize, track, resolve, and regression test system defects.
- Approach to defect severity categorization
- Approach to reporting and documenting defects
- Roles and responsibilities of MAXIMUS, State and external vendor staff
- Describe the defect management processes related to all test types
- Defect management processes after implementation.

Exhibit 3.10.2.6-10: Sample Defect Management Plan is an excerpt from the plan we delivered to the District of Columbia.



MAXIMUS

2.2 Customer Service Request Form

The Customer Service Request Form used by MAXIMUS is displayed in Figure 1 – DC PDMS Customer Service Request Form.

Provider Data Management System (PDMS) and Services Project
Customer Service Request Form

Please complete the information below and email the form to: support.dcpdms@maximus.com

Requestor Information			
Name:		Date:	
Email:		Priority:	Normal
Request Type:			
☐ Error	☐ Enhancement	☐ Ad Hoc Request	
Service Request:			
For MAXIMUS Use Only (Do Not Complete)			
Tracking #:			
Notes:			

Figure 1 – DC PDMS Customer Service Request Form

The requestor enters their Name, Email address, Date, and the Priority of the issue they are reporting. The requestor then indicates the type of request they are reporting. The area titled "Service Request" is where the requestor enters as much information regarding the issue as they can. If an error is being reported, the requestor needs to enter as much information about how the error was created as possible. This assists the business and technical staff in recreating and identifying the issue that is causing the error to occur. If the request is an Ad hoc or Enhancement request, the requestor should provide as much information regarding their request as possible so that the request can be worked with minimal discussion and questions.

2.3 Prioritization

Each request is assigned a priority level by the requesting District staff member. Table 3 – Priority Categories defines the priorities used on the DC PDMS project and how MAXIMUS responds to each priority.

Exhibit 3.10.2.6-10: Sample Defect Management Plan. *MAXIMUS uses proven methods for submitting, tracking, prioritizing, and resolving defects.*

3.10.2.6.8 Testing Requirements

The following table includes Attachment F Testing Requirements, our summarized response to each requirement, and the section(s) in our proposal in which we provide our detailed response.

ID	Testing Requirement	MAXIMUS Summarized Response
TEST02	At a minimum, the Contractor shall provide sufficient segregated environments to support testing processes that are equivalent to the following: a. Integration Testing: End-to-end testing performed to expose defects in the interfaces and in the interactions between integrated module components or other systems and validate the system's readiness to meet non-functional requirements. b. System testing: The process of demonstrating that a program, function, or integrated system components meets its requirements and objectives as stated in the requirements specification. c. Regression Testing: Testing of a previously tested function following modification to ensure that defects have not been introduced or uncovered, as a result of the changes made. It is performed each time the software or its environment is changed, and typically involves automated testing scripts. d. Parallel Testing: Validates that the system achieves the same results as compared to another system (e.g., a legacy system) or previous software version. e. Performance and Load Testing: Verifies the performance of a system will meet service level agreements and also measures the behavior of the system with increasing load (e.g. number of parallel users and/or numbers of transactions to determine what load can be handled by the system). f. User Acceptance Test: Testing conducted by the user or customer to determine whether or not a system satisfies the defined user acceptance criteria in an isolated environment.	MAXIMUS provides segregated environments for each testing process as required in the RFP. MAXIMUS maintains separate environments for testing in all of the states in which they have contracts, so we have experience in maintaining multiple environments and moving builds through each environment prior to production implementation. For further details on our approach for conducting the different types of required for the project, refer to each individual subsection within this section.
TEST03	The Contractor must identify and resolve interdependencies that restrict or impede required testing of the Contractor's solution, other enterprise modules, or module components from performing required testing. Unless otherwise identified by the State strategies to resolve interdependencies must be reviewed and approved by the State prior to implementing the resolution strategy.	MAXIMUS identifies and resolves interdependencies that restrict or impede required testing of the solution, other enterprise modules, or module components from other required testing. The State will approve all resolutions.
TEST04	The Contractor shall perform testing and present the results for each of the following test levels: Performance Test results, System Test results, Parallel Test results, Regression Test results, Integration Test results. Test results shall be traced to the use case/user story and design documentation being tested.	MAXIMUS performs testing and produces test results for performance testing, system testing, parallel testing, integration testing. JAMA Contour is used to trace the testing use case back to the design document and requirement being tested.

ID	Testing Requirement	MAXIMUS Summarized Response
TEST05	"The Contractor shall provide sufficient environments and resources for the following: a. Synchronize the software and the data from the production environment and testing and impact analysis environment at a minimum on a quarterly basis or at the discretion of the Department. b. Synchronize the software and the data from the production environment and training environment following software deployments. c. Provide a fully functioning online test environment, which includes batch and online programs, files, and supporting systems. d. Provide technical and functional support to create and analyze ""what-if"" scenarios and compare results between scenarios in the impact analysis environment. Provide an analysis of outcomes in impact analysis environment and another environment, such as production or test. e. Provide State, Contractor, and IV&V staff a minimum of read-only access to all environments and tools. f. Provide sufficient resources to support the execution of automated regression testing. h. Provide comparative analysis support of regression testing results. i. Conduct testing of approved system configuration changes, corrections or enhancements or before implementation. j. Allow Department resources and contractors designated by the Department to create and edit appropriate data to support testing efforts, including provider, member, and reference data."	MAXIMUS provides sufficient environment and resources to: a. Synchronize software and data from production for testing at least quarterly. b. Synchronize software and data for training purposes c. Provide a fully functioning online test system including the running of batch and online programs, files and supporting systems d. To provide functional and technical support to do impact analyses e. To provide State, contractor, and IV&V staff read access to all environments and tools f. Provide resources for automated regression testing g. Provide analysis of regression testing results h. Conduct testing of system configuration changes and enhancements i. Allow Department resources and contractors to create and edit appropriate data to support testing efforts MAXIMUS already provides these environments in other states, and so we are well positioned to provide this same functionality in Montana and participating states.
TEST06	"The Contractor shall ensure, in order to release code to UAT or production, it must meet the minimum acceptable defect levels: • Critical: 100% have been resolved. • High: 100% have been resolved."	MAXIMUS releases code to UAT or production only when all critical and high defects have been resolved.
TEST07	The Contractor shall plan and execute testing for all inbound and outbound interfaces, ensure accurate and secure data transmission between the solution and the ESB and coordinate with external entities as appropriate.	MAXIMUS plans and executes testing for all inbound and outbound interfaces to verify that data between the solution, the ESB, and the external entities is being sent and received appropriately. MAXIMUS has similar interfaces in other states and is experienced in reviewing similar files as part of testing. Refer to *Section 3.10.2.6.3 – User Acceptance Testing* for more information.
TEST08	The Department plans to perform UAT on all software releases as part of the contract. The Contractor's approach to establishing testing environments should not impact the Department's ability to conduct continuous UAT in a separate, dedicated environment.	MAXIMUS provides the Department a separate and dedicated environment to perform UAT continuously. Refer to *Section 3.10.2.6.3–User Acceptance Testing* for more information.
TEST09	The Contractor shall facilitate UAT as follows: a. Provide test cases and scripts from previous test levels. b. Assist the Department in developing UAT test cases. c. Provide a dedicated UAT environment to the Department and maintain the environment as needed to support continuous UAT throughout design, configure/build and testing. d. Refresh data, execute processes, and migrate releases or code fixes as requested or on an agreed-upon schedule. e. Provide test data. f. Provide a mechanism for the Department to enter defects into the online defect-tracking tool.	MAXIMUS facilitates UAT by: a. Providing test cases and scripts from previous testing b. Assisting the Department in developing UAT test cases c. Providing a dedicated UAT environment to the Department for continuous testing d. Refreshing data, executing processes, and migrating code fixes as requested e. Providing test data f. Allowing the Department to work with MAXIMUS staff to enter defects into JIRA Refer to *Section 3.10.2.6.3–User Acceptance Testing* for further details on the types of support we provide to the Department during UAT.

