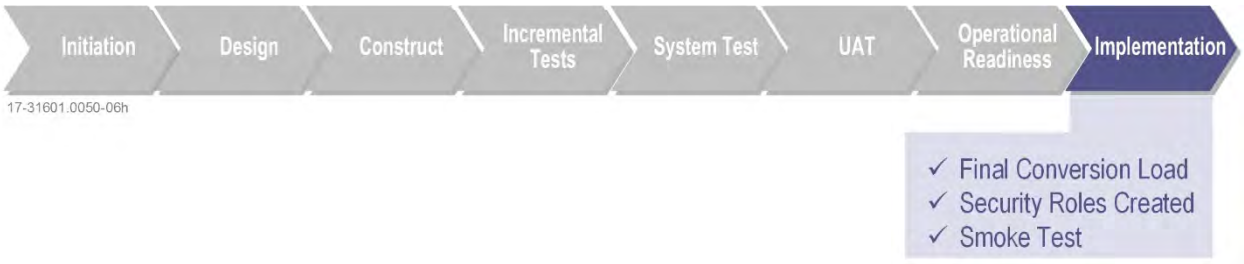
3.10.2.8.2Implementation



MAXIMUS will leverage our experience, expertise, and lessons learned from prior successful Provider Services system implementations, each of which required a full conversion of data from a legacy MMIS as well as the implementation of interfaces to the MMIS. MAXIMUS will lead the implementation activities and will be responsible for release management. Our team will implement changes and releases in each system environment, as appropriate, according to approved change control processes. MAXIMUS will assist with implementation preparations for system configuration files and data conversion programs as identified in the Implementation Plan and Data Conversion Plan. We will assist DPHHS in confirming that all integration services are in place and working properly so that the system configuration is ready to support integration with external systems, including the MMIS. We will closely monitor the new software performance and remediate any software defects promptly.

After the exit criteria have been met and the Department indicates the system is ready to "Go-Live," a flurry of activities occur over the final weeks prior to production implementation. Notifications are issued to providers to announce the new system. DPHHS and State web sites that contain instructions to Medicaid providers need to be updated with new instructional materials and links to the new Provider Services web portal.

Leading up to the implementation, we have learned that is it beneficial to attend, either in person or remotely, any weekly release planning meetings that the Department may be having with the MMIS vendor. The series of tasks required for the system implementation must be carefully coordinated between DPHHS, the MMIS vendor, and MAXIMUS. Using this set of procedures, and due to careful planning, we were able to successfully implement our major system releases in Nebraska and the District of Columbia over a weekend. This resulted in minimal impact to the Provider community, to the MMIS, and to DPHHS Provider Services staff. The conversion data extracts are taken from the source systems as close as possible to the go live date. This is to verify the data in the new Provider Services system is current with the source systems. We then load the extract data into staging tables for data purification and transformation. From the staging tables, the data is loaded into the production database. In both implementations, the web portal was available on Monday morning and transactions sent to the MMIS that same night.

A production release of the application that includes all COTS products must be built and deployed to the production platform. The disaster recovery site must be readied and operational. Batch production jobs must be scheduled. This includes interface file exchanges if they cannot be performed via web services. Procedures for reporting system problems must be defined and tested. A security scan of the application software is performed immediately prior to every production build. Once the scan is complete, the build is deployed to the production environment. The final activity before loading the users' security profiles is a smoke test conducted by MAXIMUS, which verifies that the production build is complete, functioning,

and ready for operations. Links to the new application are enabled and Providers, DPHHS, and the operations staff can begin using the system.

Once the system is implemented and MAXIMUS users, DPHHS workers, and Providers begin to use the system, MAXIMUS will provide support as needed to confirm a successful transition of system and services. During the support period, we will work in partnership with the State to identify areas of the newly installed system that may not be performing to the specifications set forth in the implementation plan. MAXIMUS technical resources will immediately begin work to resolve the non-compliant system functions and will track and address all reported issues and defects.

3.10.2.8.3Implementation and Acceptance Requirements

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

ID	Implementation and Acceptance Requirement	MAXIMUS Summarized Response
IA01	The Contractor shall follow the following process for deploying each proposed solution(s) to production: a. Submit an implementation letter to the State confirming that the solution is ready for implementation. b. Receive the State's approval of the implementation letter, accepting the Contractor's confirmation. c. Deploy the solution according to the approved Implementation Plan. d. Provide confirmation that the solution has been deployed to production and the Contractor has completed three (3) calendar days of operations without significant operational issues defined as no critical or high defects. e. Receive the State's acceptance of the system implementation.	MAXIMUS follows the process defined by the State for deploying changes to production. MAXIMUS works closely with the State to secure State approval of the implementation plan and acceptance of the implementation.
IA02	The Contractor shall monitor the initial operation of the solution to ensure that there are no immediate or ongoing adverse effects on the Department's programs according to the performance expectations identified in the Contractor's scope of work.	MAXIMUS monitors the system upon implementation to confirm no adverse effects on the Department's programs. MAXIMUS staff monitors batch job functionality continually to validate the jobs are running appropriately and that updates are being made as expected. Refer to *Section 3.10.2.8.2–Implementation* for further details.
IA03	The Contractor shall demonstrate that the System infrastructure (hardware, software, and interfaces) is operational and meets federal and State architectural, technical, security and privacy requirements as well as the business and functional requirements.	MAXIMUS demonstrates that the system is operational and meets the federal and state architectural, security and privacy requirements as well as the requirements defined in the RTM. This traceability is also found in the JAMA Contour tool, as described in *Section 3.10.2.3–Requirements Management*.
IA04	The Contractor shall provide Operational Readiness test results demonstrating that the solution meets all Service Level Agreements for system performance as defined in the scope of work.	As part of Operational Readiness, MAXIMUS provides the Department with all test results including performance load testing and security scan results. MAXIMUS provides these same test results for the systems implemented in other states as well. Service Level Agreement information is provided as required by each contract. Refer to *Section 3.10.2.8.1–Operational Readiness* for further details on our approach.
IA05	The Contractor shall conduct an Operational Readiness Walkthrough with the Department to validate the operational readiness of the Contractor, the solution, and the Department. The Department must formally sign off on the Operational Readiness Checklist prior to proceeding to implementation.	MAXIMUS builds and completes an Operational Readiness Checklist. This checklist is reviewed in weekly meetings and defines the low-level tasks that need to be completed to go live. This checklist is reviewed with the State on a regular basis so that state staff are satisfied that the system is operational and ready for go-live. Refer to *Section 3.10.2.8.1–Operational Readiness* for further details on our approach.

ID	Implementation and Acceptance Requirement	MAXIMUS Summarized Response
IA06	The Contractor shall develop Operational Readiness Review Checklists (ORR) that will examine the actual solution characteristics and the procedures of the product's operation to ensure that all hardware, software, resources, procedures, and user documentation accurately reflect the deployed state of the system.	MAXIMUS builds and completes ORRs to verify that the hardware, software, procedures, and user documentation reflect the system that is ultimately deployed to production. These checklists are created well in advance of the expected implementation date and are reviewed on a consistent basis with the State and their external vendors. Refer to *Section 3.10.2.8.1–Operational Readiness* for further details on our approach.

3.10.3 Certification

3.10.3 Certification

The Contractor must work with DPHHS and other contractors as necessary to ensure that all solutions provided by the Contractor meet requirements specified in the Mechanized Claims Processing and Information Retrieval Systems (90/10) Final Rule (CMS 2392-F) and relevant federal certification requirements as described in the most current version of the MECT Toolkit available at https://www.medicaid.gov/medicaid-chip-program-information/by-topics/data-and-systems/mect.html.

The Contractor will be responsible for providing and maintaining a solution that meets all applicable checklist items in the most current version of the Medicaid Enterprise Certification Toolkit (MECT), and supporting the review and validation of those items by the Department, IV&V Contractor, and CMS. The Contractor must become knowledgeable of all MECT-related items associated with the solution offered. The MECT Mapping document, found as Attachment D, contains the most current version of the MECT checklist items applicable to the Contractor's scope of work, mapped to the associated business requirements.

The Contractor must provide staff and other resources to support and to participate in MECT milestone reviews and other Certification activities that occur before, during and after implementation of the proposed solution(s). The Offeror must describe their approach to meet each of the Certification requirements defined in Attachment F, Requirements Matrix.

MAXIMUS offers DPHHS a proven solution 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). It includes the Medicaid Enterprise Certification Life Cycle (MECL) published by CMS and updated in July 2016. The MECL implements the modularity standard as required by the standards and conditions for Medicaid IT, as well as critical success factors. MAXIMUS is prepared to collaborate fully with the State and its Trading Partners, including all Medicaid Enterprise contractors and sub-contractors, to achieve unconditional federal certification.

Certification efforts of the MAXIMUS provider management solution are well underway in Nebraska and the District of Columbia, with both clients expecting to achieve federal certification in the coming months. MAXIMUS has been integral to these efforts by drafting certification plans and checklist responses, and preparing the evidence and artifacts required for the CMS Certification Final Review (R3). Nebraska and the District of Columbia are following the new, federal certification process, and the experience MAXIMUS has gained in this area is extensive. MAXIMUS has a comprehensive understanding of the certification items in both the 2.1.1 and 2.2 versions of the checklists, including the preferred evidence to support the requirements, as well as the artifacts in Appendix B of the MECT. MAXIMUS will perform the same service for Montana and Participating States, applying lessons learned from previous certification efforts. This section provides a detailed description of our approach to certification and demonstrates our thorough understanding of the process.

MAXIMUS understands the flexible approach to certification CMS has adopted. The MAXIMUS approach to certification is thorough, established, and verified, as proven by the certification efforts in both Nebraska and the District of Columbia. The MAXIMUS certification experience in two states using the MECT will prove invaluable for the DPHHS's goal of achieving CMS certification.

MAXIMUS certification preparation begins with a full list of certification tasks that we integrate into the larger System Implementation plan. To finalize the list of certification tasks, MAXIMUS will review the certification plan tasks with the State to validate the tasks, work products, schedule dates, task dependencies and both State and MAXIMUS responsibilities.

The MECT checklist items emphasize interoperability. The provider management module must be able to easily interface with other modules, regardless of the technology or the vendor providing the module. We are able to connect our system to the MMIS and other state systems using a variety of interface mechanisms, and we currently support the required verification data sources. Our system eliminates the current environmental constraints and provides flexible and scalable technology, required functionality, and system interoperability that may be lacking in the current MMIS architecture.

We plan to work closely with the State to plan and schedule the CMS certification review of the overall solution and we will have staff available to assist the State in readying for the certification meetings with CMS. Our knowledgeable staff will create and verify completion of the certification checklists. Verification of certification readiness includes making sure the applicable evidence and artifacts are provided, and system demonstrations are thorough and polished. Based on our experienced team and MITA aligned, ACA-compliant system, we anticipate a fast certification process.

3.10.3.1 Prepare Certification Plan

MAXIMUS fully appreciates the changing nature of CMS's MECT. With its many changes since its inception in 2007, an important component of preparation for certification begins with staying current with the dynamic nature of the toolkit. From our involvement in national CMS-attended MECT and MITA focused conferences to our role in the development of CMS-compliant best practices, MAXIMUS is well positioned to stay current with the evolution of CMS requirements for certification.

From the beginning of contract award, MAXIMUS plans for the steps necessary to achieve federal certification, relative to the most current strategy laid out by the MECT. The Certification Plan provides the roadmap for achieving federal certification within State timeframes. Not only do we develop a thorough and detailed Certification Plan, we also incorporate certification steps into other plans, such as the Test Management Plan and Implementation Plan. The MAXIMUS Certification Plan provides detail on the tasks described in *Exhibit 3.10.3-1: Certification Plan Components*.

Certification Plan Components	
Process	**Description**
Document Certification Requirements	Montana has made significant progress in identifying the current certification checklist items as listed in RFP Attachment D. We will meet with the State to review the applicable items and verify consistent understanding of each item. 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 key stakeholders as to the interpretation of individual items. Establishing a baseline understanding at the beginning of the project—determined by the most current set of requirements and strategies laid out by CMS at the time of planning—will save significant time and effort

Certification Plan Components	
Process	**Description**
	during the process. In addition, it is at this point that we establish a template for standardization of documentation, consistency, and efficiency.
Draft Initial Responses	Many checklist items are common to all States. Therefore, we are able to leverage responses and artifacts from prior certification efforts to reduce the time and effort of drafting responses and compiling supporting evidence. Our experience has also shown that a single artifact may satisfy multiple responses.
Conduct Gap Analysis	Although we are able to leverage previous responses, we will tailor material for Montana and Participating States. MAXIMUS works with the State and the IV&V vendor to identify gaps, improve responses, and hone the relevant artifacts.
Prepare and Deliver Certification Review Package	This task includes finalizing the certification checklist responses and supporting evidence and artifacts. Feedback received from IV&V and the State, along with any system updates, may require updates to the MECT checklist responses. This step also includes assembling and delivering all product evidence in support of the checklist responses as well as artifacts required by Appendix B of the MECT. These include creating reports and analyzing sample data, as well as preparing all the required documentation for submission to CMS for review prior to the CMS on-site visit. This list changes for each milestone review and MAXIMUS is familiar with the different requirements for the R2 and R3 reviews.
Support CMS Certification	MAXIMUS provides a combination of business and technical support staff to support the State in achieving CMS certification of the MAXIMUS Provider Services solution. This support occurs before, during and after system implementation. Support activities include: ▪ Consolidating required documentation for CMS and maintaining it in a central location (leveraging our own record retention and version control systems or the State's, as required) ▪ Participating in pre-certification calls as required by the State ▪ Demonstrating system functionality ▪ Supporting the CMS onsite review MAXIMUS maintains continuity in staffing during the entire certification effort, including any follow-up necessary to resolve compliance issues.

Exhibit 3.10.3-1: Certification Plan Components. *The MAXIMUS Provider Services solution meets Certification Plan tasks for achieving federal certification within State timeframes.*

The project's Certification Plan guides the tasks and activities involved in our certification approach. We will submit the Plan, which outlines the tasks and planning activities required to achieve federal certification, to the Department according to the PWPW. Our submitted Certification Plan will contain the required content as specified in requirement DOC02 and as stipulated in Attachment F. We have produced detailed Certification Plans in previous Provider Services implementations. *Exhibit 3.10.3-2: Sample Certification Plan* shows a snippet from the Certification Plan we submitted for the District of Columbia.

MAXIMUS

Certification Plan Deliverable Requirements

This plan outlines how the Contractor will work with the District, and if needed, the fiscal agent, to achieve certification as soon as possible after go-live. If the Contractor revises the Certification Plan, the District must review it, and approve in writing before implementing such changes. Version 2.0 is being submitted to reflect changes to the approach based on revised CMS certification guidance and the District decision to proceed using the MMIS Module Checklist Set, as required per number 4 in the following table.

Table 2 - Certification Plan Requirements

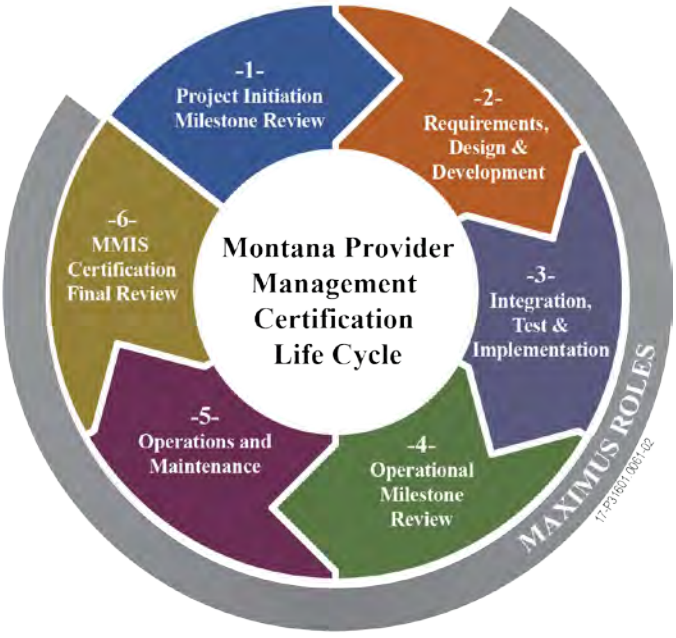
Document ID	Description
DCHT-2015-R-0002/Doc190672 Request for Proposals - Provider Data Management System and Services (PDMS) C.5.2.1.6.6	MAXIMUS has crafted our Certification Plan and approach around creating this deliverable as a living document that will be updated throughout the project leading to the creation of certification documentation that can be used to support the CMS Certification review. The specific requirements for the Certification Plan are: 1. Submit within two weeks of the initial meeting with the District 2. Provide detailed Certification Plan pertaining to the tasks MAXIMUS intends to pursue to keep certification as an ongoing body of work that must be pursued throughout the DDI period 3. Outline how MAXIMUS will work with the District, and the fiscal agent, if needed to achieve certification as soon as possible after go-live 4. Submit revisions to the District for review and written approval before implementing changes

Exhibit 3.10.3-2: Sample Certification Plan. *MAXIMUS submits the Certification Plan to DPHHS, which outlines our approach for successfully achieving federal certification. We tailor our previously created planning documents to meet the requirements of each State.*

3.10.3.2 Support Certification Activities

MAXIMUS is committed to achieving the State's goal of obtaining federal certification. The system capabilities, along with our team's exceptional experience and commitment, facilitates and expedites CMS certification. We understand that maintaining certification is an absolute priority of the State.

MAXIMUS is extremely familiar with the activities that must occur through the CMS certification lifecycle (see graphic), including preparing for the Operational (R2) and Final (R3) milestone reviews. These activities include:



- Identifying and verifying applicable checklist items
- Drafting responses to applicable certification checklist items
- Assembling documentation in support of the checklist items
  - Includes design documents, interface control documents, copies of notices and reports, configuration management documents, data center and security protocols and even screen shots.
  - Artifacts are stored in a single location that is organized to easily identify which checklist item(s) the artifact corresponds
- Assembling artifacts as required in Appendix B of the MECT (required artifacts vary between the R2 and R3 reviews and require careful attention to the MECT)
- Preparing and presenting system demonstrations for CMS, including presentation materials

While providing written responses and documentation is key to CMS certification, preparing for the actual, final milestone review is also critical. Providing easily accessible documentation and evidence helps CMS prepare for the milestone review. In addition, a milestone review kickoff meeting is held for the state and CMS to introduce their respective team members. MAXIMUS looks forward to participating in these meetings in the capacity as directed by the State. The review meetings generally last from two to four days and CMS may choose to conduct them by web conferencing, or in person.

3.10.3.3 Certification Replies

The MAXIMUS Provider Services solution is being certified in both Nebraska and the District of Columbia. As part of those efforts, we have created certification responses to six of the applicable certification checklists. This section (*Exhibit 3.10.3-3: Provider Management Checklist Replies*) provides the MAXIMUS responses to the items in the MMIS Module Provider Management Checklist from the MECT. Responses to the other applicable MECT items as referenced in Attachment D are addressed elsewhere in this proposal.

Provider Management Checklist Replies	
Reference Number - Review Criteria	**MAXIMUS Provider Services Solution Alignment with System Review Criteria**
EE.PR1.1 - The system produces notices to applicants of pending status, approval, or rejection of their applications.	The MAXIMUS Provider Services solution provides full electronic communication with Providers, including the 'Return to Provider' function for incomplete applications.
PM.PR1.1 SMA supports provider outreach through evaluation of provider networks and tracking of performance measures to ensure correct mix of providers within state.	The MAXIMUS Provider Services solution allows for Geographic Information System (GIS) search by provider type and displays concentrations of active providers within specific geographic regions. Desired provider type counts within geographic areas can be set and provider outreach can be conducted based on desired selection criteria. System dashboards allow users to view current active counts of providers in real time. Robust interface capabilities with State agencies or external entities support business functions and align with Department policy, and federal and State rules and regulations.
PM.PR1.10 The system produces responses to requests/inquiries on the adequacy of the Medicaid provider network	The MAXIMUS Provider Services solution captures address data, including county and tracks providers and provider counts of providers based on geographic region

Provider Management Checklist Replies	
Reference Number - Review Criteria	**MAXIMUS Provider Services Solution Alignment with System Review Criteria**
based on provider/beneficiary ratios by geographic region, provider type, etc.	and provider type. Our solution captures provider practice information, including office hours and whether new patients are accepted.
PM.PR1.11 The system uses consistent provider naming conventions to differentiate between first names, last names, and business or corporate names and to allow flexible searches based on the provider name.	The MAXIMUS Provider Services solution uses consistent provider naming conventions to differentiate between first names, last names, and business or corporate names. Search capabilities are flexible and allow for partial and full name searches.
PM.PR1.2 The system routes provider applications, and collects and processes provider enrollment and status information.	The MAXIMUS Provider Services solution contains a workflow engine that routes provider applications to internal worker queues for review and screening and maintains status of the provider application throughout all steps within the workflow.
PM.PR1.3 The system assigns and maintains provider numbers for all providers if the system is not natively NPI-compliant internally. Maps NPI identifiers to internal assigned numbers. Assigns and maintains provider numbers for providers not eligible for an NPI number.	The MAXIMUS Provider Services solution assigns unique provider numbers to each provider. Our solution is natively compliant with NPI and has an interface with NPPES to validate the NPI (when required). Our solution recognizes providers by type and enforces entry/validation of either Type 1 or Type 2 NPI based on provider type.
PM.PR1.4 The system flags and routes records for action if multiple internal state assigned provider numbers are associated with a single provider.	The MAXIMUS Provider Services solution contains front-end edits to prevent duplicate providers from enrolling in the system and does not allow multiple internal State assigned numbers for a single provider.
PM.PR1.5 The system supports communications to and from providers and tracks and monitors responses to the communications.	The MAXIMUS Provider Services solution includes automated and manual communications with providers based on review and screening tasks completed by enrollment specialists. All communications with providers are tracked within our solution.
PM.PR1.6 The system supports a provider appeals process in compliance with federal guidelines contained in 42 CFR 431.105.	The MAXIMUS Provider Services solution supports the State's Program Integrity office by an automated appeals process compliant with 42 CFR 431.105.
PM.PR1.7 The system maintains date-specific provider enrollment and demographic data.	The MAXIMUS Provider Services solution maintains a history of the Provider enrollment profile with an audit trail of changes.
PM.PR1.8 The system generates information requests, correspondence, or notifications based on the status of the application for enrollment.	The MAXIMUS Provider Services solution workflow engine automatically generates correspondence, sent via email, based on the status of the enrollment.
PM.PR1.9 The system tracks the sending of state furnished information to enrolled providers.	The MAXIMUS Provider Services solution maintains a history of all correspondence sent and received from a provider. Providers are able to view electronic communication received via the web portal.
PL.PR2.1 The system maintains multiple provider specific reimbursement rates with begin and end dates, consistent with State policy. Examples include: per diems, level-of-care per diems, case mix, percentage-of-	MAXIMUS works with the State to refine requirements and validate the strategy for the capture, storage, and updating of reimbursement rates and their corresponding effective dates. The system can be configured to capture this data and then sent to the MMIS in the interface file.

Provider Management Checklist Replies	
Reference Number - Review Criteria	**MAXIMUS Provider Services Solution Alignment with System Review Criteria**
charge rates, rates based on level of care, preferred provider agreements, managed care agreements, volume purchase contracts, or other cost-containment initiatives with begin and end effective dates.	
PM.PR2.1 SMA tracks and supports the screening of applications (and ongoing provider updates) for (National Provider Identifier (NPIs), State licenses, Specialty Board certification as appropriate, review team visits when necessary, and any other State and/or Federal Requirement.	The MAXIMUS Provider Services solution provides full automated screening for all required data for initial enrollment and ongoing update/revalidation. Our solution keeps a history of all screening checks and outcomes.
PM.PR2.2 The system tracks and supports any established provider review schedule to ensure providers continue to meet program eligibility requirements.	The MAXIMUS Provider Services solution maintains a revalidation schedule for each provider based on State and CMS rules. Our solution automatically generates reminder notices to providers when revalidation due dates approach.
PM.PR2.3 The system verifies provider eligibility in support of other system processes, i.e. payment of claims.	The MAXIMUS Provider Services solution maintains a full provider enrollment profile and verifies all data associated with the enrollment. Only valid, screened providers are active in our solution.
PM.PR2.4 The system captures clinical laboratory improvement amendments (CLIA) certification information and the specific procedures each laboratory is authorized to cover. Links the information for use in claims adjudication.	The MAXIMUS Provider Services solution captures CLIA data, including authorized lab procedures, for enrolling providers. Weekly refreshes on CLIA data are received and stored in our solution.
PM.PR2.5 The system cross-references license and sanction information with other state or federal agencies.	The MAXIMUS Provider Services solution provides automated interfaces with exclusion sites, including OIG LEIE, EPLS/SAM, and MCSIS. Our solution provides for verification of licenses for each state, directing the user to the appropriate licensure website based on the location of the license. The system also interfaces with the Social Security Administration's Death Master File and the National Plan and Provider Enumeration System (NPPES). In addition to checks at the time of enrollment or revalidation, providers are placed in the operator's queue to review when an adverse result is detected while the provider is enrolled.
PM.PR2.6 The system generates notices to providers of expiring Medicaid agreements and/or state licenses.	The MAXIMUS Provider Services solution generates automated correspondence to providers based on configurable business rules. Our solution captures expiration dates for all credentialing data, including licenses.
PM.PR2.7 The system maintains the capability to limit billing and providers to certain benefit plans, services, by procedure codes, ranges of procedure codes, member	The MAXIMUS Provider Services solution assigns specific category of service codes to each enrolled provider based on state defined rules.

Provider Management Checklist Replies	
Reference Number - Review Criteria	**MAXIMUS Provider Services Solution Alignment with System Review Criteria**
age or by provider type(s) or as otherwise directed by the State.	
PM.PR2.8 SMA ensures all end dates are linked, so they can be synchronized to the servicing location state licenses or other licenses as directed by the State.	The MAXIMUS Provider Services solution assigns specific category of service codes to each enrolled provider based on state defined rules. Our solution maintains effective dates (begin and end dates) for all enrollment data based on provider type. Our solution provides for automated communications to providers for licenses and re-enrollment based on license expiration dates and re-enrollment due dates. System workflows for license renewal and re-enrollment are driven by the end dates of all pertinent provider data.
PM.PR2.9 The system supports automated criminal background checks for all providers as specified by the State.	The MAXIMUS Provider Services solution supports screening of all high-risk providers and owners for fingerprint-based criminal background checks. The system allows changes to risk level that initiates the background check process when a provider becomes high-risk.
PM.PR3.1 The State plan must provide for the identification of providers by Employer identification number.	The MAXIMUS Provider Services solution collects EINs and SSNs for individual providers.
PM.PR3.10 The system maintains a flag for providers who are eligible to use electronic funds transfer (EFT) and electronic claims submission.	The MAXIMUS Provider Services solution captures EFT banking information from enrolling providers.
PM.PR3.2 The Medicaid Agency must demonstrate how the system identifies health care providers using the standard unique National Provider Identifier (NPI). The NPI is a 10-position numeric identifier, with a check digit in the 10th position, and no intelligence about the health care provider in the number. (b) Required and permitted uses for the NPI. (1) The NPI must be used as stated in § 162.410, § 162.412, and § 162.414. (2) The NPI may be used for any other lawful purpose.	The MAXIMUS Provider Services solution is natively compliant with NPI and has an interface with NPPES to validate the NPI (when required). Our solution recognizes providers by type and enforces entry/validation of either Type 1 or Type 2 NPI based on Provider type. The NPI is used solely as a key identifier and is shared with the MMIS via nightly interface.
PM.PR3.3 The system accepts, validates, and processes transactions or user entries to update and maintain provider information.	The MAXIMUS Provider Services solution provides the ability to process updates to data through multiple channels and contains edits on all provider-entered data.
PM.PR3.4 The system tracks and controls the process of reconciliation of errors in transactions that are intended to update provider information.	The MAXIMUS Provider Services solution edits are online and immediate. Our solution handles error processing with the MMIS interface and allows users to view and take action on any potential errors passed from the MMIS.
PM.PR3.5 The system maintains current and historical multiple address capabilities for providers.	The MAXIMUS Provider Services solution maintains current and historical address information for providers. Our solution maintains a primary business address, pay to address, remittance address, and mail to address as part of the standard implementation.

Provider Management Checklist Replies	
Reference Number - Review Criteria	**MAXIMUS Provider Services Solution Alignment with System Review Criteria**
PM.PR3.6 The system maintains an audit trail of all updates to the provider data, for a time period specified by the state.	The MAXIMUS Provider Services solution keeps a full audit trail of all data in the system. This data is never archived.
PM.PR3.7 The system maintains providers' drug enforcement administration (DEA) numbers.	The MAXIMUS Provider Services solution captures and maintains the DEA number. The system directs users to validate the DEA number through the available DEA verification website.
PM.PR3.8 The system provides capability to do mass updates to provider information, based on flexible selection criteria.	The MAXIMUS Provider Services solution assigns specific category of service codes to each enrolled provider based on State defined rules.
PM.PR3.9 The system maintains indicators to identify providers that are fee-for-service (FFS), managed care organization (MCO) network only, and other state health care program participants.	Indicators can be added to our solution that can qualify their type participation in the Medicaid program.

Exhibit 3.10.3-3: Provider Management Checklist – MECT 2.1 (MMIS Module). *The MAXIMUS Provider Services solution meets all Provider Management Checklist items for CMS Certification.*

User Interface Requirements

The MAXIMUS Provider Services solution meets the MECT user interface requirements. We assembled documentation to demonstrate compliance during the R3 certification review for the State of Nebraska. We will consolidate these and other artifacts into a User Interface Style Guide to define the standards for user interfaces as specified in requirement DOC46 as specified in Appendix F as scheduled in the approved PWP. This Style Guide can be used as an artifact as the State prepares for R2 and R3 milestone reviews with CMS.

Exhibit 3.10.3-4: Sample MECT Responses based User Interface Style Guide describes the artifacts MAXIMUS supplied for the R3 reviews in both Nebraska and the District of Columbia.

User Interface Style Requirement	MAXIMUS Response and Evidence
User ability to customize or make adjustments (e.g. language support, font size) to portal presentation.	Screen shots showing system display in different languages and different font size according to the user's browser settings. Note this requirement was removed in the 2.2 version of the MECT.
Users utilizing scripting languages and/or assistive technology have the ability to access the information, field elements, and functionality required for electronic form or page completion and submission including directions and cues.	Our solution is 508 compliant. We provide before deployment and after deployment reports designed to demonstrate 508 compliance. *Note: This requirement was removed in the 2.2 version of the MECT.*
User Interface organization so documents are readable without requiring an associated style sheet.	Documents are viewable without requiring a style sheet. Documents are stored in standard, readable formats such as PDF and JPG. The Application Response PDF supports the response, as well as a demonstration of document upload and retrieval. *Note: This requirement was removed in the 2.2 version of the MECT.*

User Interface Style Requirement	MAXIMUS Response and Evidence
User Interfaces identifying row and column headers for data tables.	In our solution, all data tables have column headers to describe the contents of each column. As evidence, we supplied a design and screenshot showing the Provider Screening page in which there is a grid with column headings to describe the contents of each column. *Note: This requirement was removed in the 2.2 version of the MECT.*
User Interfaces informing users when a timed response is required and given sufficient time to indicate more time is required.	Our solution issues an alert to the user after 60 minutes of inactivity to either be logged out or remain active. A design and screenshot support this requirement. *Note: This requirement was removed in the 2.2 version of the MECT.*
User Interfaces providing a method that permits users to skip repetitive navigation links.	The MAXIMUS Provider Services solution provides a 'Prior' and 'Next' button on each webpage (within a system workflow) to allow users to easily navigate from one screen to the next. Our solution also has a navigation menu drop-down that allows users to directly navigate to any screen within the system. Designs and screenshots and demonstration support compliance with this item. *Note: This requirement was removed in the 2.2 version of the MECT.*
User Interfaces provide text titles for frames to facilitate frame identification and navigation.	The MAXIMUS Provider Services solution user interface contains a title of each section and sub-section of a web page. PDMS contains a drop-down menu that contains the title of each screen within the application that allows for easy navigation by users. Design documents, screenshots, and system demonstration all support this requirement.
User Interfaces use markup to associate data cells and row/header cells for data tables that have two or more logical levels of row or column headers. (TA.CS.9)	The system uses appropriate markup as needed to associate data cells and row/header cells for data tables. Design and screenshots as well as system demonstration support compliance with this item. *Note: This requirement was removed in the 2.2 version of the MECT.*

Exhibit 3.10.3-4: Sample MECT Responses based User Interface Style Guide. *The MAXIMUS Provider Services solution meets all MECT requirements for the user interface.*

Certification Requirements

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

ID	Certification Requirement	MAXIMUS Summarized Response
CERT01	The Contractor shall develop a Certification Crosswalk that describes how the Contractor's deliverables and other documentation align with federal certification requirements and MECT milestone reviews.	To verify deliverables and other documentation align with federal certification requirements, MAXIMUS deliverables will contain an indicator to designate the certification checklist item to which it corresponds.
CERT02	The Contractor shall complete quarterly and milestone updates of the CMS Certification Checklists as requested by the State.	We maintain checklist responses and supporting artifacts as changes occur during the life of the contract. This includes quarterly and milestone updates as well as other dates requested by the State.
CERT03	The Contractor shall validate the system against the CMS Certification Checklists	The CMS Certification Checklists serve as a requirements guide to the design and support of our solution and are used for system validation.
CERT04	The Contractor shall contribute to the quarterly IV&V certification reports.	Ongoing and open dialogue with the IV&V vendor is key to success. In that spirit, we will contribute to the quarterly IV&V certification reports.

ID	Certification Requirement	MAXIMUS Summarized Response
CERT05	The Contractor shall provide staff resources to support MECT milestone review and certification activities including participating in planning activities, meetings and other activities as required by CMS.	Our experience has taught us that preparation and open communication are key in preparing for CMS milestone reviews. MAXIMUS participates fully in meetings with CMS, the State and other vendors as necessary to conduct a successful milestone review that can result in federal certification.
CERT06	The Contractor shall assist the Agency in preparing certification artifacts, evidence and presentation materials, e.g., Requirements/ user stories and/or use cases for functional and non-functional requirements, data, business, capacity/performance, security/privacy/HIPAA compliance, usability, maintainability, interface, 508 compliance, disaster recovery, traceability to test plans or test cases.	The Certification Plan includes steps for preparing the required documentation, including reports and all completed systems documentation and storing and providing it in one location. We understand the vast amount of documentation required for a successful certification and we will assist the Agency in preparing all artifacts, evidence and presentation materials.
CERT07	The Contractor shall participate and support as needed in CMS certifications of the other modules	We understand the need to demonstrate interoperability as States move to modular solutions. We understand the State may be pursuing certification of its other modules and we will participate and support these efforts as requested by the State.
CERT08	The Contractor shall expeditiously correct, all required remediation activities related to certification findings on a schedule to be approved by CMS and the State.	MAXIMUS does not anticipate certification deficiencies. However, if deficiencies are found, MAXIMUS will promptly Deficiencies that could affect certification will be addressed as soon as possible at no additional cost to the State.
CERT09	The Contractor shall use appropriate testing, configuration and change control procedures for all changes made to the solution during the certification process.	We establish appropriate testing, configuration and change control procedures early in the project and strictly adhere to these procedures during the certification process.
CERT10	The Contractor shall update system, user, and training documentation as necessary to support the certification process and to reflect changes that have been made to the solution during the certification process.	Maintaining current documentation is key to successful implementation and ongoing system support independent of CMS certification. However, CMS certification emphasizes this point. Documentation must be consistent with system functionality particularly during CMS reviews and demos. We update system, user, and training documentation to reflect the changes that have been made to the solution during the certification process.
CERT11	The Contractor shall ensure system CMS Certification through correct design, implementation, documentation and certification support.	While the CMS certification checklists serve as a requirements document, CMS certification is much broader and requires proof of adherence to project management protocols, such as change control and regular status reporting. These efforts support the certification process as we demonstrate compliance with correct design, implementation, and documentation and provide ongoing certification support.
CERT12	The Contractor shall coordinate with the State to develop CMS Certification Checklist documentation for each MECT Checklist requirement.	CMS has a strong interest in States providing documentation that is easily referable back to the checklist item and is easily accessible. As stated above, the Certification Plan includes steps for preparing the required documentation in coordination with the State.
CERT14	The Contractor shall populate the certification document repository, as each required item/artifact is completed and approved.	We coordinate with our State and IV&V partners in the delivery of certification items and artifacts. We will populate the certification document repository as the items are completed and approved according to the process established in the initial steps of the Certification Plan.
CERT16	The Contractor shall present at milestone reviews and other certification meetings as directed by the State.	We will present the certification responses and supporting artifacts, as well as demos of the solution at milestone reviews and other certification meetings as directed by the State.