ID	Testing Requirement	MAXIMUS Summarized Response
TEST10	The Contractor shall provide Department resources or their designee access to test cases, test results and defect tracking via online tools. The Department reserves the right to inspect artifacts and results at any time.	MAXIMUS provides the Department with test cases, tests results, and JIRA. MAXIMUS works with the Department to review testing artifacts as requested.
TEST11	The Department reserves the right to conduct independent testing of the solution at any time. The Contractor must cooperate with the Department or its designee, and provide environments, data, and technical support for independent testing.	MAXIMUS works directly with the Department to provide environments, data, and support for all testing. MAXIMUS will cooperate with the Department to provide environments, data, and technical support for independent testing, if required.
TEST12	The Contractor's testing environments shall be sized to be capable of mirroring the production System in its infrastructure, files, databases, processing, and reporting.	MAXIMUS provides environments that are capable of mirroring the production system and its entire infrastructure. This functionality exists for all MAXIMUS instances. Both our System Testing and UAT test environments are fully loaded with a complete set of conversion data from the source MMIS system.
TEST13	The Contractor shall work proactively with the State's designated testing resources to review all test results and provide the necessary system and functional information to create verification procedures and user acceptance test cases.	MAXIMUS works closely with the State to review all test results and to support the UAT effort in its entirety. MAXIMUS testers are available to work side by side with State testing resources to validate UAT test cases.
TEST14	The Contractor shall coordinate with the Department and specific module component vendors to conduct integration testing.	MAXIMUS works with the State and their external vendors to conduct integration testing of the Montana Provider Services module and all external systems. MAXIMUS testers are available to work side by side with State and external vendors to confirm that we complete thorough integration testing. Refer to *Section 3.10.2.6.3–User Acceptance Testing* for more information.
TEST19	The Contractor shall develop test criteria and algorithms for expected outcomes prior to production of reports.	MAXIMUS writes and delivers test criteria and algorithms for expected outcomes prior to producing reports. We provide this information to the State prior to testing so the State can verify reports.
TEST20	The Contractor shall ensure that the Project Work Plan allocates sufficient time to the State's user acceptance testing activities relative to the detailed scope of work, requirements and gaps, the number of manually executed test cases, and the complexity of module integration. The Contractor' will be responsible for extended user acceptance testing if the proposed testing duration is not sufficient for the State to validate the module.	MAXIMUS builds a project work plan that includes sufficient time for the State to complete a thorough user acceptance test of the system. The project work plan allows for six weeks of UAT, starting with small pieces of the system and working to the point of completing a full integration test and parallel testing. Based on our experience in implementing Provider Services modular systems, we have already factored this additional time into our project work plan.

3.10.2.7 Training

3.10.2.7 Training

The Contractor must provide training to designated MPATH team members, DPHHS training staff and other staff responsible for training to achieve an understanding of the new system, services, or release. The training will incorporate a train-the-trainer model so that participants can, in turn, provide training to additional users. Users must become proficient in using and viewing information in the Contractor's solution in order to ensure effective and efficient business operations and service delivery. The Offeror must describe their approach to meet each of the detailed training requirements defined in Attachment F, Requirements Matrix.

For MAXIMUS, training is not just a contractual obligation, but a way to achieve an operational standard that ensures employee readiness to serve Providers in ways that help the State achieve its goals for Medicaid Provider enrollment and revalidation. We will establish a robust training program to prepare trainers who will then train staff. The trainers will be prepared to train staff to conduct screening and enrollment activities accurately and consistently and to use the system effectively in all aspects of their job duties. Our training program will also include training sessions for designated agency staff. In addition to the initial training, we will provide additional training when there are major enhancements to the system.

Our training plan for the Provider Services Module is customized to meet the training goals of DPHHS. Training will be primarily instructor-led and will be comprehensive in content to ensure all project staff members are fully prepared to utilize all features of the Provider Services system.

In addition to traditional, in-person training, MAXIMUS will develop, publish, implement, and maintain online searchable and printable end user manuals. These will be submitted to the State within agreed upon timeframes to allow adequate time for review and revisions. Additional training materials to be developed include job aids, computer-based training, user guides, and publications according to State-approved content, format, and schedules.

We will leverage the considerable experience and best practices established by our training partner, Microassist of Austin, Texas. Established in 1988, Microassist began as a technical training company to assist organizations in training their employees on how to use computers. Over the years, Microassist has expanded the training it offers to over 200 end-user application and high-end technical and security courses; in addition, Microassist serves organizations with training development and delivery in varied capacities, to include classroom, eLearning, or blended methods.

In 1992, Microassist was awarded its first contract with the State of Texas for IT instructor-led training. Three years later, Microassist began using tools, such as the JAWS screen reader and ZoomText Magnifier, to teach end-user application software to the visually impaired.

Microassist has:

- Been selected by the Texas Department of Information Resources (DIR) for their training contracts for over twenty-five consecutive years, and is one of the largest current training vendors for the State of Texas.
- Created custom learning solutions used by State of Texas agencies, Fortune 100 enterprises, and small organizations, and used by a significant portion of their clients.
- Become one of the leaders for creating accessible TAC 206- and 213-compliant eLearning applications for State of Texas agencies, and has provided groundbreaking presentations on the topic.
- Created enterprise-scale, secure web applications, and training that are used by 20,000 users to search and manage more than 20 million database records.
- Provided web application maintenance and support for eight large agencies.
- Installed and maintained learning management systems.