3.10.4 Operations, Maintenance, and Configuration

3.10.4 Operations, Maintenance, and Configuration

The Contractor shall provide Operations support, Maintenance, and ongoing Configuration of the provided Solution(s) throughout the life of the Contract. This includes providing Operations support as described in the scope of work as well as

> providing Maintenance and Enhancements to the provided Solution(s). The Contractor will follow project management and system development processes throughout the life of the Contract.

MAXIMUS uses a well-defined and proven approach to application support of the MAXIMUS Provider Services solution after implementation. Operations and Maintenance (O&M) support is not simply a break-fix and enhancement effort. A variety of activities must occur to keep the system operating at the best possible level of performance with no disruptions in service. These activities include:

- Fielding, researching and resolving issue reports
- Monitoring system performance and response time
- Monitoring and updating system security
- Scheduling, executing and verifying the execution of batch procedures
- Notification and distribution of regularly scheduled reports
- Prioritizing, planning, scheduling, testing and implementing system enhancements
- Implementing and testing third party software upgrades
- Implementing and testing hardware and network upgrades

MAXIMUS issues weekly status reports and holds meetings similar to those held during the Transition Phase continue for the life of the contract. MAXIMUS finds frequent and open communication is critical to keep all parties well informed of the status of the system and business processing activities of Medicaid Provider application processing. The format and content of the weekly status report changes from the topics that were important during Transition to operational issues and requests. Much of the discussion at the weekly meetings is about service requests initiated by our clients. *Exhibit 3.10.4-1: Support Processes* describes the support processes for reporting issues and requesting enhancements to the system.

Support Process	Description
Reporting Issues	Reporting issues is the process by which the DPHHS informs MAXIMUS of problems encountered in the processing of provider applications. An issue report might be written when an unexpected system action occurs, there is slow response time, a data anomaly is found, or there is a problem with a document upload.
Requesting Information	Users may encounter unexpected scenarios that the Operations team cannot address. Providers sometimes perform actions that are unexpected, such as submitting multiple applications with similar information. Technical support may be needed to help identify and resolve these types of problems.
Submitting Enhancement Requests	Submitting an enhancement request is the process by which the DPHHS requests MAXIMUS to perform a system change that is necessary to keep the system functioning as needed for daily operations. Enhancements may not have originally been defined by requirements, but the change may be required due to evolving CMS requirements, requests for additional reports, etc.

Exhibit 3.10.4-1: Support Processes. *Support requests can occur as result of issues encountered by users, a need for technical research and assistance, or modifications needed to the system.*

Each of these support processes requires DPHHS to issue a request to MAXIMUS. To facilitate the exchange and formalize the communication process, MAXIMUS uses the Customer Service Request (CSR) described in *Section 2.15.1–Customer Service Request Form*. DPHHS emails completed forms to Support.MTProvider@maximus.com. MAXIMUS technical and business support staff monitors this email inbox.

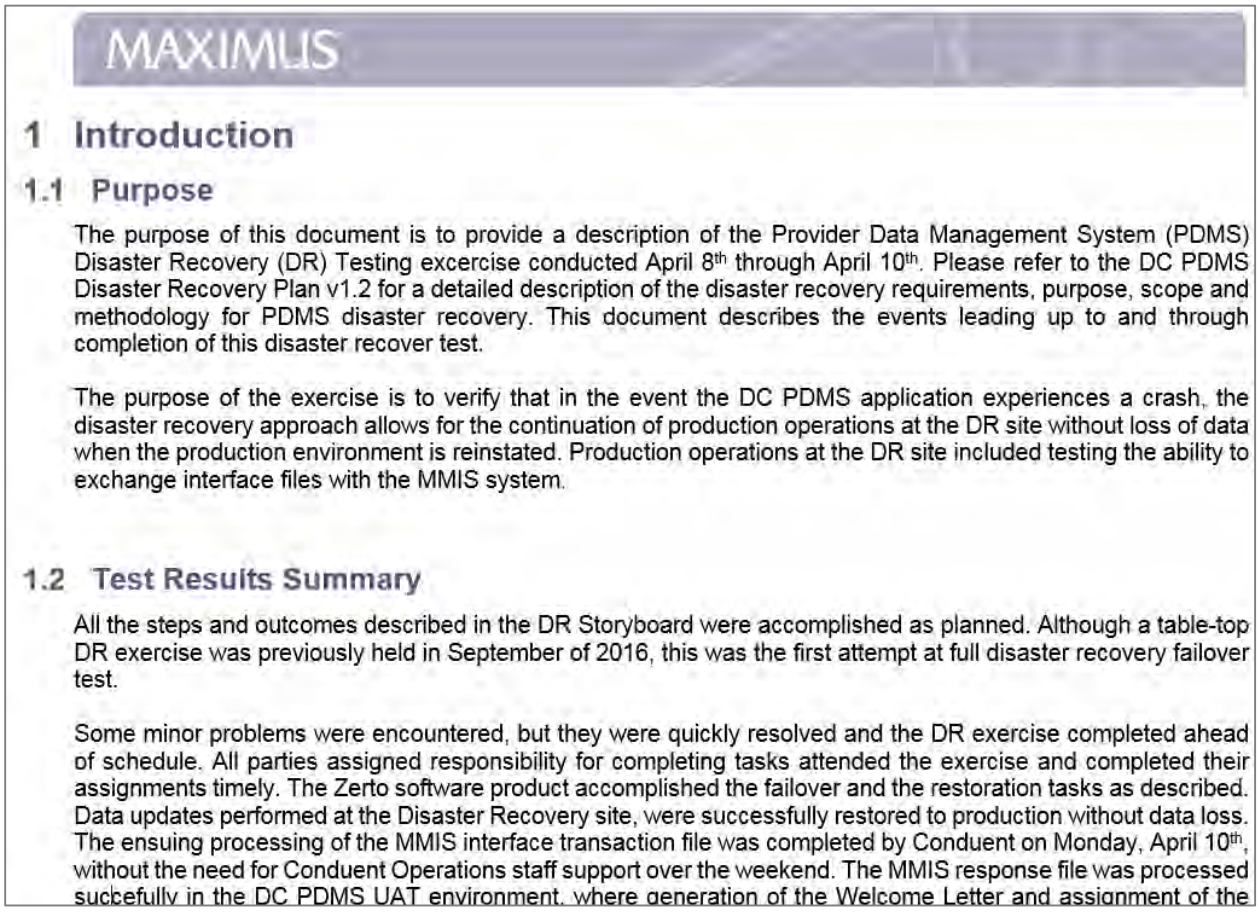
Upon receipt of the CSR, the MAXIMUS business analyst logs the request in JIRA. If the request indicates an error has occurred, our business analyst researches, documents, and assigns a priority. If the issue can be resolved without a software change, we propose a resolution and close the issue. Business analysts are frequently able to address items such as training issue or informational requests without software changes. If the business analyst cannot resolve the issue, the analyst passes the JIRA ticket to the development lead for further triage and assignment based on the request's priority.

MAXIMUS staff log enhancement requests JIRA. MAXIMUS works these items similar to system defects, except DPHHS will set the priority for enhancements and determine when they are needed. MAXIMUS will work with DPHHS to develop the schedule for at least three software releases in advance. We schedule software releases every three to four weeks, which may include defect fixes and enhancements. All software changes go through three testing cycles: unit, system, and user acceptance. After implementation, MAXIMUS staff smoke test the software release to make sure it is ready for production.

Once per month, MAXIMUS Data Center staff will meet with DPHHS management to discuss system performance reports, SLAs, and the current schedule for hardware, system software, and third-party COTS software upgrades. This meeting will include a discussion of regularly scheduled maintenance activities, disaster recovery testing, security breach attempts and any unscheduled and planned downtimes.

Disaster Recovery/Business Continuity Test Report

The contents of our Disaster Recovery/Business Continuity Test Report will be guided by the project's Business Continuity and Disaster Recovery Plan. This required deliverable will be submitted to the Department following our annual disaster recovery exercise. Our Test Report contains the required content as specified in requirement OMC03 as specified in Appendix F, including the outcome, and any corrective action or revisions we will make as a result of the test. We have produced detailed Test Reports in our previous Provider Services implementations. *Exhibit 3.10.4-2: Sample Test Report* shows a snippet from the Disaster Recovery/Business Continuity Test Report we submitted for the District of Columbia.



MAXIMUS

1 Introduction

1.1 Purpose

The purpose of this document is to provide a description of the Provider Data Management System (PDMS) Disaster Recovery (DR) Testing excercise conducted April 8th through April 10th. Please refer to the DC PDMS Disaster Recovery Plan v1.2 for a detailed description of the disaster recovery requirements, purpose, scope and methodology for PDMS disaster recovery. This document describes the events leading up to and through completion of this disaster recover test.

The purpose of the exercise is to verify that in the event the DC PDMS application experiences a crash, the disaster recovery approach allows for the continuation of production operations at the DR site without loss of data when the production environment is reinstated. Production operations at the DR site included testing the ability to exchange interface files with the MMIS system.

1.2 Test Results Summary

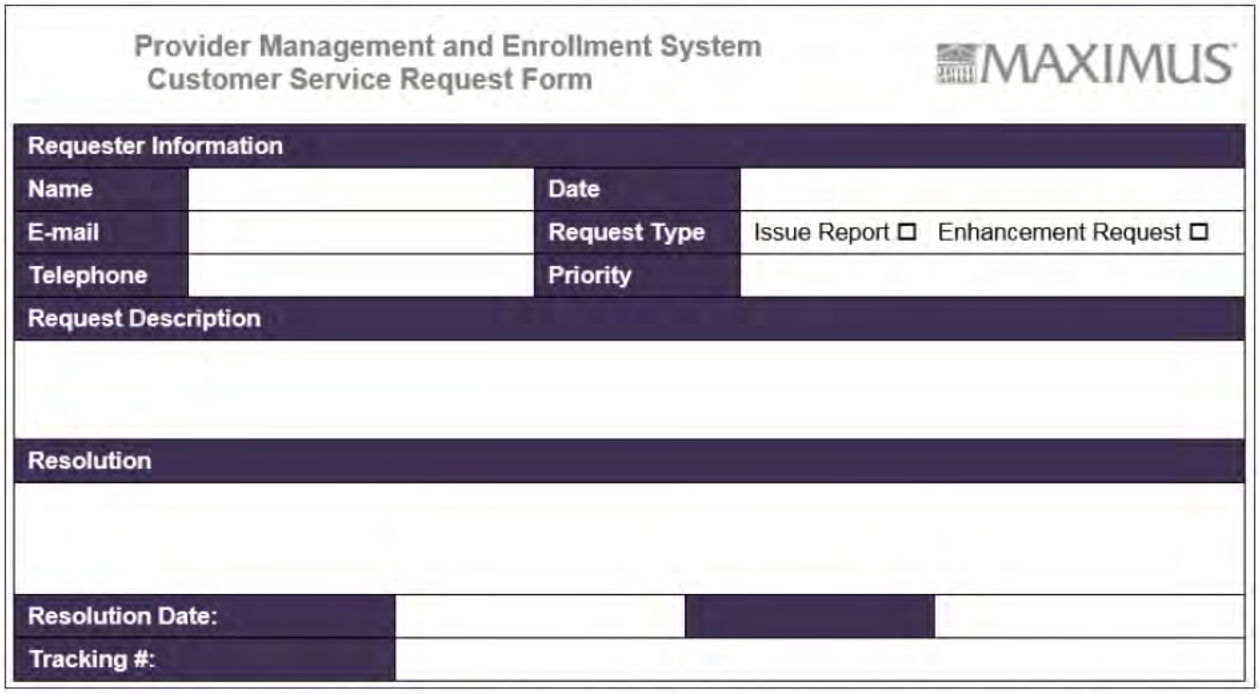
All the steps and outcomes described in the DR Storyboard were accomplished as planned. Although a table-top DR exercise was previously held in September of 2016, this was the first attempt at full disaster recovery failover test.

Some minor problems were encountered, but they were quickly resolved and the DR exercise completed ahead of schedule. All parties assigned responsibility for completing tasks attended the exercise and completed their assignments timely. The Zerto software product accomplished the failover and the restoration tasks as described. Data updates performed at the Disaster Recovery site, were successfully restored to production without data loss. The ensuing processing of the MMIS interface transaction file was completed by Conduent on Monday, April 10th, without the need for Conduent Operations staff support over the weekend. The MMIS response file was processed succefully in the DC PDMS UAT environment, where generation of the Welcome Letter and assignment of the

Exhibit 3.10.4-2: Sample DR/BC Test Report. *MAXIMUS submits a through report of the results and lessons of our annual Disaster Recovery and Business Continuity testing.*

Customer Service Request Form

Exhibit 3.10.4-3: Customer Service Request Template displays the Customer Service Request Form that MAXIMUS uses.



Provider Management and Enrollment System
Customer Service Request Form

MAXIMUS

Requester Information			
Name		Date	
E-mail		Request Type	Issue Report ☐ Enhancement Request ☐
Telephone		Priority	
Request Description			
Resolution			
Resolution Date:			
Tracking #:			

Exhibit 3.10.4-3: Customer Service Request Template. *The CSR is the communication vehicle for DPHHS to submit issue requests and enhancement requests.*

The requestor enters the Name, Email address, Date, and the Priority of the issue the requestor is 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 we can work the request with minimal discussion and questions.

Prioritization

The requesting DPHHS staff member assigns a priority level to each request. *Exhibit 3.10.4-4: Priority Categories* defines the priorities used on the project and how MAXIMUS responds to each priority.

Priority Categories	Description
Critical	Critical requests are those for which no workaround exists and the system must be changed to function properly. These requests will always be scheduled for completion before other tasks. Critical requests should be resolved in a matter of hours if they are directly affecting a broad user base of system users.

Priority Categories	Description
High	Major requests are those that must be addressed quickly due to inefficiencies using the system in its current state, implementation deadlines based on federal or state regulations, or a higher value placed on the result of completing the request relative to other tasks.
Medium	Normal requests are those that can be addressed in the longer term due to sufficient workarounds for the problem, infrequent occurrence or a low impact to the daily business.
Minor	Minor requests are tracked, but will not be worked independently unless there are no other requests to complete. As a rule, minor defects are corrected in conjunction with other higher priority defects fixes to the same components.

Exhibit 3.10.4-4: Priority Categories. *We define severity and priority levels of changes.*

The MAXIMUS Team reviews each request and determines if further discussion is necessary or if a specification is required. On a weekly basis, we review the complete list of open requests with DPHHS staff to:

- Confirm the assigned priorities
- Review the estimates
- Confirm the planned release schedule

MAXIMUS understands and agrees to the following:

Priority Categories	Performance Requirement
Critical	100% will be completed and implemented by the required implementation date.
High	80% will be completed and implemented by the required implementation date and 100% will be implemented within five business days of the required implementation date.
Medium	75% will be completed and implemented by the required implementation date and 100% will be implemented within ten business days of the required implementation date.

System Availability

System availability is a key metric that MAXIMUS must meet for the project. MAXIMUS assures that the solution will be available 99.5% of the time, 24 hours per day and seven days a week excluding approved planned downtime. Our team will perform system assessments on the application and infrastructure components to determine performance metrics and plan upcoming system upgrades. As part of our system maintenance activities, we will provide reports of all hardware, software, and network maintenance activities that affect the MAXIMUS Provider Services solution, to the State in an approved schedule. We will work with DPHHS to identify the appropriate content and media for the deliverable.

We plan well in advance for any system downtime so allow all system users to prepare. We will notify the State at least five business days prior to the installation or implementation of hardware, software network, and data center environmental changes that require downtime. We also understand that sometimes unknown issues occur that may require system downtime to correct. In these cases, we will notify and obtain approval from the State at least five business days prior to scheduling nonemergency system

downtime or maintenance for during normal hours of operation. We will follow the documented processes and understand the Department must approved the planned downtime.

In instances when a critical issue is encountered that requires downtime, MAXIMUS will restore availability using procedures in the Business Continuity and Disaster Recovery Plan within four hours from the start of the unscheduled downtime. If there are emergency deficiencies, defined as those causing severe financial or productivity impacts within one hour of the initial deficiency or within fifteen minutes of becoming aware of the issue, whichever is earlier. We will provide the plan for resolution within two hours of the notification of the deficiency to the Department and resolve the deficiency within 24 hours of the notification of the deficiency to the Department.

3.10.4.1 Maintenance and System Enhancements

> 3.10.4.1 Maintenance and System Enhancements
>
> Throughout the life of the contract there are two distinct classifications of work that all MPATH Module Contractors will perform maintenance and system enhancements.

After initial implementation of the MAXIMUS Provider Services solution, we will launch the processes for controlling maintenance and system enhancements to our solution. These modifications to the system follow established processes for change control and are implemented following a meticulous approach and according to the priorities established by the State. Although the tasks for regular maintenance and enhancements are different, both classifications must be executed in concert to secure successful deployment. The MAXIMUS approach assures coordinated development and efficient implementation.

Maintenance

> Maintenance
>
> DPHHS defines maintenance for each MPATH module as follows:
>
> 1. Making configuration updates as requested by DPHHS. Configuration includes changes to table values, parameters, codes, and business logic, including hardcoded business logic.
> 2. Correcting deficiencies (defects) found in the solution(s) based on detailed requirements described in the scope of work and published design specifications.
> 3. Correcting deficiencies (defects) found in the solution(s) based on a failure to meet the detailed requirements in completed enhancement, configuration or maintenance requests.
> 4. Conducting research requested by DPHHS or required to support the Department. For example:
>
> a. System behavior and results
> b. New healthcare initiatives
> c. Best practices research across states and industry
> d. Impacts of new State and federal legislation
>
> 5. Performing mass adjustments or mass changes as requested by DPHHS or required to support Montana Healthcare Programs (for example, errors in pricing, eligibility, cost share, and financial code assignments, TPL discovery, and provider reimbursement changes).
> 6. Performing regular maintenance as needed by DPHHS required to support Montana Healthcare Programs. Examples of maintenance include but are not limited to:
>
> a. Performance optimization.
> b. Database management.
> c. Software, hardware, and tools (e.g., patches, upgrades, and replacement).
> d. Interface, report, and correspondence changes.
> e. Making corrections or changes to maintain the integrity of the system or the data within it (e.g., backing out changes, correcting duplicate records, cleansing corrupt data, adding security measures, adding redundancy).
>
> 7. Using appropriate testing, configuration, and change control procedures.