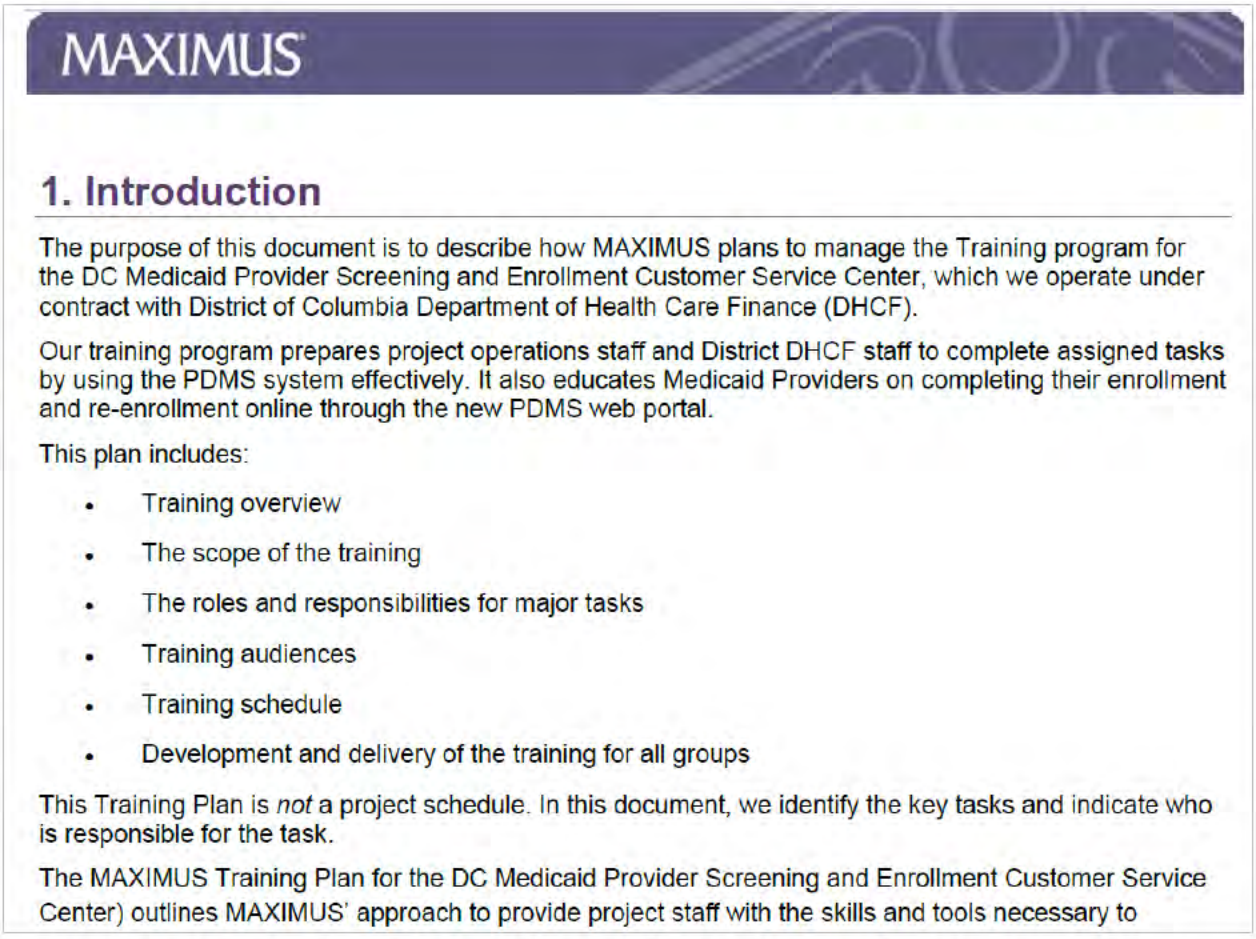
- Extensive experience in business process, workflow analysis, and implementation, and how this relates back to providing managed training services.

As part of the MAXIMUS team, Microassist will perform a crosswalk comparing existing MAXIMUS communication, training, and publication documents with the requirements for this contract. A gap analysis will show where current training materials require augmentation (for example, an awareness of regulations may be consistent, but how to apply those regulations in the new system may require a revision in existing material). Microassist will propose changes to address any differences between existing documentation and new requirements.

Training Plan

Our Training Plan for the State will be built on the foundation we already have in place in other Provider Management projects. Training will be primarily instructor-led and will be comprehensive in content to ensure all users are fully prepared to operate the MAXIMUS Provider Services solution. We will deliver and maintain the Training Plan according to the schedule in the approved PWP.

The Training Plan guides the tasks and activities involved in our training approach. This required deliverable will be submitted to the Department well in advance of the Operational Readiness phase and will outline all of the tasks and planning activities required to implement the Provider Services solution. Our submitted Training Plan will contain the required content as specified in requirement DOC27, as well as the required user documentation required by DOC07 as specified in Attachment F. We have produced detailed Training Plans in all previous Provider Services implementations. *Exhibit 3.10.2.7-1: Sample Implementation Plan* shows a snippet from the Training Plan we submitted for the District of Columbia.



MAXIMUS

1. Introduction

The purpose of this document is to describe how MAXIMUS plans to manage the Training program for the DC Medicaid Provider Screening and Enrollment Customer Service Center, which we operate under contract with District of Columbia Department of Health Care Finance (DHCF).

Our training program prepares project operations staff and District DHCF staff to complete assigned tasks by using the PDMS system effectively. It also educates Medicaid Providers on completing their enrollment and re-enrollment online through the new PDMS web portal.

This plan includes:

- Training overview
- The scope of the training
- The roles and responsibilities for major tasks
- Training audiences
- Training schedule
- Development and delivery of the training for all groups

This Training Plan is *not* a project schedule. In this document, we identify the key tasks and indicate who is responsible for the task.

The MAXIMUS Training Plan for the DC Medicaid Provider Screening and Enrollment Customer Service Center) outlines MAXIMUS' approach to provide project staff with the skills and tools necessary to

Exhibit 3.10.2.7-1: Sample Training Plan. *MAXIMUS submits a Training Plan to DPHHS that outlines our approach for successfully training applicable users or Trainers on the Provider Services solution. We tailor our previously created planning documents to meet the requirements of each State.*

The Training team follows a standard instructional design methodology combined with a project-specific development process to implement curriculum targeted at producing job-ready personnel. Our collaborative process allows for the development of effective, efficient training by having repeatable processes, well-defined deliverables, and suitable measurements for evaluation and improvement. The training plan describes our strategy and approach for how all users and system maintenance staff are trained to operate our solution. The purpose of the training plan is to assist the training team in analyzing, designing, developing, implementing and evaluating the state's training needs for the Provider Services module.

Exhibit 3.10.2.7-2: Training Plan shows the sections we will include in the Training Plan.

Training Plan Section	Content Description
Stakeholder Identification	The training plan identifies the trainers to be trained in the operation of our solution.
Types of Training	This section describes the types of training to be provided for each role of all stakeholders and the method of training

Training Plan Section	Content Description
Training Location	This section lists the location of the training that will be conducted on site by MAXIMUS
UAT Staff Training	This section contains a description of training that may be needed for agency staff for any user acceptance software tools to be used
Training Schedule	This section contains the training schedule, meeting topics, and materials to be used for all training

Exhibit 3.10.2.7-2: Training Plan. *MAXIMUS will deliver a training plan to DPHHS that will document our approach for the training of all required users.*

We will coordinate with DPHHS to develop a training plan with the format, content, and media approved by the state. The training plan includes strategies for training audience groups for the train-the-training delivery format. The completed training plan will be submitted for state approval as scheduled in the PWP.

The plan, at a minimum, addresses the training approach for the train-the-trainer delivery method, course objectives, and desired outcomes. In addition, Microassist's instructional designers will create a training needs analysis, assessing the target audience and their knowledge and skills, and make recommendations on the delivery approach (instructor-led, elearning, video, blended or another solution) based on this analysis. Microassist summarizes the proposed training materials required in the task analysis, and a lesson plan is created for instructor-led delivery and a design plan will be created for online modules. The approach for maintaining training documentation and related resources is discussed, as well as any necessary training for system updates. A feedback mechanism is also discussed through training session evaluations, surveys and other methods, so that the training experience may be improved.

This training plan is updated frequently, as needed by any changing state requirements. Train-the-trainer courses include teach-backs and other components to help instructors convey information. These elements may be identified in the training plan, with knowledge, experience, skills, and abilities identified for each topic.

Train the Trainer

We will assign a team of Microsassist and MAXIMUS specialists to design and deliver training. The team includes instructional designers, facilitators, instructors, and instructor assistants.

These roles are described in more detail below:

- Instructional Designer – creates curriculum in conjunction with subject matter experts and facilitators
- Facilitator – learns system, works with instructional designers to develop curriculum, absorbs material, teaches instructors and instructor assistants, audits classes, instructor reinforcement and clarification
- Instructor – provides classroom management and training delivery for the new trainers
- Instructor Assistant – assists instructors in delivering trainer content, distributing job aids and handouts, taking attendance, notating "parking lot" items, and other classroom activities

Typically, these teams work in tandem to absorb the content, create curriculum, teach to trainers, and provide an environment in which trainers can learn how best to deliver content to end users.

Educational Materials

MAXIMUS will coordinate with the State to produce and maintain accurate and comprehensive educational materials, including but not limited to, classroom courses, job aids, computer-based training modules, user guides, publications and other materials according to State-approved content, format, and schedules.

For all course material, Microassist strictly adheres to instructional design principles. Microassist's training development process starts with determining business or learning objectives and continues with a task analysis for accomplishing each objective. See *Exhibit 3.10.2.7-3* for the process Microassist uses for eLearning (computer-based training module) development. Microassist uses a similar process for instructor-led, blended, and webinar formats.

Exhibit 3.10.2.7-3: *Microassist Typical Training Development Process for eLearning. Microassist follows a detailed approach to all aspects of eLearning*

Microassist's instructional designers work closely with subject matter experts and other stakeholders to identify goals and learning objectives for each respective suite of training sessions. We then create a high-level overview or task analysis that describes the approach.

Course Materials

Microassist consults with stakeholders and develops the appropriate supporting curriculum. This can include instructor manuals, trainer guides, student manuals, job aids, and other material. Depending on the course, it may include presentation slides.

Formal curriculum serves multiple purposes. It sets out the material that the instructor needs to teach and provides trainers and users with reference material that they can refer to after the class has been completed. Just as importantly, consistent and well-developed curriculum helps ensure that multiple instructors teach the course the same way, ensuring that the trainers (and through them, users) will receive equivalent instruction regardless of when, where, or with whom they take the course.

Instructor-led course development follows a review and revision process similar to eLearning. Opportunity is given at each stage of development for stakeholders to review and revise the curriculum. Changes and suggestion are much more effectively incorporated when presented earlier in the process.

As part of the Option B services, we will provide web-based video instruction. The following steps are most relevant for web-hosted video training and demonstration.

Storyboards

Storyboards provide more detail and are the visual and textual descriptions of what each video scene will look like. Storyboards are usually developed in a tool such as Word or PowerPoint. The storyboard contains screen shots as example images with an accompanying narration script. The storyboard outlines each action that occurs in the elearning and serves as the reference for both Microassist and the state.

Perhaps more than any other stage, the storyboard requires a focused review process. This is the opportunity for the SME and other stakeholders to scrutinize and change images, screenshots, and particular word choices, both on screen and in narration. Agreeing on the storyboards is an essential part of the process, as it is much easier to make adjustments to visuals or narrations before production and recordings. While some changes can be made during the post-production phase, it is usually a challenging (and sometimes costly) endeavor.

Production

Once the storyboards pass review, Microassist begins the production process. This process includes recording the narrations, filming visuals, capturing screen recordings, and combining the elements, including additional graphics to create a rough cut of the video. This is where the module comes to life.

The State will review the video’s first draft to ensure both the narration and action on the screen accurately represent the process for the user. Upon confirmation, Microassist proceeds with finishing the full video. The finished video is then placed in a testing environment, where it can be reviewed and tested by the State. The result of this collaborative process is a video that is both technically accurate and instructionally effective, while meeting scope, budget, and timeline.

Review Points for Web-Based Video

The State and MAXIMUS, with Microassist, mutually agree upon a development schedule that supports the state's desired delivery date. We see this project as highly collaborative requiring frequent and clear communication. At the same time, it is important that we both manage our organizations from a time standpoint to ensure we meet our deliverable deadlines this project.

Accessibility

Because online video is delivered in a web-based format, it must meet the accessibility requirements of State of Montana and WCAG 2.0 AA. Microassist designs videos that bear accessibility in mind from the beginning, ensuring, for example, that colors have sufficient contrast so that users who are colorblind can perceive the material; that a screen reader will be able to access all of the material; that videos are captioned; and that all screen content can be reached using the keyboard only. Videos are closed captioned, and are provided with a transcript, and may include appropriate audio description (adding additional commentary that describes visual content to people who are blind, such as "pot of boiling water" when the video pans to a pot on the stove, for example).

By addressing accessibility early and continuously, Microassist avoids the timely and costly process of remediating courses after development.

Training Requirements

The following table includes Attachment F Training Requirements, our summarized response to each requirement, and the section(s) in our proposal in which we provide our detailed response.

ID	Training Requirement	MAXIMUS Summarized Response
TRN01	The Contractor shall provide technical training to agency project resources and designated contractors to develop an understanding of how to monitor the system using available tools and dashboards while leveraging technical and functional documentation and/or reports.	The MAXIMUS Provider Services solution contains robust tools and dashboard for agency project resources and designated contractors to monitor the system. Our training curriculum includes technical training in understanding how to monitor the system through the accurate and complete use of these online tools. In addition, technical and functional documentation serve as additional resources to ensure maximum use of all system monitoring features.
TRN04	The Contractor shall update training materials when changes occur.	As part of our standard project management approach, changes to the system require updates to training materials. Our business analysts are tasked with making those updates to ensure training materials are kept current.
TRN05	The Contractor shall collaborate with the agency to finalize a training schedule.	A significant step in ensuring system implementation readiness is developing the training schedule so that training does not occur too soon before system rollout. We collaborate with the agency to develop and maintain a training schedule for all users.
TRN06	The Contractor shall maintain and update the training environment with training data to use during user training.	Hands-on training is key to system use readiness. We will maintain and update the training environment with training data to use during user training. This environment is online and accessible from any authorized computer.
TRN07	The Contractor shall provide train-the-trainer sessions for Agency resources or designated agency resources and other staff responsible for training.	MAXIMUS is experienced in delivering train-the-trainer sessions and we look forward to providing these sessions for agency resources or other staff responsible for training.
TRN08	The Contractor shall utilize a variety of delivery methods to best meet the training objectives. Examples include online self-paced training presentations, in-person classroom setting, written material, and demonstrations.	Adult learners grasp concepts and absorb new information differently and a variety of tools must be made available to support any type of learning. We use a variety of delivery methods to best meet the training objectives. We will provide in-person training to the trainers and will make written user guides available on the solution website.
TRN09	The Contractor must provide training necessary to support new functionality and/or major software releases that materially change the user interaction.	As the system evolves, so does the training necessary for the users to fully take advantage of all system features. In the event of a major software release that materially changes the user interaction, we will provide the necessary training to the trainers.
TRN10	The Contractor shall provide training to Agency staff and other designated module vendors on the overall data management strategy and investigating data or process issues related to module integration.	Module integration is key to a successful enterprise and a requirement for CMS certification. We will work closely with Agency staff and other module vendors to ensure a common understanding of the overall data management strategy and other data or process issues related to module integration.