8. Updating system, user, and training documentation and online help to reflect changes that have been made to the solution.

9. Performing the activities above to maintain customizations implemented as part of an approved enhancement.

10. Perform incremental integration services via configuration. Incremental integration services should be included in the DDI costs.

If incremental integration can be handled using configuration, the integration will fall under the definition of maintenance, if the incremental integration requires system development and testing efforts the integration will fall under the definition of enhancement.

All maintenance activities will be performed at no additional cost to the State in the Contractor's response. The Contractor will be required, at no additional cost, to add resources necessary to complete all activities by the required due date. Maintenance activities and any associated hours will not be applied to the system enhancement hourly pool.

MAXIMUS will provide system maintenance of the MAXIMUS Provider Services solution for the duration of the contract and all applicable extensions. Our comprehensive maintenance approach is an extension of our Transition methodology. We will include regular patches of any identified defects, conduct MAXIMUS Provider Services solution enhancement activities, and conduct system hardware and software maintenance required for ongoing system reliability. Our system maintenance team will continually monitor the application and infrastructure performance and conduct maintenance activities. In the broadest sense, the scope of our system maintenance approach for our solution consists of three primary support areas:

- System Maintenance Support
- System Availability Support
- System Enhancement Support

Our Maintenance Support methodology deals with the support provided to DPHHS for maintaining system user information, and reporting errors and issues in the Production system. We will implement processes that describe how DPHHS reports system defects and other issues to MAXIMUS and how we will go about completing the required tasks to correct the defect and deploy the updated functionality into production.

System availability will generally be focused on planned hardware and software updates to keep in alignment with project requirements as well as dealing with any unplanned downtime or system outages. Our System Maintenance Team will coordinate system availability with DPHHS to maximize the processing availability of the system. Our Enhancement Support processes employ the methods used by DPHHS and MAXIMUS to identify, report, and specify a required enhancement to the MAXIMUS Provider Services solution, regardless of the source from which those changes originate. 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 DPHHS. Our technical support and maintenance plan for the project will provide a customer centric solution to DPHHS for both ongoing maintenance and enhancement support needs.

As defects are reported by DPHHS, operations staff, or another authorized source and entered into our JIRA tracking system, the MAXIMUS system maintenance team will immediately analyze the issue, assign responsibility, create a task list and resolve the issue according to the agreed upon timeframes in the contract. We will report deficiencies to the Department within the following timeframes:

Category	Definition	MAXIMUS Action
Emergency	Causing severe financial or productivity impacts	▪ Notify the Department within one hour of initial deficiency or within 15 minutes of becoming aware of the issues, whichever is earlier. ▪ Provide plan for resolution within two hours of notification of the deficiency to the Department ▪ Resolve within 24 hours of the notification of the deficiency to the Department
Major	Causing serious disruption to operations and services where there is no alternative or workaround	▪ Notify the Department within one hour of becoming aware of the issue ▪ Provide plan for resolution within four hours of notification of the deficiency to the Department ▪ Resolve within 36 hours of the notification of the deficiency to the Department
Moderate	Affects a small number of users, causes inconvenience, or delays business or prevents use of a fully supported service	▪ Notify the Department within 24 hours of becoming aware of the issue

Throughout the System Maintenance period, MAXIMUS will manage a monthly System Maintenance Review Meeting that will focus on a review of all plans for system maintenance discussed and agreed upon with the State in the annual maintenance schedule. A monthly status report will be created that includes a status of reference file update projects, progress toward existing and pending project activities, including impacts on any other ongoing projects and any other critical project information.

The status report will be used to guide the monthly System Maintenance Review Meetings that will cover the following topics:

- Programmatic and/or configuration revisions, additions, and deletions addressing DPHHS-specific upgrades, fixes, and enhancements
- Infrastructure upgrades, fixes, and enhancements that MAXIMUS is implementing that may impact the MAXIMUS Provider Services solution and/or its overnight batch cycle
- Upgrades, changes, and enhancements being implemented to meet and maintain Centers for Medicare and Medicaid Services (CMS) certification requirements
- Review and update of a System Maintenance Issue Log; MAXIMUS will post this updated log to the shared project repository weekly within 48 hours following the meeting

Regardless of the size of the system maintenance projects, MAXIMUS will continue to use the formal processes defined during the Transition period to control defect reporting, system modification, testing, and implementation. Regardless of the cause of the issue, use of standardized processes will verify we adequately manage system changes in the future.

System Enhancements

> System Enhancements
>
> DPHHS defines systems enhancements as follows:
>
> 1. System enhancements exclude any activities defined in "Maintenance" above.

2. New features or functionality that fall outside the scope of all RFP requirements, Offeror's RFP response, the contract, or agreements of any supplemental negotiations.

The State must approve both the design and level of effort prior to the start of development or configuration for system enhancements. DPHHS must approve any changes to the design or level of effort that occur after the original approval. The level of effort billed cannot exceed the level of effort approved by DPHHS. The level of effort incurred to complete an enhancement will be applied to the System Enhancement Pool once the enhancement is implemented and approved by the Department. If the level of effort exceeds the System Enhancement Pool hours remaining, the Department may choose to utilize hours from the next Contract operations year or have the Contractor invoice the Department for the balance at the rates defined in Attachment G, Provider Pricing Schedules, Schedule E – Resource Hourly Rates.

The Contractor must provide an estimate of any impact to annual operations cost, for the enhancement during the operations phase of the Contract if applicable. Reimbursements for any additional operations costs must be addressed in a contract amendment.

Our enhancement support procedures will be similar to those used during the system implementation phase of the MAXIMUS Provider Services solution. Our enhancement support processes provide for the following types of activities:

- Identification and definition of new requirements
- Design, development, testing, documentation, and implementation activities associated with maintaining the system
- Implementation of enhancements
- Activities required to track approved modifications and report status and progress to DPHHS

Responding to system enhancements is a critical component of our overall technical support and maintenance approach. MAXIMUS recognizes the importance of tracking hours expended for system enhancements during the operations support period separately from staff hours expended to provide routine support for the system.

As such, once DPHHS submits an enhancement request, MAXIMUS will perform detailed analysis to assess the estimate of the change in terms of requirements gathering, design, development, testing, implementation, and oversight. We will present recommendations including alternate approaches to meet the State's needs. We will present the analysis results to the State, in accordance with the State approved Change Management Plan. No further work will begin on the enhancement until DPHHS has approved the change in writing and prioritized the updates for a future release.

Enhancements for major system releases will follow our full SDM, which includes Release Planning, Requirements Definition, Design, Development, Testing, and Implementation. The MAXIMUS approach to system maintenance and enhancement is based on an incremental build methodology based upon an iterative configuration. For each system enhancement, MAXIMUS will provide a design document to the State for review. We understand the State has the right to reject modifications that do not meet State-defined requirements. Our development approach and standards follow a structured, repeatable development cycle, with each development stream producing independent functional components we promote through development and testing as we identify system changes during the requirement definition sessions. We anticipate enhancement design documents that are well aligned with State requirements.

System Enhancement Pool – DDI Base

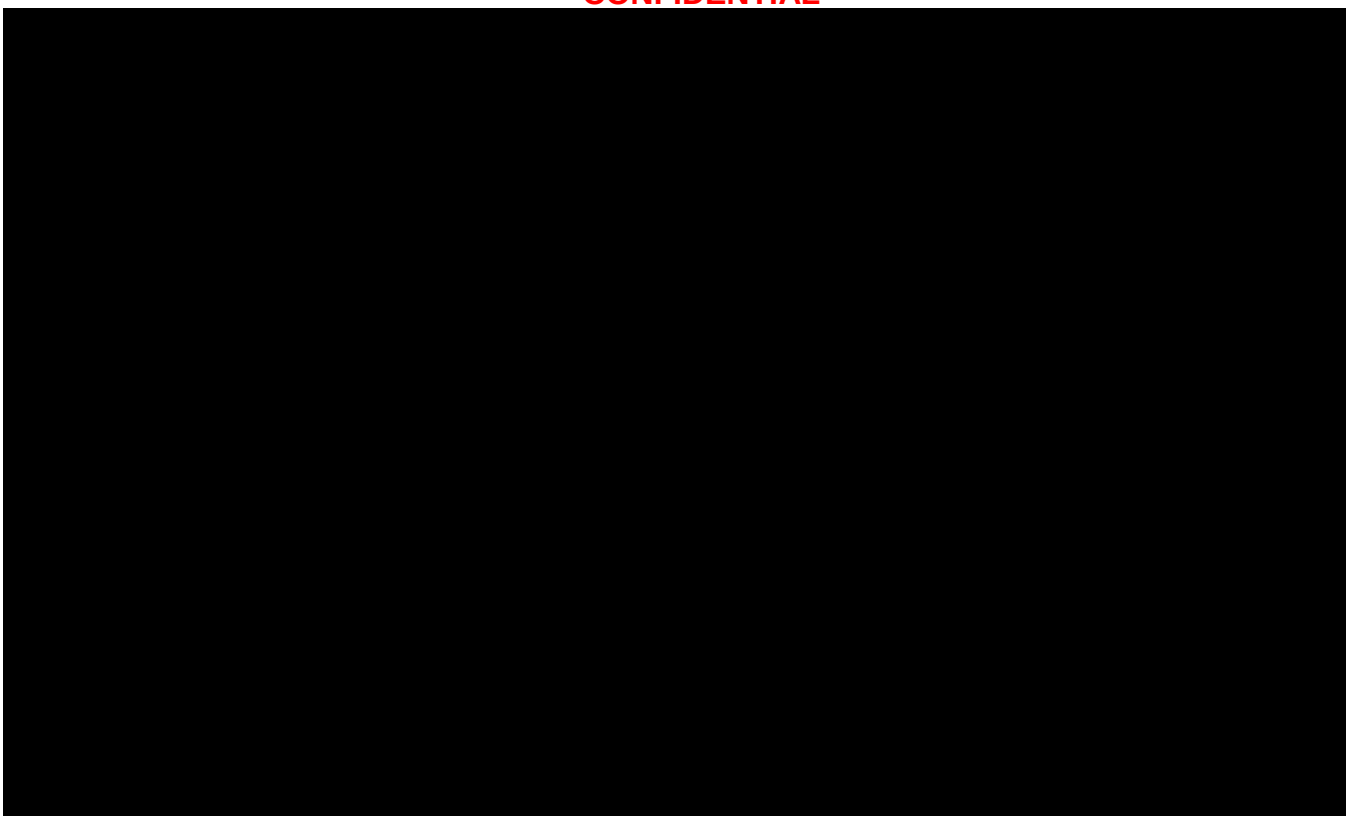
> System Enhancement Pool
>
> DPHHS recognizes that enhancements to the solution may be required periodically throughout the life of the contract to meet mandated Federal or State rules or regulations or to provide increased efficiency in operations or promote cost savings. The Contractor will add resources as necessary to complete enhancements by the required due date.
>
> System Enhancement Pool for DDI Base Scope of Work
>
> The Contractor will provide 1,500 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 1,500 system enhancement pool hours are included in the offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.
>
> The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one-month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

MAXIMUS appreciates the evolving nature of federal and state requirements for provider enrollment that might require a systems enhancement. Enhancements may also be needed to make the system more efficient or streamlined. We plan for these enhancements and follow the approach in our agreed change control process.

We carefully track the hours expended on enhancements. These hours are captured in our Jira tool and are categorized by activity: design, development, and testing. Staff members are required to enter these hours in the Jira tool, shown in *Exhibit 3.10.4-5: Jira Work Tracking*. We use this mechanism to track the 1500 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of those hours is included in our fixed price and in Schedule D-Enhancement Pool Hours.

Effective and accurate tracking is essential as any unused system enhancement pool hours will be rolled over to the pool for Operations or may be adjusted downward at the discretion of the State with a one-month notification and with the cost of the contract reduced proportionally.

CONFIDENTIAL



System Enhancement Pool – DDI Option A

> System Enhancement Pool for DDI Option A Scope of Work
>
> The Contractor will provide 500 system enhancement pool hours for the duration of the DDI phase of the contract for the Option A Scope of Work. The cost of these 500 system enhancement pool hours are included in the offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.
>
> The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one-month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

We will use the Jira tool to track the 500 system enhancement pool hours for the DDI phase of the contract, Option A Scope of work. The cost of those 500 hours is included in our fixed price and in Schedule D-Enhancement Pool Hours. Enhancements require the skills of many personnel, including business analysts, developers, and testers. The cost of all these roles is included in the system enhancement pool.

Effective and accurate tracking is essential as any unused system enhancement pool hours will be rolled over to the pool for Operations or may be adjusted downward at the discretion of the State with a one-month notification and with the cost of the contract reduced proportionally.

System Enhancement Pool – DDI Option B

> System Enhancement Pool for DDI Option B Scope of Work
>
> The Contractor will provide 250 system enhancement pool hours for the duration of the DDI phase of the contract for the Option B Scope of Work. The cost of these 250 system enhancement pool hours are included in the offeror's fixed price and

included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort.

The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one-month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.

We will use the Jira tool to track the 250 system enhancement pool hours for the DDI phase of the contract, Option B Scope of work. The cost of those 250 hours is included in our fixed price and in Schedule D-Enhancement Pool Hours. Enhancements require the skills of many personnel, including business analysts, developers, and testers. The cost of all these roles is included in the system enhancement pool.

Effective and accurate tracking is essential as any unused system enhancement pool hours will be rolled over to the pool for Operations or may be adjusted downward at the discretion of the State with a one-month notification and with the cost of the contract reduced proportionally.

System Enhancement Pool – Operations Base

System Enhancement Pool for Operations Base Scope of Work

The Contractor will provide 500 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 500 system enhancement pool hours are included in the Offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D – Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G, Provider Pricing, Schedule D – Enhancement Pool Hours.

We will use the Jira tool to track the 500 system enhancement pool hours for the operations phase of the contract per operations year. The cost of those 500 hours is included in our fixed price and in Schedule D-Enhancement Pool Hours. Enhancements require the skills of many personnel, including business analysts, developers, and testers. The cost of all these roles is included in the system enhancement pool.

Effective and accurate tracking is essential as any unused system enhancement pool hours may be rolled over to the next operations year, or may be adjusted downward at the discretion of the State with a one-month notification and with the cost of the contract reduced proportionally.

System Enhancement Pool – Operations Option A

System Enhancement Pool for Operations Option A Scope of Work

The Contractor will provide 100 system enhancement pool hours during the Operations phase per operations year for the Option A Scope of Work. The cost of these annual 100 system enhancement pool hours are included in the Offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.

Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D – Enhancement Pool Hours. The cost of the

> contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G, Provider Pricing, Schedule D – Enhancement Pool Hours.

We will use the Jira tool to track the 100 system enhancement pool hours for the operations phase per operations year for the Option A Scope of Work. The cost of those 100 hours is included in our fixed price and in Schedule D-Enhancement Pool Hours. Enhancements require the skills of many personnel, including business analysts, developers, and testers. The cost of all these roles is included in the system enhancement pool.

Effective and accurate tracking is essential as any unused system enhancement pool hours may be rolled over to the next operations year, or may be adjusted downward at the discretion of the State with a one-month notification and with the cost of the contract reduced proportionally.

System Enhancement Pool – Operations Option B

> System Enhancement Pool for Operations Option B Scope of Work
>
> The Contractor will provide 100 system enhancement pool hours during the Operations phase per operations year for the Option B Scope of Work. The cost of these annual 1500 system enhancement pool hours are included in the Offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort.
>
> Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D – Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G, Provider Pricing, Schedule D – Enhancement Pool Hours.
>
> The Offeror must describe their approach to meet each of the detailed Operations, Maintenance, and Configuration requirements defined in Attachment F, Requirements Matrix.

We will use the Jira tool to track the 100 system enhancement pool hours for the operations phase per operations year for the Option B Scope of Work. The cost of those 100 hours is included in our fixed price and in Schedule D-Enhancement Pool Hours. Enhancements require the skills of many personnel, including business analysts, developers, and testers. The cost of all these roles is included in the system enhancement pool.

Effective and accurate tracking is essential as any unused system enhancement pool hours may be rolled over to the next operations year, or may be adjusted downward at the discretion of the State with a one-month notification and with the cost of the contract reduced proportionally.

Operations, Maintenance, and Configuration Requirements

The following table includes Attachment F Operations, Maintenance, and Configuration Requirements, and our summarized response to each requirement, which can be found in more detail in this section.

ID	Operations, Maintenance, and Configuration Requirement	MAXIMUS Summarized Response
OMC01	The Contractor shall cooperate and assist the Department in responding to all law enforcement, federal and State audit and review requests. The Contractor shall provide audit support including, random sample generation, data extracts, hard-copy documents, and provide any requested data or information.	We understand the support the State may need from MAXIMUS and the MAXIMUS Provider Services solution in the event of potential litigation and investigation actions. "Support" could take the form of supplying data, providing audit trails, or testifying in depositions or in court. The solution maintains data for an indefinite period and is easily retrievable in the form of an ad hoc query within the parameters defined by the State.
OMC02	The Contractor shall support the disaster recovery activities that will provide timely failover and create relevant documented policies and procedures to implement a recovery.	MAXIMUS understands the importance of a comprehensive Business Continuity and Contingency Plan/Disaster Recovery (DR) Plan to address how we will recover from a disaster that impacts our primary data center or network and continue the processing enrollments and updates for Providers within the MAXIMUS Provider Services solution. As a major Health and Human Services vendor with many mission critical applications, MAXIMUS has extensive experience in architecting disaster recovery solutions for applications like our solution. The DR plan discusses the methodology and approach for a successful failover to the DR site in the event the production system is rendered inoperable.
OMC03	The Contractor shall conduct an annual test of the Disaster Recovery and Business Continuity Plan and submit the Disaster Recover/Business Continuity Test Report that includes the outcome, corrective action plan, and revisions, if any, to the Department.	MAXIMUS DR plan will include all the steps necessary to complete the recovery of affected systems from a disaster. Our experience during the annual tests will confirm we are able to recover the entire system within the timeframes specified in our DR Plan. The DR Test Report includes the outcome, corrective action plan and any revisions to the Department.