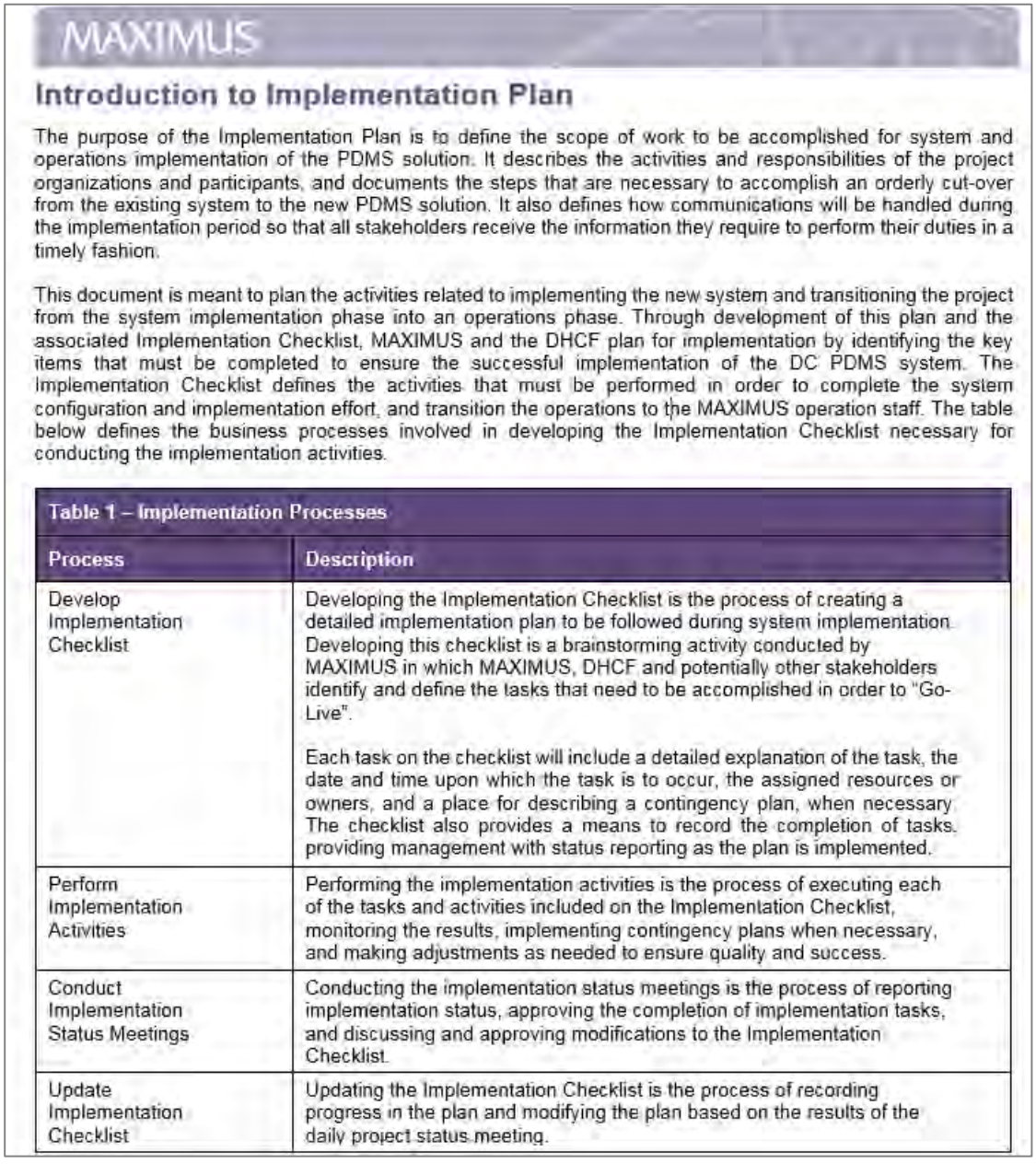
ID	Training Requirement	MAXIMUS Summarized Response
TRN11	The Contractor shall develop and maintain electronic training guides and materials to support the Train the Trainer instruction.	Electronic training guides are beneficial for ease of use and the ability to search for keywords. In the event users save versions offline, we develop and maintain electronic training guides with versioning so the user can be certain the most recent version is being accessed. The newest versions will be distributed prior to Train the Trainer sessions when there are significant system enhancements.
TRN13	The Contractor shall provide training and support to State staff and individuals designated by the State (e.g., IV&V, QA/QC vendor), on the use of DDI tools provided by the contractor. This may include traceability tools, document repositories and testing tools.	MAXIMUS uses an industry standard suite of tools and methods to facilitate Project Management. However, not all stakeholders will have experience with these tools and there may be variations MAXIMUS uses. Therefore, in addition to user training on the MAXIMUS Provider Services solution, we will prepare and deliver training on our project management tools, including SharePoint (document repository), Microsoft Office, JIRA (issue and defect tracker) and JAMA Contour (RTM).
TRN14	The Contractor shall provide training on the system for UAT testers. The Contractor shall provide updated User and System Documentation to UAT testers to support the UAT effort.	Accurate testing is essential to a successful UAT effort and is a significant step in system enhancement rollouts. As new functionality is developed and tested, we will schedule and provide training on the new functionality to all UAT testers.
TRN15	The Contractor shall conduct training for identified system/component users on the system relative to their use initially and upon updated functionality prior to the initial production deployment and within 45 days of each major release into the Production environment	Our comprehensive initial delivery includes training for all user roles and functionalities. System enhancements may touch the functionality of one or all roles within the system Within 45 days of each major release, we will conduct training on the updated functionality. We address this requirement in our response to Option B Provider Services.
TRN16	The Contractor's solution shall provide web-based video instruction.	Microassist shall provide web-based video. The state may opt to have video integrated with an eLearning solution, or blended with instructor-led training delivery. The steps of storyboarding, state reviews, and production are outlined above in this section.
TRN17	The Contractor shall develop and provide as necessary, training for the Provider Community. The training must be structured to address the Contractor's solution functionality for enrollment, maintenance, and revalidation.	MAXIMUS has vast experience in training Medicaid providers. We have developed materials and delivered training to the provider user community specifically on our solution in both our Nebraska and District of Columbia operations. The training addresses provider data entry points, navigation and application submission functions for enrollment, maintenance, and revalidation. We address this requirement in our response to Option B Provider Services.

3.10.2.8 Implementation and Acceptance

> 3.10.2.8 Implementation and Acceptance
>
> Prior to implementation, the Contractor must demonstrate readiness to implement the solution and to provide operational support and maintenance of the proposed solution(s) for the remainder of the Contract term. The Contractor is responsible for managing the end-to-end implementation of the proposed solution. DPHHS expects the Contractor to help formulate strategies for a successful transition.
>
> DPHHS must formally approve the implementation of the solution based on pre-defined acceptance criteria. DPHHS's acceptance of the solution will initiate the Operations, Maintenance and Configuration phase of the contract. The Offeror must describe their approach to meet each of the implementation and acceptance requirements defined in Attachment F, Requirements Matrix.

MAXIMUS will demonstrate to the Department that the Provider Services solution is ready for implementation. We understand our responsibility for managing the initial implementation of the system as well as all subsequent releases into the production environment. MAXIMUS will work with the Department during the early phases of the project to define fully, and to agree upon the acceptance criteria that will be the guideline to determine the production-readiness of the system. MAXIMUS understands that the Department's acceptance of the production system will transition the project from the DDI phase into the Operations, Maintenance, and Configuration phase of the project.

The tasks and activities involved in our implementation approach will be guidance for the project's Module Implementation Plan. This required deliverable will be submitted to the Department well in advance of the Operational Readiness phase and will outline the tasks and planning activities required to implement the Provider Services solution. Our submitted Module Implementation Plan will contain the required content as specified in requirement DOC13 as specified in Attachment F. We have produced detailed Implementation Plans in all three of our previous Provider Services implementations. *Exhibit 3.10.2.8-1: Sample Implementation Plan* shows a snippet from the Implementation Plan we submitted for the District of Columbia.



MAXIMUS

Introduction to Implementation Plan

The purpose of the Implementation Plan is to define the scope of work to be accomplished for system and operations implementation of the PDMS solution. It describes the activities and responsibilities of the project organizations and participants, and documents the steps that are necessary to accomplish an orderly cut-over from the existing system to the new PDMS solution. It also defines how communications will be handled during the implementation period so that all stakeholders receive the information they require to perform their duties in a timely fashion.

This document is meant to plan the activities related to implementing the new system and transitioning the project from the system implementation phase into an operations phase. Through development of this plan and the associated Implementation Checklist, MAXIMUS and the DHCF plan for implementation by identifying the key items that must be completed to ensure the successful implementation of the DC PDMS system. The Implementation Checklist defines the activities that must be performed in order to complete the system configuration and implementation effort, and transition the operations to the MAXIMUS operation staff. The table below defines the business processes involved in developing the Implementation Checklist necessary for conducting the implementation activities.

Table 1 – Implementation Processes

Process	Description
Develop Implementation Checklist	Developing the Implementation Checklist is the process of creating a detailed implementation plan to be followed during system implementation. Developing this checklist is a brainstorming activity conducted by MAXIMUS in which MAXIMUS, DHCF and potentially other stakeholders identify and define the tasks that need to be accomplished in order to "Go-Live". Each task on the checklist will include a detailed explanation of the task, the date and time upon which the task is to occur, the assigned resources or owners, and a place for describing a contingency plan, when necessary. The checklist also provides a means to record the completion of tasks, providing management with status reporting as the plan is implemented.
Perform Implementation Activities	Performing the implementation activities is the process of executing each of the tasks and activities included on the Implementation Checklist, monitoring the results, implementing contingency plans when necessary, and making adjustments as needed to ensure quality and success.
Conduct Implementation Status Meetings	Conducting the implementation status meetings is the process of reporting implementation status, approving the completion of implementation tasks, and discussing and approving modifications to the Implementation Checklist.
Update Implementation Checklist	Updating the Implementation Checklist is the process of recording progress in the plan and modifying the plan based on the results of the daily project status meeting.

Exhibit 3.10.2.8-1: Sample Implementation Plan. *MAXIMUS submits a Module Implementation Plan to DPHHS, which outlines our approach for successfully implementing the Provider Services solution. We tailor our previously created planning documents to meet the requirements of each State.*

The Module Implementation Plan will indicate the order in which the system will be built, tested, and integrated for further testing. It also indicates how builds can be rolled back in the event there are critical issues that need to be pulled out of the integrated system. The plan identifies all the steps toward receiving a go/no-go decision from the Department, including Roles and Responsibilities for all stakeholders.

In this subsection of our proposal, we provide the details for how we approach the implementation tasks for the project and how those tasks will lead to a successful implementation of the system. Our recommended approach includes two primary tasks that, based on our experience, will lead to a successful implementation of our Provider Services system. The two tasks are Operational Readiness and Implementation.

3.10.2.8.1 Operational Readiness

During the Operational Readiness Phase, MAXIMUS performs all required tasks to ready the system for implementation and transition to production. These tasks include execution of the Disaster Recovery Testing and Security Scan. *Exhibit 3.10.2.8-2: Operational Readiness* illustrates the primary activities that need to be completed as we transition from User Acceptance Testing into Operational Readiness.

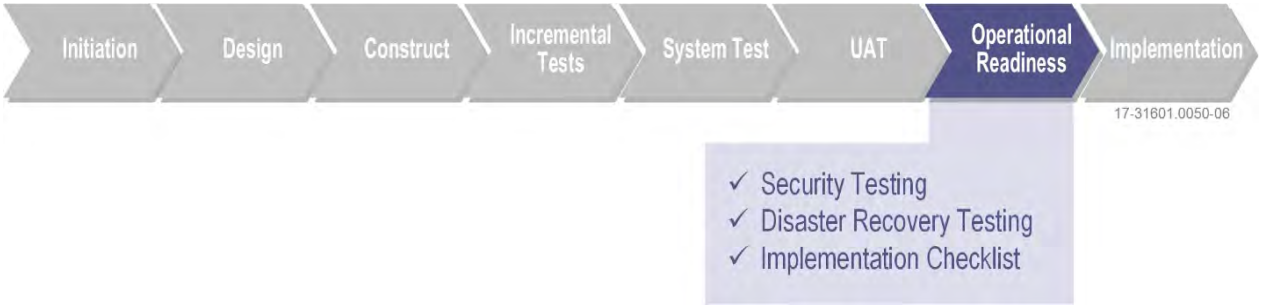


Exhibit 3.10.2.8-2: Operational Readiness. *MAXIMUS starts Operational Readiness preparation and assessment well before implementation activities begin.*

MAXIMUS understands the importance of Day One readiness and uses operational readiness as the formal method to review the results of acceptance testing along with the results of other tasks such as training and infrastructure implementation to determine if the system and business operations as a whole are ready to move to production. Operational readiness review is the final task required for the system to be approved and moved to production. It is a conglomeration of all preparation tasks and serves as a final check to ensure that the application, system configurations, user setups, and operational readiness are all complete. It also ensures that the organization is ready for production including the successful training of the staff to use the new system.