ID	Operations, Maintenance, and Configuration Requirement	MAXIMUS Summarized Response
OMC04	The Contractor shall provide Operations support, Maintenance, and ongoing Configuration of the provided Solution(s) throughout the life of the Contract. This includes providing Operations support as described in the scope of work as well as providing Maintenance and Enhancements to the provided Solution(s). The Contractor will follow project management and system development processes throughout the life of the Contract. The Agency defines maintenance for each module as follows: 1. Making configuration updates as requested by the State. Configuration includes changes to table values, parameters, codes, and business logic, including hardcoded business logic. 2. Correcting deficiencies (defects) found in the solution(s) based on detailed requirements described in the scope of work and published design specifications. 3. Correcting deficiencies (defects) found in the solution(s) based on a failure to meet the detailed requirements in completed enhancement, configuration or maintenance requests. 4. Conducting research requested by the State or required to support the Department. For example: a. System behavior and results b. New healthcare initiatives c. Best practices research across states and industry d. Impacts of new State and federal legislation 5. Performing mass adjustments or mass changes as requested by the State or required to support the State's healthcare programs (for example, errors in pricing, eligibility, cost share, and financial code assignments, TPL discovery, and provider reimbursement changes). 6. Performing regular maintenance as needed by the State required to support the State's healthcare programs. Examples of maintenance include but are not limited to: a. Performance optimization. b. Database management. c. Software, hardware, and tools (e.g., patches, upgrades, and replacement). d. Interface, report, and correspondence changes. e. Making corrections or changes to maintain the integrity of the system or the data within it (e.g., backing out changes, correcting duplicate records, cleansing corrupt data, adding security measures, adding redundancy). 7. Using appropriate testing, configuration, and change control procedures. 8. Updating system, user, and training documentation and online help to reflect changes that have been made to the solution. 9. Performing the activities above to maintain customizations implemented as part of an approved enhancement. 10. Perform incremental integration services via configuration. Incremental integration services should be included in the DDI costs.	Throughout the life of the contract, MAXIMUS will provide operations support, maintenance, and enhancements of our solution following the established project management and systems development processes. Our approach to correcting deficiencies and implementing enhancements may be based on State requests for configuration updates to table values, parameters, codes, and business logic. As stated elsewhere in this section, our approach to correcting deficiencies (defects) found in the solution is based on detailed requirements or a failure to meet the detailed requirements in completed enhancement, configuration, or maintenance requests. We may also conduct research requested by the State or required to support the department for items such as system behavior and results, new healthcare initiatives, best practices research from across the states and industry and impacts from new State or federal legislation. We will also perform mass adjustments or mass changes as requested by the State or required to support the State's healthcare programs. The State may also require regular maintenance to support the healthcare programs, such as performance optimization, database management, software, hardware, and tools; interface, and report and correspondence changes. There may also be corrections or changes to maintain the integrity of the system or the data within it, such as backing out changes, correcting duplicate records, cleansing corrupt data, or adding security measures or redundancy. As with other build efforts, MAXIMUS follows established processes for controlling the design, configuration, testing, and release of enhancements and defect remediation, including change control. Part of this process includes updating system, user and training documentation and affected online help to reflect the changes. Process is important to maintain customizations implemented as part of the approved enhancement. We understand that incremental integration may be necessary to accommodate other modules. These will be considered either enhancements or maintenance, depending on whether the item in our solution is configurable. Incremental integration services are included in the DDI costs.
OMC05	The Contractor shall provide a notification web page that displays when the system is unavailable for scheduled maintenance or unscheduled outages.	MAXIMUS Provider Services solution displays a message to users trying to access the system in the unlikely event of an unplanned outage or during scheduled maintenance.

ID	Operations, Maintenance, and Configuration Requirement	MAXIMUS Summarized Response
OMC06	The Contractor shall have processes in place to restrict access when inappropriate system access or misuse is detected.	The MAXIMUS Provider Services solution requires a password reset after 3 failed login attempts. The system also provides an on demand report that lists users that have been requested to reset their passwords.
OMC07	The Contractor shall test and implement all production ready patches, upgrades, and releases for all software, firmware and operating systems in a timely manner, in coordination with other modules.	The MAXIMUS Project Manager and Technical Manager will work with the State Contract Administrator and other managers to plan releases and determine which tasks (errors, enhancements, and Ad Hoc requests) are to be implemented in each release in coordinate with other modules. Following our established development processes, we will create a system test plan for each release, as well as make updates to the training materials per the training plan. In addition, release planning will determine the actual date upon which the release will take place and will have to account for time necessary to System Test and User Acceptance Test system modifications, prior to implementation in a release. The State Contract Administrator will approve each release before it is actually implemented.
OMC12	The Contractor shall notify the appropriate user community, as defined by the State, of system events (e.g., major system changes and system outages).	For planned system outages, we notify the State in advance. A maintenance page is put up for providers accessing the system during the outage.
OMC15	The module Contractor shall provide help desk services to provide level 0 (customer self-service) level 1(basic support), level 2 (moderate support) that includes as appropriate, escalation to the State and level 3 (technical/integration) support related to the functionality of the module's scope of work. Level 1 help desk is the first point of contact and is responsible for logging the issue and, if possible, assisting the user.	Based on our experience in other operations, MAXIMUS is accustomed to providing help desk services, including following escalation processes as necessary. Level 0 (customer self-service) support is available using online help text and user manuals. Level 1 basic support is provided through an online chat function or telephone call where the issue is logged and the if possible, the user is assisted. Moderate support may include escalation to the State. We provide level 3 support following the established procedure of staff submitting tickets to the technical team for triage and prioritization.
OMC16	The Contractor shall provide online help for external and internal users.	The MAXIMUS Provider Services solution offers accordion style online help to providers by embedding the help text within the actual web page enrollment forms for quick reference. The solution also contains field level help text as well as field level error messages.
OMC17	The Contractor shall provide 1,500 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 1,500 system enhancement pool hours are included in the offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort. The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.	MAXIMUS agrees to the terms to provide 1500 system enhancement pool hours during the DDI phase. The cost of these hours is included in the fixed price in Attachment G and Schedule D and includes personnel costs. Any unused hours will be rolled over to the enhancement pool for Operations or adjusted downward at the discretion of the State but with a one-month notification and with a proportional cost reduction.

ID	Operations, Maintenance, and Configuration Requirement	MAXIMUS Summarized Response
OMC18	The Contractor shall notify the Department when updated reference materials (e.g., Requirements Matrices, Manuals, System Documentation, System Design Documentation, User Documentation, Business Rules Catalog, and Training Materials) are available for review.	MAXIMUS updates manuals and other system documentation when the solution changes. We will notify the Department when these materials are available for review.
OMC19	The Contractor shall provide 24x7 access to the Department for all reference materials (e.g., Requirements Matrices, Manuals, System Documentation, System Design Documentation, User Documentation, Business Rules Catalog, and Training Materials).	Project materials will be stored on a Sharepoint site that is accessible 24x7. Online manuals are available 24x7 on the solution website.
OMC21	The Contractor will provide 500 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 500 system enhancement pool hours are included in the Offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort. Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours.	MAXIMUS agrees to provide 500 systems enhancement pool hours during the operations phase per operations year at a cost included in the fixed price and in Attached G and Schedule D. The unused pool hours will be rolled forward to the next operations year or adjusted downward at the discretion of the State with a one-month notification by the State of any reduction. The cost of the contract would be reduced proportional to the cost of the reduction in system enhancement pool hours using the rates in the proposal.
OMC22	The Contractor shall provide 500 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 500 system enhancement pool hours are included in the offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort. The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.	MAXIMUS agrees to provide 500 systems enhancement pool hours during the DDI phase at a cost included in the fixed price and in Attached G and Schedule D. The unused pool hours will be rolled forward to the next operations year or adjusted downward at the discretion of the State with a one-month notification by the State of any reduction. The cost of the contract would be reduced proportional to the cost of the reduction in system enhancement pool hours using the rates in the proposal.
OMC23	The Contractor will provide 100 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 100 system enhancement pool hours are included in the Offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort. Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G Pricing Schedule, Schedule D-Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours.	MAXIMUS agrees to provide 100 systems enhancement pool hours during the operations phase per operations year at a cost included in the fixed price and in Attached G and Schedule D. The unused pool hours will be rolled forward to the next operations year or adjusted downward at the discretion of the State with a one-month notification by the State of any reduction. The cost of the contract would be reduced proportional to the cost of the reduction in system enhancement pool hours using the rates in the proposal.

ID	Operations, Maintenance, and Configuration Requirement	MAXIMUS Summarized Response
OMC24	The Contractor will provide 250 system enhancement pool hours for the duration of the DDI phase of the contract. The cost of these 250 system enhancement pool hours are included in the offeror's fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool for DDI includes personnel cost for all resources supporting the system enhancement effort. The unused system enhancement pool hours for DDI will be rolled over to the system enhancement pool for Operations or the number or system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for DDI will require one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G, Provider Pricing Schedules, Schedule D-Enhancement Pool Hours.	MAXIMUS agrees to provide 250 systems enhancement pool hours during the DDI phase at a cost included in the fixed price and in Attached G and Schedule D. The unused pool hours will be rolled forward to the next operations year or adjusted downward at the discretion of the State with a one-month notification by the State of any reduction. The cost of the contract would be reduced proportional to the cost of the reduction in system enhancement pool hours using the rates in the proposal.
OMC25	The Contractor will provide 100 system enhancement pool hours during the Operations phase per operations year. The cost of these annual 100 system enhancement pool hours are included in the Offeror's fixed price and included in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all staff supporting the system enhancement effort. Unused system enhancement pool hours for each year of operations may be rolled forward to the next operations year or the number of system enhancement pool hours may be adjusted downward, at the discretion of the State. Any reduction in the number of system enhancement pool hours for operations will require a one month notification by the State, and the cost of the contract will be reduced proportional to the cost of the reduction in system enhancement pool hours eliminated using the rates provided in Attachment G Pricing Schedule, Schedule D-Enhancement Pool Hours. The cost of the contract will be reduced proportional to the cost of the unused hours using the rates provided in Attachment G Pricing Schedules, Schedule D-Enhancement Pool Hours.	MAXIMUS agrees to provide 100 systems enhancement pool hours during the operations phase per operations year at a cost included in the fixed price and in Attached G and Schedule D. The unused pool hours will be rolled forward to the next operations year or adjusted downward at the discretion of the State with a one-month notification by the State of any reduction. The cost of the contract would be reduced proportional to the cost of the reduction in system enhancement pool hours using the rates in the proposal.

3.10.5 Key Personnel and Resources

Our named key personnel have extensive experience with modular Provider Services system development and implementation, along with a history of successful project management engagements. As the only vendor with three installed instances of a Medicaid Provider Services module, our key personnel have the most experience with the challenges inherent in adopting new technology within a legacy environment. The Provider module implementation is early in the MPATH timeline and is among the first to test the structure and governance of the enterprise; laying the foundation for the modules to come. Our key personnel have the experience, the Medicaid program expertise and the technical skills to ensure a successful implementation of the Provider Services Modules and to also assist the State and the other partners with the implementation of the MPATH enterprise.

> 3.10.5 Key Personnel and Resources
>
> The Offeror must provide key personnel to be assigned to the DDI and Certification phases of the project. At a minimum, key personnel shall include a Project Manager, Contract Manager, Testing Lead, Integration Lead and a Certification Lead. DPHHS will review and approve all key personnel.
>
> The Offeror shall provide key personnel for the Operations, Maintenance and Configuration phase of the Project. At a minimum, key personnel shall include a Project Manager, Technical Manager and a Contract Manager. The Offeror must identify other key personnel for the Operations, Maintenance and Configuration phase of the project. DPHHS will review and approve all key personnel.
>
> For all phases of the Project, the Offeror's Project Manager will be required to perform work at the Primary Project location (Helena, Montana) unless approved by DPHHS to work remotely. Other Offeror staff working remotely, must be available to

> work in Helena, Montana at the Department's request for functions necessary to support the scope of work (e.g., risk review meetings, root cause analysis sessions, integration planning, release planning, operational readiness reviews, UAT, implementation, and production deployment). For any work performed at a location other than the Helena, Montana, the Offeror must identify the specific location (city, state, country), describe the type of work to be performed, and the percent of the total hours for that type of work at that location.
>
> The Offeror must propose a staffing approach to meet each of the requirements detailed in Attachment F, Requirements Matrix.

After a careful review of the RFP requirements, we have assembled an excellent team for the Provider Services Solution project that brings the complementary background and experience necessary to meet the diverse program management, business, and technical skills required in the RFP.

As we establish our team, we identify specific staff roles and responsibilities for everyone involved in the Project and incorporate relationships, activities, and touch points for personnel that help prevent "work silos" and inefficiencies. We assign key personnel to positions that are critical to the success and oversight of the project and define additional staff positions to be filled by staff who meet the specific qualifications at the time the project begins. We assign these senior staff members before the project begins and we use their skills continually throughout the project, ensuring continuity throughout the duration.

Our team possesses the following skill sets:

- Senior project oversight staff with extensive senior management leadership qualifications, significant Medicaid provider management qualifications and Project Management Professional (PMP) certifications to provider senior project leadership and oversight
- Project management staff with a diverse mix of project management, Medicaid and technical qualifications to implement the required processes, to manage the activities appropriately and timely, and to provide overall project leadership to the business and technical teams
- Technical management staff with experience leading and advising multi-discipline technical teams
- System development staff, including functional and technical experts in Provider Services, Medicaid, and system development and implementation to maintain, operate, and enhance the various releases throughout the life of the program
- Supplemental expertise in system infrastructure and hosting, training program development and execution, and a wide variety of technology expertise in reporting platform implementation

We augment the main project team with data center and enterprise network experts to provide a reliable infrastructure that supports system development and testing along with connectivity with the Montana infrastructure. We also recognize the need to have Security and Privacy experts to validate compliance with the wide array of state and federal requirements in these areas. We have also included a Compliance Manager in our organization to make certain adherence to the many SLAs is assured.

MAXIMUS has reviewed the requirements listed in RFP Section 3.10.5. The key staffing requirements directly align with the staffing model we use for Provider Services modular implementations. We have assigned staff to each key staff position and identified additional key staff members for positions that are pivotal for success. These named key staff positions are available for DDI and Certification. Our staffing approach also, provides continuity of staff as we move from DDI to Operations, Maintenance, and

Configuration of the system. We understand that DPHHS will review and approve all key positions and are confident that DPHHS will accept our qualified staff.

The MAXIMUS key staff model contains the following components:

- For the DDI and Certification phases, we will provide key personnel, including a Project Manager, Contract Manager, Testing Lead, Integration Lead, and a Certification Lead. We have also proposed a Business Analyst Lead and two Development Leads because we understand the importance of these roles to the project.
- For the Operations, Maintenance and Configuration phase, we will provide key personnel, including a Project Manager, Technical Manager, and a Contract Manager. We anticipate moving staff from the DDI phase of the project to fill these positions to provide continuity and support our ability to maintain the solution in production.
- For all phases of the Project, our Project Manager will perform work at the Primary Project location (Helena, Montana for the Montana contract) unless approved by DPHHS to work off-site. The Business Analyst Lead will also perform work onsite and is readily available to meet with the State.
- MAXIMUS employs a work-at-home model for many of our professional staff. We secure network connectivity using a VPN and have corporate policies and procedures in place to enforce security and privacy requirements. The majority of our development team is located in the Denver, Colorado area and we can easily collaborate in our corporate office in that location. At project start, we will identify the specific work location (city, state, country), describe the type of work to be performed, and the percent of the total hours for that type of work at that location.
- Our remote staff will be available to work in Helena, Montana, at the Department's request, for functions necessary to support the scope of work. We plan to have key personnel on site for requirements review, gap analysis walkthrough, and the multitude of design reviews. We also support testing, operational readiness and implementation with onsite resources. MAXIMUS will work closely with DPHHS to identify and schedule onsite visits as required to for the project.

In the following subsections, we provide a detailed discussion of our staffing approach, key personnel, and resources allocation.

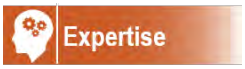
Staffing Approach

> The Offeror must propose a staffing approach to meet each of the requirements detailed in Attachment F, Requirements Matrix.

We have assembled an excellent team for the Montana MPATH Provider Services Module project which brings the complementary skills necessary to meet the diverse program management, business and technical skills required in the RFP. Included in the MAXIMUS Team are experienced staff from our partners at Microassist which bring depth and expertise to the team. Our team possesses the following skill sets:

- A Contract Manager with extensive senior management leadership qualifications, significant Medicaid provider management qualifications and Project Management Professional (PMP) certification

- A PMP-certified Project Manager with a diverse mix of project management, Medicaid, and technical qualifications; and experience in Montana with the Department of Labor, Technology Services Division
- Our PMP-certified Provider Services Solution Architect has extensive Medicaid and Human Services system development experience and is responsible for coordinating all updates to our solution platform across all projects
- Our system development staff includes functional and technical experts in Provider Services, Medicaid, and system development and implementation; they will maintain, operate, and enhance the various releases throughout the life of the program
- Supplemental expertise through Microassist in training program development and execution
- Expertise in security and privacy standards, requirements, and audits led by our Chief Security Officer and our Privacy Official
- Expertise in the delivery of business operations, contact centers, and customer support through our Standardized Operations and Analytics (SOA) practice



MAXIMUS selected the project team for this engagement specifically for the skills and abilities they possess. We are veterans of working with government agencies in highly dynamic and political environments. We offer Montana a valuable real-world understanding of the need for new advanced provider solutions and for understanding how the resulting processes improve healthcare availability and outcomes. We also bring an important understanding of the provider community, the functionality of the Medicaid support systems (including the MMIS) and federal policy regarding the Medicaid program. No other vendor can match our qualifications in bringing modular Medicaid provider services solutions to a variety of states. Our staff are veterans of these projects; adding valuable real life knowledge to our delivery team.

Montana Provider Services Module Project Organizational Structure

The organization chart shown in *Exhibit 3.10.5-1: MAXIMUS Proposed Organizational Chart for Provider Services Module* depicts the proposed MAXIMUS organizational structure for this project which includes all phases, as well as Options A and B Services. As part of our delivery solution, we integrate the plans for the base system and both Options into a single delivery organization. MAXIMUS utilizes this best practice so that all components are implemented using the same schedule that more effectively supports requirements review, testing, disaster recovery, and operational readiness.

CONFIDENTIAL

MAXIMUS has a keen understanding of the staff requirements necessary to support the operational functions, systems, and data interfaces needed for this project. Our experienced project team under the direction of our Contract Manager; who is a nationally recognized Medicaid systems expert, gives the State confidence that we have provided the level of staff necessary so the State can effectuate its promise to deliver excellent services to its providers while enabling new technology and advanced business processes.