The planning documentation that we produce leading up to Go-Live will be detailed and well-scripted, and will clearly define the individual persons responsible for each of the Go-Live tasks. We shape these plans based on our recent and practical experience in implementing Provider Services solutions for other states. From a system perspective, this means that we need to have planned for a specific set of tasks related to both the Provider Services system deployment to the production environment as well as the deployment of the MMIS system changes that will need to be in place once the system is in production.

MAXIMUS confirms operational readiness by developing an implementation checklist that identifies all the activities that must be done prior to when a go live decision can be rendered. Testing must be completed, defects must be remediated, and security protection and disaster recovery capability must be confirmed. Users must be trained, providers must be notified, and the production data center, database, and applications must be deployed. The Operational Readiness (OR) Plan defines these tasks, establishes target completion dates, and defines responsibility for each of the categories of OR tasks. The Implementation Checklist takes the plan to a much lower and more actionable level of detail. *Exhibit 3.10.2.8-3: Implementation Checklist* a small section of the checklist we used for our recent implementation for the District of Columbia.

MAXIMUS Operations Team
Implementation Checklist

Implementation Lead: **Juli Mattfeldt**
Contact: [redacted]
JuliMattfeldt@maximus.com

Item	Category	Task Description	Responsibl	Status	Target D	Cpt Dt	Comments & Questions
14	**Conversion**	Conduct the conversion data load	Diwakar Emani	Not Started	1/4/2017		
15		Run the conversion verification reports	Diwakar Emani	Not Started	1/5/2017		
16		Review and verify the conversion reports	John Walz	Not Started	1/5/2017		
17		Send the conversion reports to DHCF & Xerox	John Walz	Not Started	1/6/2017		
18		Use the DC PDMS UI to verify conversion load of data, reference tables and security	Jon Puckett	Not Started	1/6/2017		
19	**Operation Readiness**	Create the final production build of the program code and migrate to the the production environment.	Diwakar Emani	Not Started	1/6/2017		
20		Perform smoke testing in Production environment after deployment of final code.	Jon Puckett	Not Started	1/6/2017		Can we build scripts that we use to verify that reference tables, etc are good? Add a back up before the smoke test and a restore after the back up.
21		Enable access to the production system	Diwakar Emani	Not Started	1/9/2017		
28		Load and verify the Production Security Roles	Diwakar Emani	Not Started	1/3/2017		8/31/2016 - Is there an inquiry role.
		Switch the OnBase server to point to production instead of UAT	Diwakar Emani	Not Started	1/7/2017		

Exhibit 3.10.2.8-3: Implementation Checklist. *MAXIMUS creates an Implementation Checklist during Operational Readiness and facilitates weekly meetings with required Stakeholders to track tasks to completion.*

Weekly meetings are held to update the status of the checklist items, monitor progress against the schedule, address concerns and resolve issues. The checklist contains different tasks for the Operation team, DPHHS, and MAXIMUS. Inputs to the OR assessment include:

- System Test Results
- UAT Test Results
- Data Conversion Results
- Interface Test Results
- Security Test Results
- Disaster Recovery Test Results
- User and Procedural Documentation Delivery Schedule

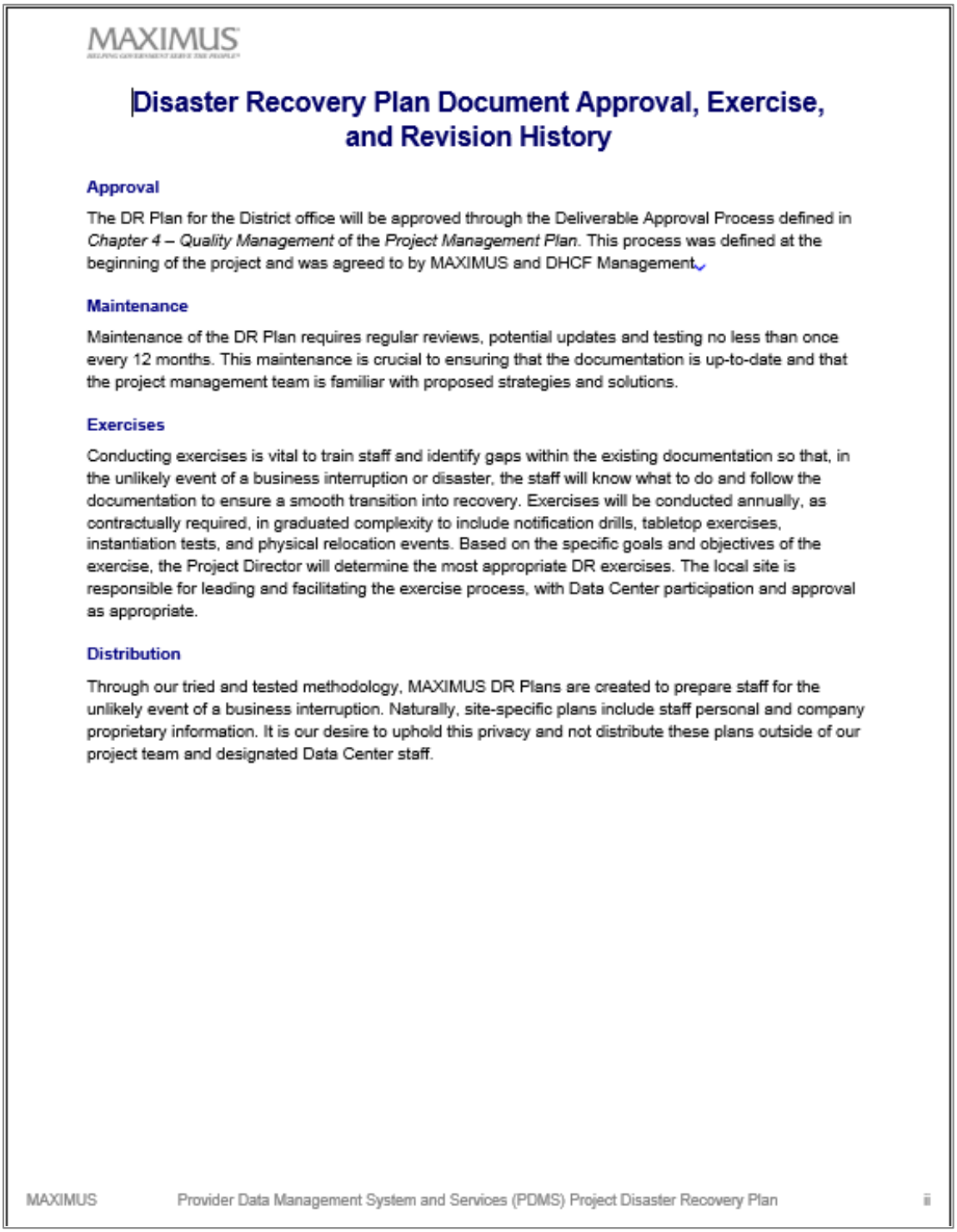
The exit criteria for proceeding to implementation must include an assessment of any remaining defects as a means to determine whether the system is ready for implementation. Outcomes desired from UAT must be clearly defined and measured to satisfy DPHHS' expectations are met. Exit criteria must be defined in advance so that all project participants understand what is required to approve the system for implementation. MAXIMUS commits to completing all high and critical defects prior to implementation.