In the event Option A Provider Services is selected, MAXIMUS will integrate the additional team members into our base module team. By doing this, Option A functions will be designed and implemented as an integrated component of the base system with integrated deliverables and the certification plan.

If Option B Provider Services is also selected, MAXIMUS will provide the State with an integrated plan that includes both the system and operations infrastructure implementation components. We have

CONFIDENTIAL

extensive experience integrating our system and operational teams so we are able to maximize the base system organization to seamlessly incorporate the Option B components.

Our approach to implementing the options maximizes the existing team structure and minimizes the impact to the State by reducing the need to review different deliverables for the various options. We believe this approach reduces project risk and gives the State a more comprehensive view of the provider services module based on the options selected. Our team has experience in implementing the base system with or without the defined options so the state can be confident in our staffing model and plan.

Key Personnel

Our key personnel, who we describe in this section, are integral to effective delivery and management of this project. In addition to named key personnel, MAXIMUS will augment the project team with resources employed by the company who have the broad array of skills necessary to support the different business functions. These will include technical analysts and developers who will support system development, testing, and implementation tasks, and business analysts who will assist in the creation of the test plan and support integration testing and user acceptance testing with State staff. We will engage system architects, database administrators, security analysts, and infrastructure engineers to oversee the stability, security, and quality of the deployment. The structure and size of our company enables the project team to call on resources across the organization to support the implementation effort.

Each named key personnel will hold just one key role on the project unless otherwise approved by the Department. We anticipate moving key personnel from the DDI phase of the project to the Operations phase to provide continuity and so that knowledgeable staff are present as we move to production utilization of the module.

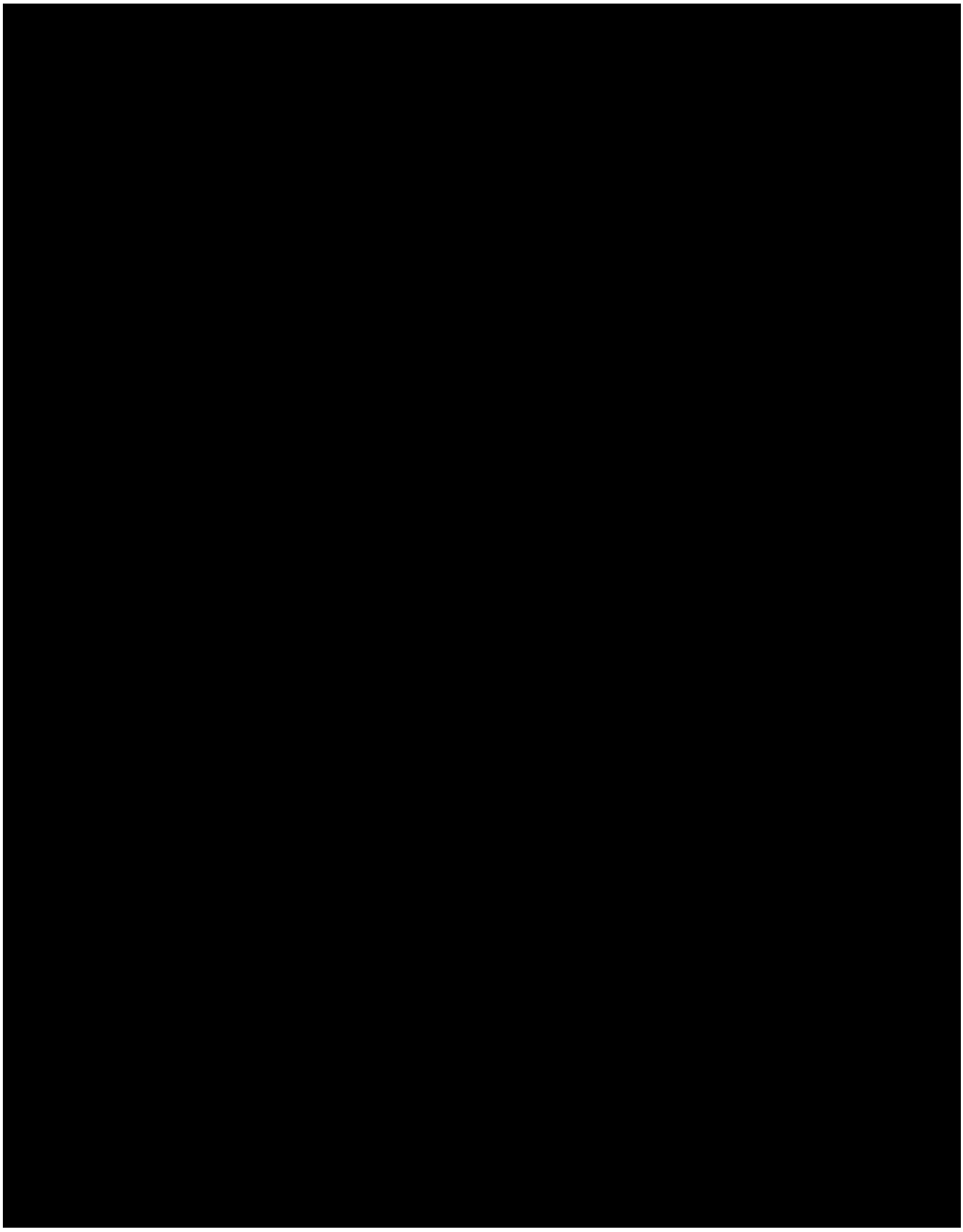
Following this section, we include a full resume for all key personnel, including project role, qualifications, and the years of experience, prior work experience, education, skills, certifications, and references.

All Phases

Across all phases of the Provider Services Module project, MAXIMUS is proposing the same Project Manager, Contract Manager, and Integration Lead / Technical Manager.

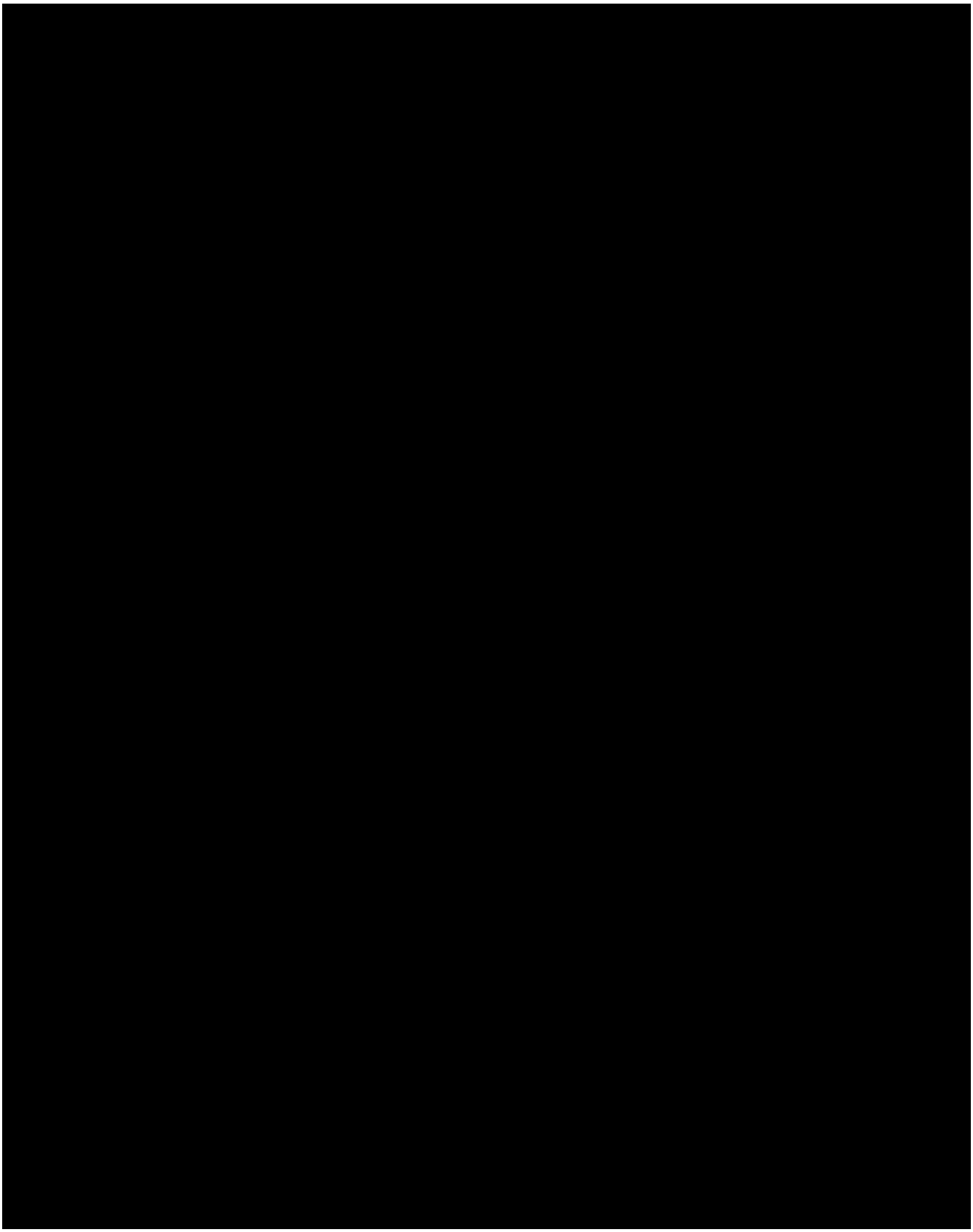
CONFIDENTIAL

CONFIDENTIAL



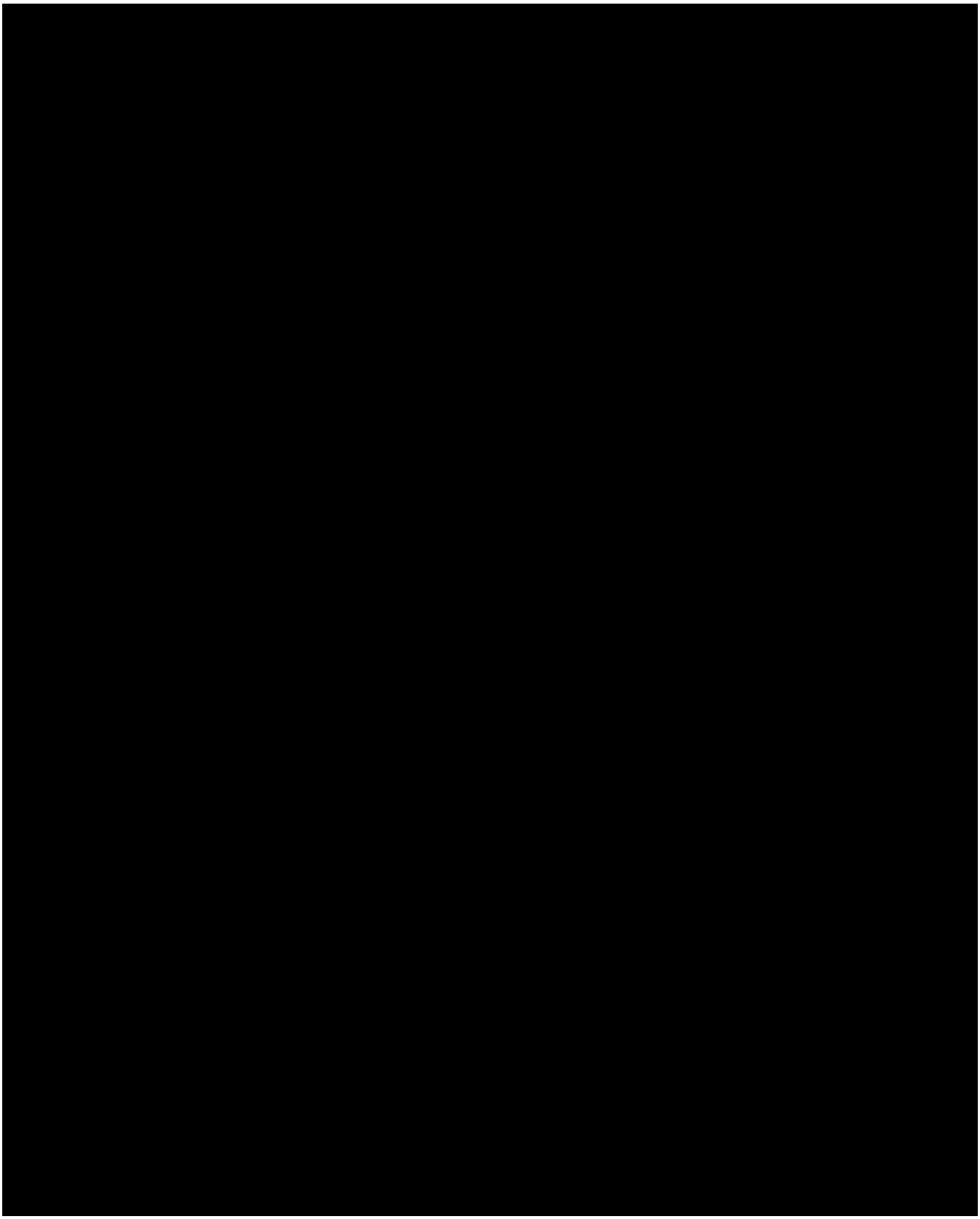
CONFIDENTIAL

CONFIDENTIAL



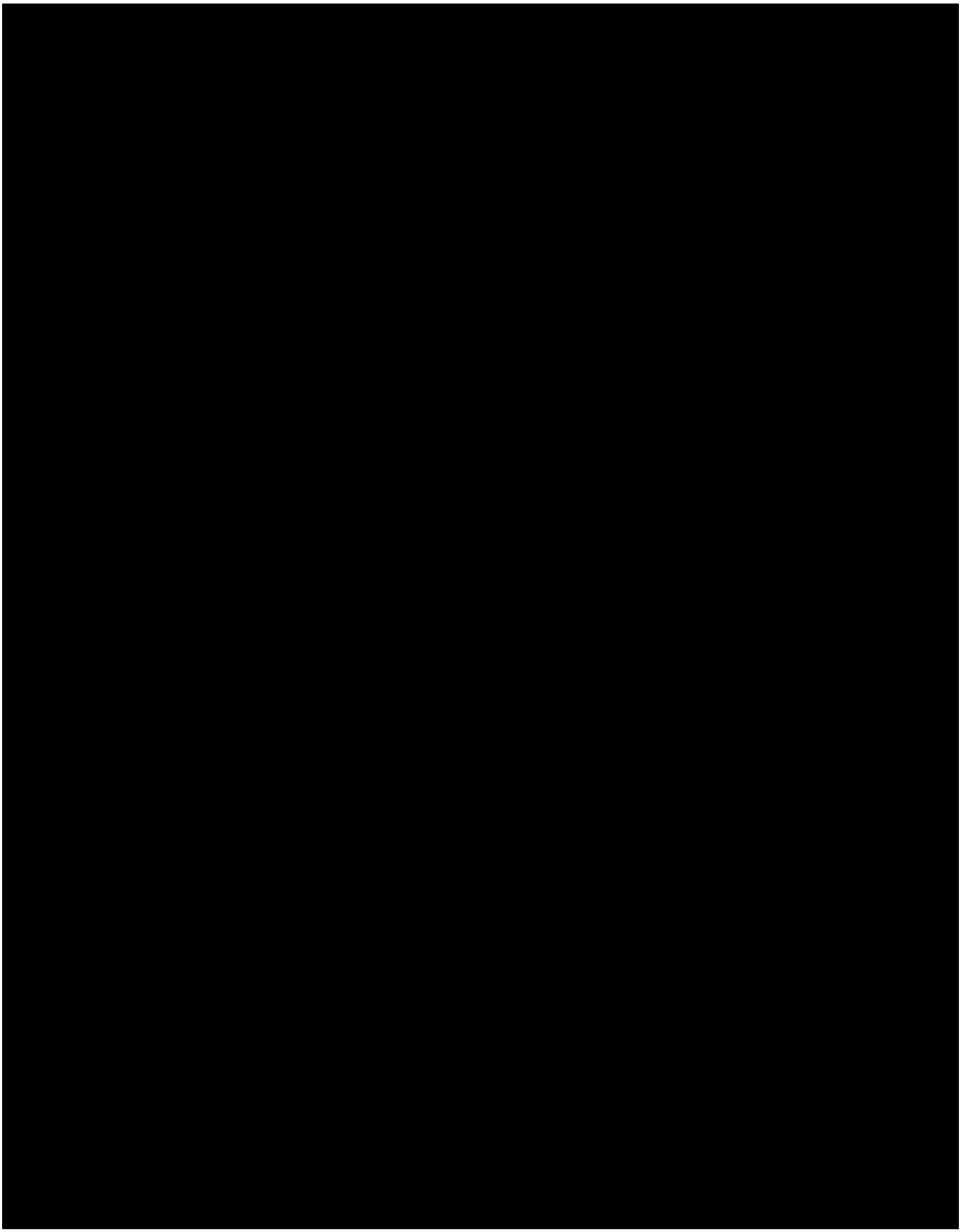
CONFIDENTIAL

CONFIDENTIAL



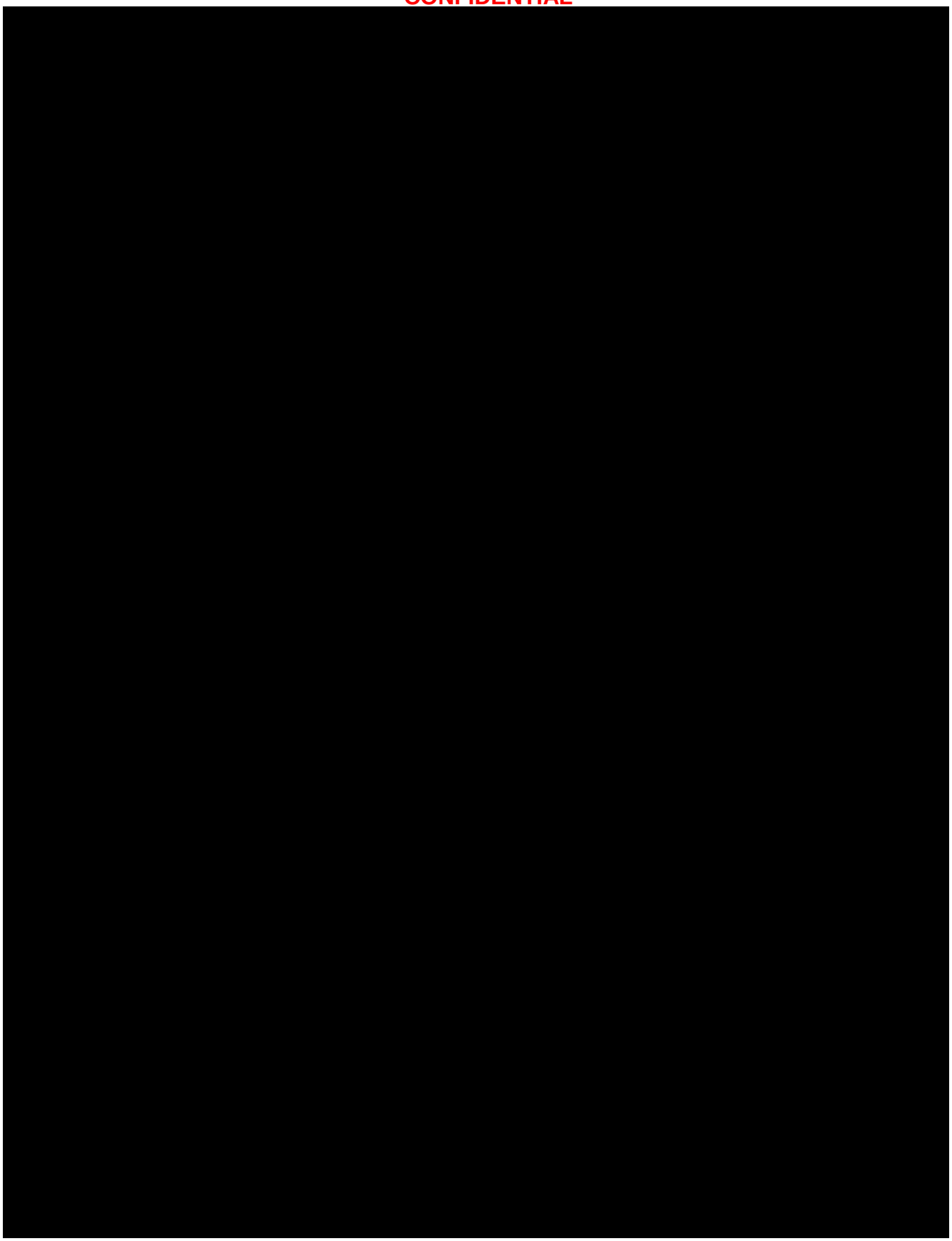
CONFIDENTIAL

CONFIDENTIAL



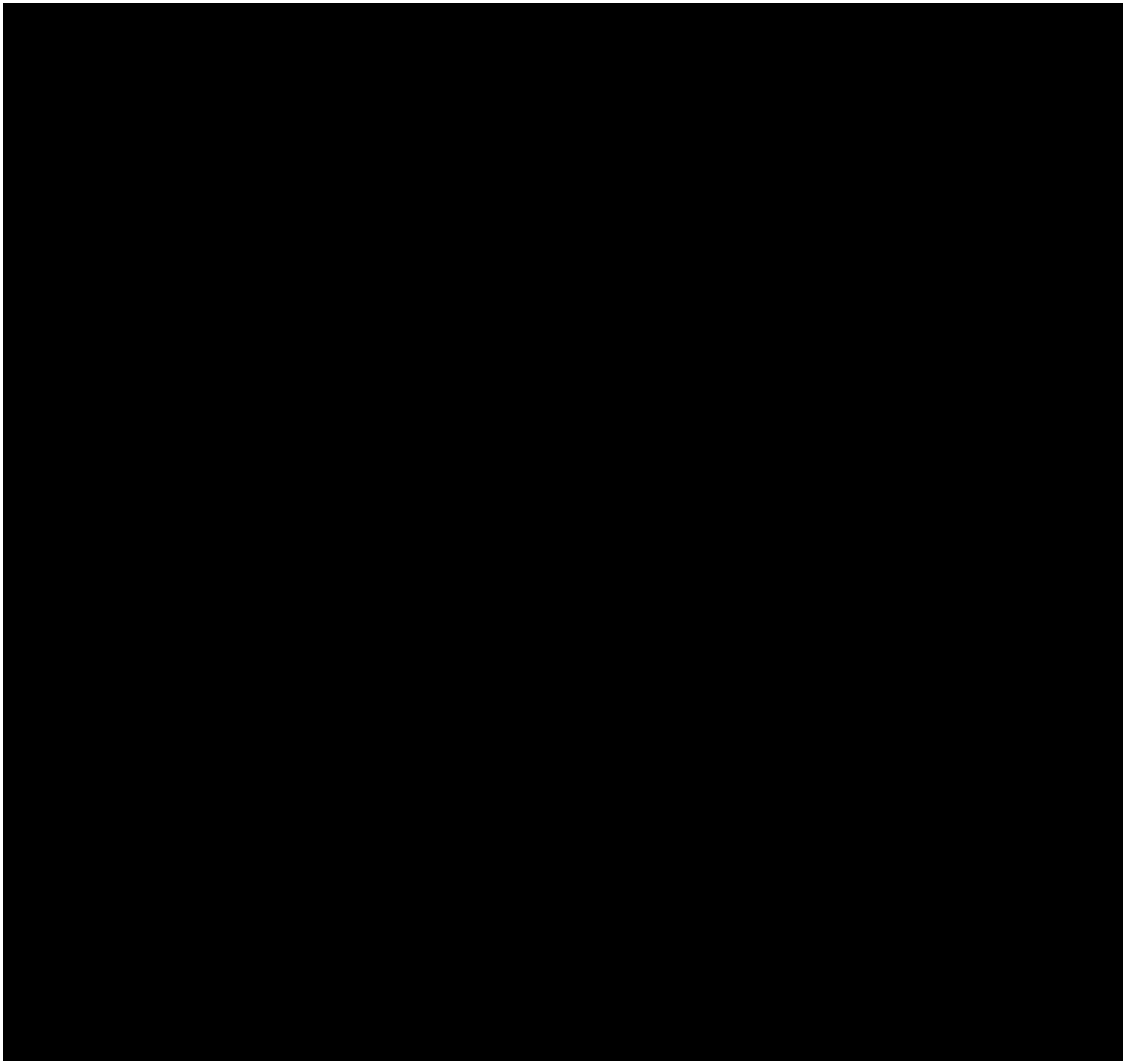
CONFIDENTIAL

CONFIDENTIAL



CONFIDENTIAL

CONFIDENTIAL



The MAXIMUS Hiring Process

From time to time, it is necessary to replace key personnel, or other staff members. If this occurs, MAXIMUS understands the timeline requirements for replacement of key personnel and commits to replacing key personnel with an equally qualified substitute. The MAXIMUS process for recruitment of new staff is comprehensive and designed to rapidly identify and onboard new hires.

Our end-to-end staffing process, from staff screening to staff management and retention, as illustrated in *Exhibit 3.10.5-2: MAXIMUS Staffing Approach*, enables timely recruitment, hiring, and training of qualified employees to adequately staff our projects efficiently regardless of fluctuating work volumes.

CONFIDENTIAL

Exhibit 3.10.5-2: MAXIMUS Staffing Approach. *We hire the most qualified staff members and provide them with the training and support needed to succeed at their job and provide our clients quality service.*

At MAXIMUS, we do more than simply hire qualified people — we empower our staff with the right structure, processes, and tools to achieve required and desired program outcomes. When we bring in new staff, we follow an established MAXIMUS approach to recruiting, hiring, and training project staff — an approach that has proven successful in quickly getting new team members on board and ready to serve clients. *Exhibit 3.10.5-3: MAXIMUS Hiring Process* shows the steps we take to identify and hire talented individuals for all our projects, including this Provider Services Module project.

Step 1: Identify Need

- Identify the recruitment need based on contractual requirements and performance and quality goals

Step 2: Recruiting Strategies

- Advertise job positions internally and externally via the internet, one-stops, and local community-based organizations
- Target advertising for special skills such as bilingual capabilities

Step 3: Job Descriptions

- Develop job description for all positions
- Develop specific qualification levels for each position
- Consider prior work experience, multi-lingual requirements, and education

Step 4: Receive and Screen Resumes

- Human Resources Recruitment Team reviews and screens all resumes
- Develop specific screening criteria for each staff position with preference given to those with prior relevant experience
- Reject resumes that do not meet minimum screening criteria
- Send a rejection letter to each candidate whose resume does not meet initial screening criteria

Step 5: Pre-Interview Process

- Schedule interviews with appropriate candidates
- Applicants complete pre-employment application packets
- Conduct screening interviews/tests to measure candidate aptitude skills

Step 6: Final Interview Process

- Conduct final interviews with Human Resources and appropriate department manager
- Rate candidates using skills interviewing criteria
- Require interviewers to provide rating and hiring recommendation
- Complete final hiring recommendation form that includes potential start date and salary
- Program Manager approves hiring decision

Step 7: Reference and Criminal History Checks

- Ask all candidates recommended for employment to provide supervisory references from their last three employers
- Human Resources Recruitment Team is responsible for coordinating reference checking. Develop a reference checklist so that certain critical questions are asked
- All candidates sign a release allowing a criminal history reference check
- Conduct criminal history and reference checks, a critical activity, particularly on programs where staff work directly with the general public
- Positions are not offered to candidates convicted of a felony involving illegal gain or use of government funds, grants, contracts, or Medicaid or Medicare monies; or convicted of embezzlement, wire fraud, mail fraud, or securities violation

Step 8: Send Candidate Offer Letters

- Offer letters sent to final candidates on completion of reference checks and criminal history checks
- Offer letter includes candidate's title, job description, starting salary, report date, reporting location, and training schedule
- Offer letter includes basic information concerning the benefits package
- All candidates are asked to sign and return the offer letter as acceptance of the terms and conditions presented

OF_8 Steps to Employment

Exhibit 3.10.5-3: MAXIMUS Hiring Process. *DPHHS and this project are best served by a large company such as MAXIMUS which can efficiently handle fluctuating staff levels. We have a large staff base and an established hiring processes.*

Prior to conducting formal interviews, we ask applicants to complete pre-employment application packets. We also conduct screening interviews to measure candidate aptitude skills. If appropriate, we test applicants to help verify they have the required skills. In addition to undergoing pre-employment screening, all potential staff members participate in a formal interview process. We have a series of interviewing techniques including behavioral interviews, role-playing, and skills-based qualifications that help us find the right people.

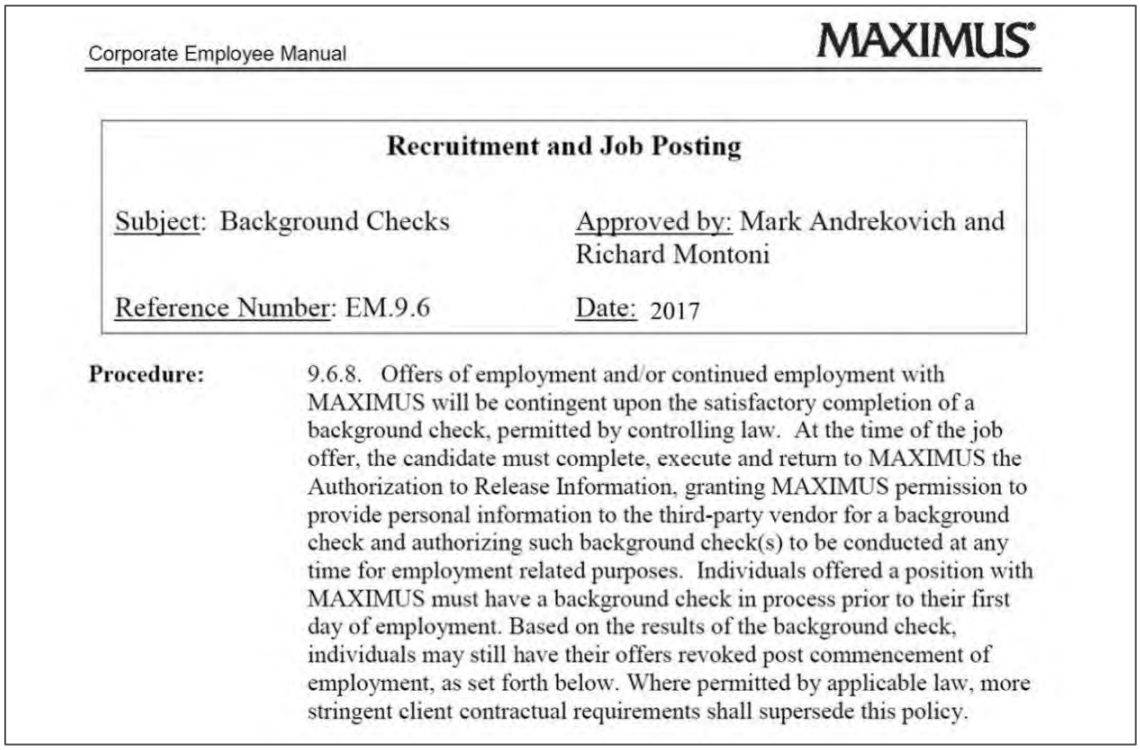
MAXIMUS maintains an Affirmative Action and Equal Employment Opportunity Policy.

> *We employ qualified persons of the greatest ability without discrimination against any employee or applicant for employment because of race, color, gender, age, religion, religious beliefs, sex, sexual orientation, gender identity, national origin, physical or mental disability, U.S. veteran status, genetic information, marital status, creed, citizenship status, or any other status protected by law, except where gender is a bona fide occupational requirement.*
>
> *MAXIMUS is committed to this policy and takes affirmative action to employ and advance in employment all qualified minorities, women, individuals with disabilities, and protected U.S. veterans. We are far more strongly bound to the policy by the fact that adherence to the principles involved is the only acceptable American way of life.*
>
> *In furtherance of MAXIMUS policy regarding EEO and affirmative action, MAXIMUS has developed written Affirmative Action Programs which sets forth the policies, practices and procedures that MAXIMUS is committed to in order to ensure that its policy of nondiscrimination and affirmative action for qualified minorities, qualified females, qualified individuals with disabilities, qualified protected veterans is accomplished.*

Background Checks

For candidates, we check references and conduct background checks. Per Attachment F, requirement KR19, in this subsection, we describe the MAXIMUS process for performing background checks for non-US citizens or Green Card holders.

As a contractor of government health and human services operations and system projects, MAXIMUS maintains stringent security protocols. To enforce the security of our customers, data, and operations, we conduct extensive background checks on each employee and potential employee. Background checks are a critical element of our staffing process, and we verify that 100 percent of our staff members clear such checks. We adhere to our rigorous Standard Operating Procedures and the RFP requirements for background checks for all project employees. *Exhibit 3.10.5-4: MAXIMUS Background Check Requirements* shows an excerpt from our Corporate Employee Manual regarding background checks.



Corporate Employee Manual MAXIMUS

Recruitment and Job Posting

Subject: Background Checks

Approved by: Mark Andrekovich and Richard Montoni

Reference Number: EM.9.6

Date: 2017

Procedure:

9.6.8. Offers of employment and/or continued employment with MAXIMUS will be contingent upon the satisfactory completion of a background check, permitted by controlling law. At the time of the job offer, the candidate must complete, execute and return to MAXIMUS the Authorization to Release Information, granting MAXIMUS permission to provide personal information to the third-party vendor for a background check and authorizing such background check(s) to be conducted at any time for employment related purposes. Individuals offered a position with MAXIMUS must have a background check in process prior to their first day of employment. Based on the results of the background check, individuals may still have their offers revoked post commencement of employment, as set forth below. Where permitted by applicable law, more stringent client contractual requirements shall supersede this policy.

Exhibit 3.10.5-4: MAXIMUS Background Check Requirements. *To protect our customers, staff, facilities, and data, MAXIMUS conducts thorough background checks on all new hires.*

MAXIMUS uses E-Verify to verify a prospective staff member's citizenship/residency and their eligibility to work legally in the United States. Our process for background checks is the same for all hires regardless of citizenship.

We use Orange Tree Employment Screening to perform our background checks. The standard Orange Tree background check includes the following:

- County, Statewide, and Federal Criminal Record Search
- Social Security Number Trace
- Office of the Inspector General List of Excluded Individuals and Entities and General Services Administration Excluded Parties List
- National Criminal Records Search
- National Sex Offender Registry Search
- Employment Verification
- Education Verification

The background checks that Orange Tree conducts are consistent with our high ethical standards and our awareness of the ongoing safety of our staff and operations.

3.10.5.1 Resource Allocation Schedules

3.10.5.1 Resource Allocation Schedules

Offerors must complete the Resource Allocation Schedules provided in Attachment H, Resource Allocation Schedules. These schedules serve as the representation of Offeror's plan for staffing the project by resource type. Offeror should include additional information as necessary to explain the Offeror's resource allocation. If the Offeror has one or more subcontractors, the Offeror must submit a Schedule A and Schedule B with a comprehensive total for all FTE and hours representing the effort of the prime contractor and all subcontractor work in total. In addition, a separate Schedule A and Schedule B for each contractor (prime contractor and subcontractor) must be submitted.

Table 3.10.5.1 Resource Allocation Schedules (These schedules are provided in Attachment H, Resource Allocation Schedules).

List of Resource Allocation Schedules	
Schedule	Title
Schedule A	Number of Full Time Equivalent
Schedule B	Number of Hours

All schedules must be completed in full at the time of submittal. The resource types listed in the schedule are not exhaustive, nor should the Contractor assume that DPHHS is requesting resources from each category. Use any resource type listed above and/or add resource types necessary to successfully deliver the scope of work.

Schedule A: This schedule details the number of full time equivalents the Offeror plans to allocate to the project by phase and by resource type.

Schedule B: This schedule details the number of resource hours the Offeror plans to allocate to the project by phase and by resource type.

MAXIMUS includes our completed Resource Allocation Schedules in Attachment H, Resource Allocation Schedules. These schedules are the representation of our plan for staffing the project by resource type. We include additional information as necessary to explain our resource allocation.

We include a Schedule A and Schedule B with a comprehensive total for all FTE and hours representing the effort of MAXIMUS as the prime contractor and our subcontractor work in total. We are proposing one subcontractor, Microassist, and include a separate Schedule A and Schedule B for them.

Key Personnel and Resources Requirements

The following table includes Attachment F Key Personnel and Resources Requirements and our summarized response to each requirement, for which additional information is provided in this *Section 3.10.5–Key Personnel and Resources*.