During OR assessment the Operation Support Team role assignments are confirmed and approved by DPHHS. Communications mechanisms, production schedules, and the responsibilities of MAXIMUS and DPHHS staff are also defined.

In three prior implementations, MAXIMUS used Operational Readiness as the vehicle to efficiently transition from the testing phases to full implementation. A two-week Operational Readiness test simulates production operations in a carefully orchestrated series of tests that verify the users and the system are ready to process production provider applications and reenrollments. Our experience has proven that the two most critical aspects of implementation are data conversion and the readiness of the MMIS interface. Our focus on these aspects of the system from the completion of the Project Initiation Phase continues through all DDI phases, including implementation.

Operational readiness is the phase of the project that the State uses to review the results of all implementation activities and determine if the system is ready to "Go Live." Operational Readiness Testing simulates production and is the final verification that the system is ready and the operation staff are prepared for production.

Besides completing testing of the system for Operational Readiness, during the Operational Readiness phase, MAXIMUS also completes the Business Continuity and Disaster Recovery Plan. This plan documents the strategies and capabilities to safeguard and resume business functions within pre-determined timeframes established in the RFP. The Business Continuity and Disaster Recovery Plan integrates with and supports the business objectives of the State. *Exhibit 3.10.2.8-4: Sample Disaster Recovery Plan* is a snippet of the Disaster Recovery Plan that was delivered to the District of Columbia.



MAXIMUS

Disaster Recovery Plan Document Approval, Exercise, and Revision History

Approval

The DR Plan for the District office will be approved through the Deliverable Approval Process defined in *Chapter 4 – Quality Management* of the *Project Management Plan*. This process was defined at the beginning of the project and was agreed to by MAXIMUS and DHCF Management.

Maintenance

Maintenance of the DR Plan requires regular reviews, potential updates and testing no less than once every 12 months. This maintenance is crucial to ensuring that the documentation is up-to-date and that the project management team is familiar with proposed strategies and solutions.

Exercises

Conducting exercises is vital to train staff and identify gaps within the existing documentation so that, in the unlikely event of a business interruption or disaster, the staff will know what to do and follow the documentation to ensure a smooth transition into recovery. Exercises will be conducted annually, as contractually required, in graduated complexity to include notification drills, tabletop exercises, instantiation tests, and physical relocation events. Based on the specific goals and objectives of the exercise, the Project Director will determine the most appropriate DR exercises. The local site is responsible for leading and facilitating the exercise process, with Data Center participation and approval as appropriate.

Distribution

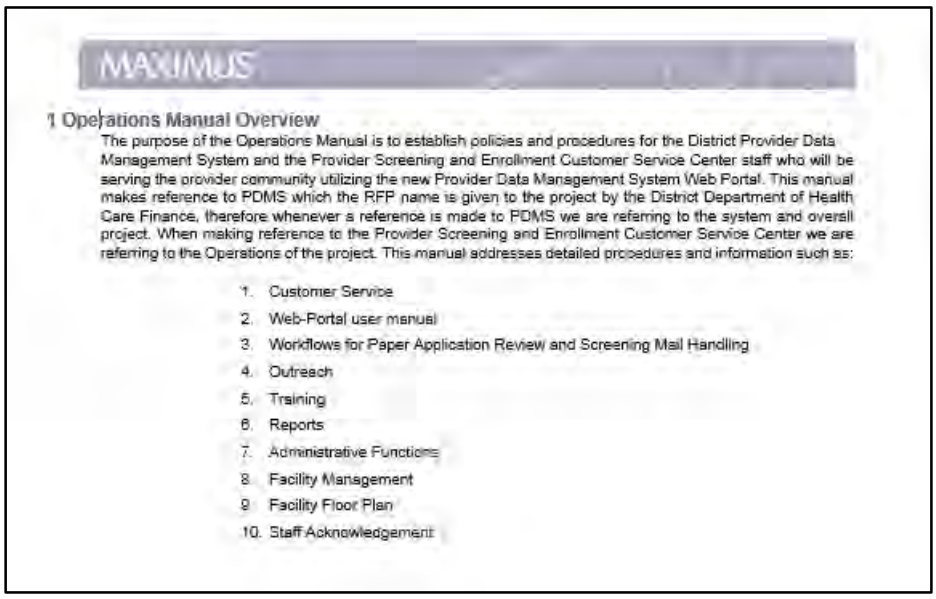
Through our tried and tested methodology, MAXIMUS DR Plans are created to prepare staff for the unlikely event of a business interruption. Naturally, site-specific plans include staff personal and company proprietary information. It is our desire to uphold this privacy and not distribute these plans outside of our project team and designated Data Center staff.

MAXIMUS Provider Data Management System and Services (PDMS) Project Disaster Recovery Plan ii

Exhibit 3.10.2.8-4: Sample Disaster Recovery Plan. *MAXIMUS creates a Business Continuity and Disaster Recovery Plan during Operational Readiness to validate the business continuity and disaster recovery site execution.*

It is also important to prepare Operations for the implementation and the work that will be occurring once the system is in production. To prepare the Operations Team for implementation, we develop an

Operations Manual to outline job functions, and how the system supports job functions. *Exhibit 3.10.2.8-5: Sample Operations Manual* is an excerpt from the operations manual that we developed for the District of Columbia.



MAXIMUS

1 Operations Manual Overview

The purpose of the Operations Manual is to establish policies and procedures for the District Provider Data Management System and the Provider Screening and Enrollment Customer Service Center staff who will be serving the provider community utilizing the new Provider Data Management System Web Portal. This manual makes reference to PDMS which the RFP name is given to the project by the District Department of Health Care Finance, therefore whenever a reference is made to PDMS we are referring to the system and overall project. When making reference to the Provider Screening and Enrollment Customer Service Center we are referring to the Operations of the project. This manual addresses detailed procedures and information such as:

1. Customer Service
2. Web-Portal user manual
3. Workflows for Paper Application Review and Screening Mail Handling
4. Outreach
5. Training
6. Reports
7. Administrative Functions
8. Facility Management
9. Facility Floor Plan
10. Staff Acknowledgement

Exhibit 3.10.2.8-5: Sample Operations Manual. *MAXIMUS creates an Operations Manual to prepare Operations staff for system implementation.*

Besides prepping Operations staff for post implementation work, it is important to develop documentation to be used by the business analysts and technical staff throughout Operations and Maintenance. As part of Operational Readiness, MAXIMUS develops an Operations, Maintenance, and Configuration Plan. This plan includes, but is not limited to:

- Technical Architecture/Hosting Operations
- Monitoring of daily operations performance
- Performance of routine maintenance
- Maintenance of user documentation
- On line help approach
- Change management approach
- Maintenance of system documentation
- Maintenance of training documentation
- Archiving requirements
- Roles, responsibilities and timelines for releases
- Reporting of SLAs

This plan defines for the State and MAXIMUS staff how operations procedures will be handled once the system is implemented in production. Having this plan aids in making sure all stakeholders are aware of how teams will interact during O&M. This makes communications clearer and supplements the plans built as part of the project management plan.