ID	Key Personnel and Resources Requirement	MAXIMUS Summarized Response
KR01	The Contractor can use off-shore and near-shore resources. However, offshore or near shore resources cannot develop security controls. The Contractor shall advise the Department when work is being completed by offshore or near shore resources. The Contractor shall ensure that all Contractor practices and procedures, including but not limited to secure coding practices are used by all resources.	MAXIMUS is not using offshore or near shore resource for any aspect of our project including to develop security controls. We will advise the Department if this changes.
KR02	The Contractor, and any of its subcontractors, shall work cooperatively with module Contractors and Department staff to ensure the success of the program.	MAXIMUS, and any of our subcontractors, will work cooperatively with module Contractors and Department staff toward program success.

CONFIDENTIAL

ID	Key Personnel and Resources Requirement	MAXIMUS Summarized Response
KR03	The Contractor shall help prevent project delays and address them if they occur. This includes assurances that sufficient resources and knowledgeable, experienced staff are available to meet the required project schedule.	MAXIMUS will help prevent project delays and address them if they occur, by providing sufficient resources and knowledgeable, experienced staff to meet the required project schedule. With three Medicaid Provider Services module implementations, MAXIMUS is offering the most experienced resources of any vendor. Our experience also assures the State that we understand the staffing requirements for meeting the project schedule.
KR04	The Contractor shall provide sufficient personnel to administer and execute required project activities, including approvals, during development, implementation, and operations.	MAXIMUS will provide sufficient personnel to administer and execute required project activities, including approvals, during development, implementation, and operations.
KR06	The Contractor shall provide key personnel that at a minimum include the Project Manager, the Contract Manager, the Testing Lead, Integration Lead and a Certification Lead during the DDI and Certification Phases of the Program. Key personnel shall not hold more than one key role unless otherwise approved by the Department. The Department will review and approve all key personnel.	During the DDI and Certification Phases, MAXIMUS will provide key personnel, including the Project Manager, the Contract Manager, the Testing Lead, Integration Lead, and a Certification Lead. Our key personnel will not hold more than one key role unless otherwise approved by the Department.
KR07	Key personnel described in the proposal shall become named resources on the project and are subject to the following requirements: a. Key personnel shall not be transferred or removed without prior approval of the Department. b. The Department will approve key personnel assigned to the Contract. c. The Department reserves the right to request removal of any Contractor staff or subcontractor staff, if applicable, assigned to the project, and the Contractor shall comply with any such request immediately. d. If a vacancy occurs in a key role, the Contractor shall fill the position in compliance with identified SLAs.	MAXIMUS proposed key personnel will become named project resources and are subject to the following requirements: ■ Key personnel will not be transferred or removed without prior approval of the Department. ■ The Department will approve key personnel assigned to the Contract. ■ The Department reserves the right to request removal of any MAXIMUS staff or subcontractor staff, if applicable, assigned to the project, and MAXIMUS will comply with any such request immediately. ■ If a vacancy occurs in a key role, MAXIMUS will fill the position in compliance with identified SLAs.
KR08	The Contractor must designate a Project Manager to represent and oversee the day-to-day activities of the project. This individual shall serve as the Department's primary point of contact for matters relating to the project and serve as a liaison for certification, collaborating with other contractors, and stakeholders.	[redacted]
KR09	The Contractor's Project Manager must meet the following qualifications including: a. A minimum of seven (7) years' project management experience managing projects of similar size and scope, preferably in Medicaid or the healthcare industry. This experience must include relevant experience within the last three (3) years from the release date of the RFP. b. Project Management experience should include each phase of the system development life cycle. c. Project management certification through the Project Management Institute (PMI) is preferred.	[redacted]
KR10	The Contractor must designate an Integration Lead to manage the design, configuration/build, integration, defect management, and implementation of the Contractor's scope of work.	[redacted]

CONFIDENTIAL

ID	Key Personnel and Resources Requirement	MAXIMUS Summarized Response
KR11	The Contractor's Integration Lead must meet the following qualifications including: a. Minimum of five (5) years leading system design and integration projects, including the technical design and implementation of projects similar in size and scope to this project. b. Experience must involve directing multi-discipline technical teams producing integration solutions (e.g., Service Oriented Architecture, network, hardware and software). c. A Bachelor's Degree in Information Systems Engineering, Computer Science, or a related field is preferred.	[redacted]
KR12	The Contractor must designate a Testing Lead to coordinate all testing activities.	[redacted]
KR13	The Contractor's Testing Lead must meet the following qualifications including: a. Minimum of three (3) years experience leading testing activities for a project similar in size and scope to this project. b. In-depth understanding of the testing lifecycle and all artifacts required to successfully validate the system.	[redacted]
KR14	The Contractor must designate a Contract Manager to be the single point of contact for matters concerning the Contractor's performance under the Contract. This person shall have the authority to make decisions that are binding to the Contract, shall be responsible for timely completion of the project, and shall be responsible for meeting all contractual obligations.	[redacted]
KR15	The Contractor's Contract Manager must have a minimum of five (5) years' contract management experience managing related services with similar budgets, preferably in Medicaid or the healthcare industry and for a project similar in size and scope to this project.	
KR16	The Contractor shall submit two (2) references for each of the key personnel being proposed for the project. Each reference should depict relevant and current experience for work completed no more than seven (7) years prior to the date of this RFP.	MAXIMUS is submitting 2 references for each of the key personnel being proposed for the project. Each reference depicts relevant and current experience for work completed no more than 7 years prior to the date of this RFP.
KR17	The Contractor must demonstrate that it can commit an adequate level of technical and human resources sufficient to complete the project within the required time frame and to meet the quality requirements outlined in this RFP. Furthermore, the level of technical and human resources which the Contractor agrees to commit to the project at the time of proposal must be maintained throughout the life of the project at a necessary level to complete the scope of work.	With 18,000 employees globally, MAXIMUS will commit the adequate level of technical and human resources sufficient to complete this project within the required timeframe. Having successfully completed similar projects for other states, we are familiar with the demands of this project and will meet the RFP quality requirements. We agree to commit to and maintain the technical and human resources to this project throughout the life of the project at a necessary level to complete the scope of work.
KR18	The Contractor's staff shall have sufficient experience appropriate for their role.	Each of our staff members will have sufficient experience appropriate for their roles, which we clearly define on every project we manage.
KR19	The Contractor must supply a Personnel Background Check Attestation (written documentation) of a favorable background check for Contractor personnel who might reasonably be expected to access sensitive and confidential member data contained in any system accessed during the course of the Contract. The Department may request the removal of staff for disqualifying offenses. Contractor must describe their process for performing background checks for non-US citizens or Green Card holders.	MAXIMUS will supply a Personnel Background Check Attestation (written documentation) of a favorable background check for our personnel who might reasonably be expected to access sensitive and confidential member data contained in any system accessed during the course of the Contract. In Section 3.10.5, MAXIMUS describes our established corporate procedures for complete background checks for all employees, including non-US citizens or Green Card holders.
KR20	The Contractor's Project Manager shall be required to perform work at the State's primary project location (e.g., city, state), unless approved by the Department to work remotely.	[redacted] will perform work at the State's primary project location (e.g., city, state), unless approved by the Department to work remotely.

CONFIDENTIAL

ID	Key Personnel and Resources Requirement	MAXIMUS Summarized Response
KR21	The Contractor's staff shall be available Monday through Friday as early as 7:00 AM MST and as late as 6:00 PM in the time zone of the participating State.	MAXIMUS staff will be available Monday through Friday as early as 7:00 AM MST and as late as 6:00 PM in the time zone of the Participating State.
KR22	For any work performed at a location other than the primary Project site, the Contractor must identify the specific location (city, state, country), describe the type of work to be performed, and the percent of the total hours for that type of work at that location.	For work performed at a location other than the primary Project site, MAXIMUS will identify in the Staffing Plan the specific location (city, state, country), describe the type of work to be performed, and the percent of the total hours for that type of work at that location.
KR23	The Contractor's staff working remotely, must be available to work in the State's primary project location at the Department's' request for functions necessary to support the scope of work (e.g., risk review meetings, root cause analysis sessions, integration planning, release planning, operational readiness reviews, UAT, implementation, and production deployment).	MAXIMUS staff working remotely will be available to work in the State's primary project location at the Department's request for functions necessary to support the scope of work.
KR24	In the event that key personnel resign or are terminated, the Contractor shall provide the Department with immediate notice of the vacancy and an action plan for backfilling the position until a replacement is found and approved by the Department. A key personnel position must not be vacant for more than fourteen (14) consecutive days. The Contractor may not fill vacant key personnel positions with other existing key personnel without approval by the Department. The Department will also have the authority to approve proposed replacements of key personnel by the Contractor.	In the event that Key Personnel resign or are terminated, MAXIMUS will provide the Department with immediate notice of the vacancy and an action plan for backfilling the position until a replacement is found and approved by the Department. We will not leave a Key Personnel position vacant for more than 14 consecutive days, or fill the positions with other existing Key Personnel without approval by the Department.
KR25	The Contractor's key personnel and/or management replacement must meet the minimum qualifications for the position. The Contractor shall provide a detailed resume for a proposed key personnel and/or management replacement. Replacements are subject to Department approval prior to any assignment.	MAXIMUS Key Personnel and/or management replacement will meet or exceed the minimum qualifications for the position. We will provide the Department with a detailed resume to demonstrate such qualifications.
KR26	The Contractor shall provide the appropriate level of knowledge transfer/training to Contractor staff.	MAXIMUS will provide the appropriate level of knowledge transfer/training to our staff.
KR28	The Contractor must designate a Certification Lead to coordinate all certification activities.	[redacted]
KR29	The Contractor's Certification Lead must meet the following qualifications including: a. Minimum of three (3) years experience certifying systems against industry standards for projects similar in size and scope to this project. b. In-depth understanding of the most current MECT certification lifecycle required to successfully validate the system.	[redacted]
KR30	The Contractor shall provide key personnel that at a minimum includes a Project Manager, Contract Manager and a Technical Manager for the Operations, Maintenance and Configuration phase of the project. Key personnel shall not hold more than one key role unless otherwise approved by the Department. The Contractor must identify other key personnel for the Operations, Maintenance and Configuration phase of the project. The Department will review and approve all key personnel.	MAXIMUS has named a Project Manager, Contract Manager, and Technical Manager for the Operations, Maintenance, and Configuration phase of the project. Our Key Personnel will hold only one key role unless otherwise approved by the Department. We have also identified other key personnel for the Operations, Maintenance, and Configuration phase of the project.

3.10.6 Project Closeout and Turnover

3.10.6.1 Project Closeout and Turnover

3.10.6 Project Closeout and Turnover

At least twelve months prior to the end of the contract, the Contractor will provide an initial turnover plan to detail how the Contractor will manage the completion and closure of all work for the Contract and deliver project artifacts, including deliverables, data, and anything needed to operate and maintain the integrity of the Montana Healthcare Programs and systems.

Transition activities will be dependent upon the nature of the solution or services, which may include but is not limited to:

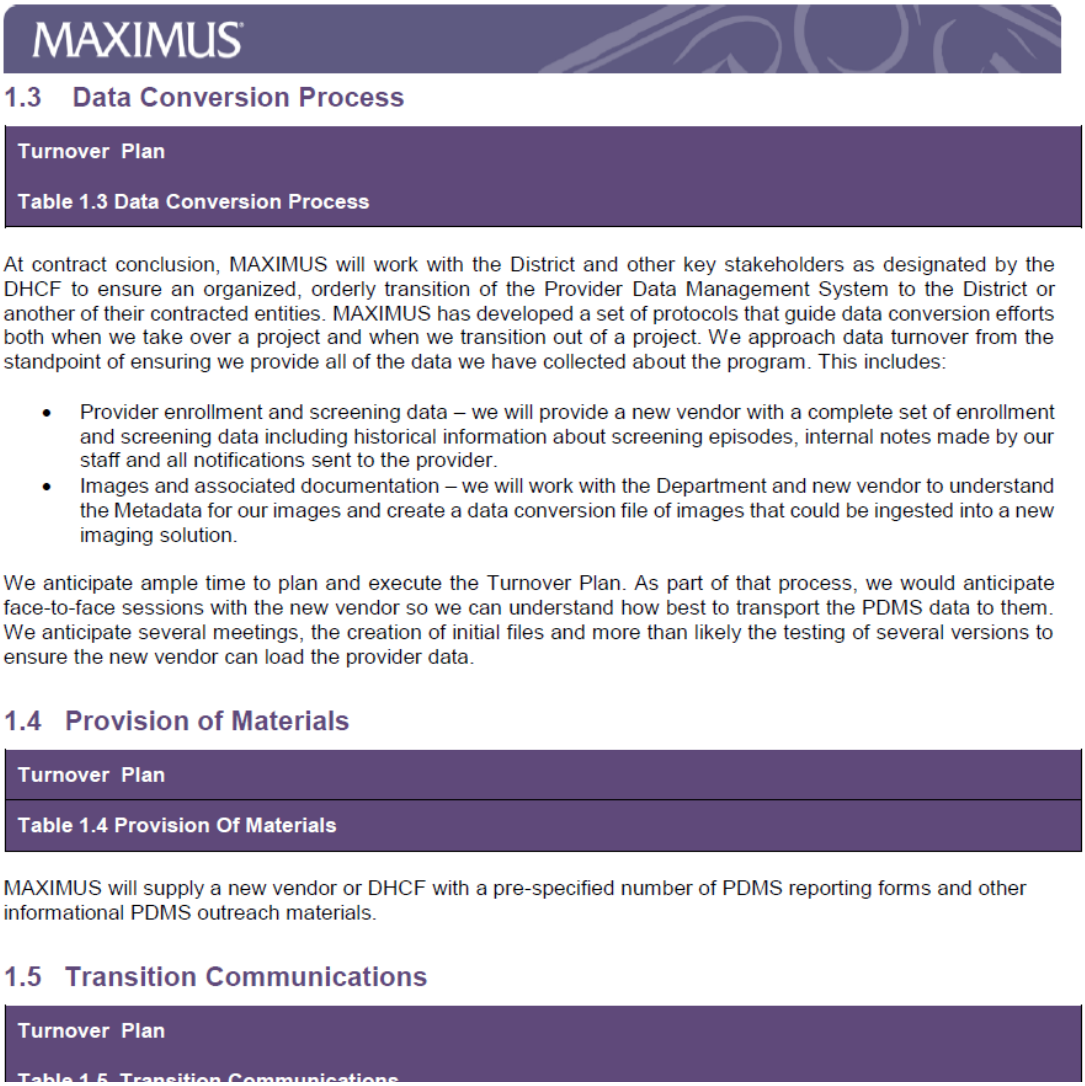
- State Owned and hosted
- State Owned and Contractor hosted
- State Leased software and State-hosted
- State Leased software hosted by a third party
- Software as a Services (SaaS)

The Contractor must demonstrate that all contractual requirements have been met, transition operational tasks to a new Contractor and/or DPHHS completed, and provide lessons learned from the project prior to the end of the contract term. The Offeror must describe their approach to meet each of the Project Closeout and Turnover requirements defined in Attachment F, Requirements Matrix.

The tasks and activities involved in our turnover approach will be guided by the project's Turnover Plan. This required deliverable will be submitted to the Department at least twelve months prior to the end of the contract, and an Updated Turnover Plan at six months prior to the end of the contract. This plan will outline the tasks and planning activities required to transition from the MAXIMUS Provider Services solution.

MAXIMUS understands the numerous activities that must occur to support a smooth transition. Our proposed approach to turnover includes tasks, subtasks and a proposed schedule for turnover, including supplying the Monthly Turnover Reports during the turnover phase and the Turnover Results Report required at completion of turnover activities. According to the Turnover Plan and the Updated Turnover Plan, we will update the operational tasks and procedures, and will provide a list of incomplete tasks, such as system defects, modifications or enhancements, mass adjustments, reference updates, and configuration requests. The MAXIMUS Turnover Plan describes the vendor and state coordination activities that will occur during the turnover task and implementation of the activities with the end goal of continued system and services as deemed necessary by the Department. Coordination with the successor vendor or the state is key to a smooth transition. As such, our Transition Plan will contain a detailed description of the services required to fully take over system, technical, and business functions outlined in the Contract, including an estimate of the number and type of personnel required to support the technical platform and supporting services. We will organize the data and documentation in a format required by the State (e.g., by provider unique ID and provider name).

Our Turnover Plan will contain the required content as specified in requirement DOC37 as specified in Appendix F. We have produced Turnover Plans in previous Provider Services implementations. *Exhibit 3.10.6-1: Sample Implementation Plan* shows a snippet from the Implementation Plan we submitted for the District of Columbia.



MAXIMUS

1.3 Data Conversion Process

Turnover Plan

Table 1.3 Data Conversion Process

At contract conclusion, MAXIMUS will work with the District and other key stakeholders as designated by the DHCF to ensure an organized, orderly transition of the Provider Data Management System to the District or another of their contracted entities. MAXIMUS has developed a set of protocols that guide data conversion efforts both when we take over a project and when we transition out of a project. We approach data turnover from the standpoint of ensuring we provide all of the data we have collected about the program. This includes:

- Provider enrollment and screening data – we will provide a new vendor with a complete set of enrollment and screening data including historical information about screening episodes, internal notes made by our staff and all notifications sent to the provider.
- Images and associated documentation – we will work with the Department and new vendor to understand the Metadata for our images and create a data conversion file of images that could be ingested into a new imaging solution.

We anticipate ample time to plan and execute the Turnover Plan. As part of that process, we would anticipate face-to-face sessions with the new vendor so we can understand how best to transport the PDMS data to them. We anticipate several meetings, the creation of initial files and more than likely the testing of several versions to ensure the new vendor can load the provider data.

1.4 Provision of Materials

Turnover Plan

Table 1.4 Provision Of Materials

MAXIMUS will supply a new vendor or DHCF with a pre-specified number of PDMS reporting forms and other informational PDMS outreach materials.

1.5 Transition Communications

Turnover Plan

Table 1.5 Transition Communications

Exhibit 3.10.6-1: Sample Turnover Plan. *MAXIMUS will submit a Turnover Plan to DPHHS, which outlines our approach for successfully turning over the Provider Services solution. We tailor our previously created planning documents to meet the requirements of each State.*

The turnover plan describes the activities, responsibilities, and timeline for transitioning to another Contractor. This document lays out a cooperative approach to provide the technical and functional training required for the new vendor to confidently assume Operations and Maintenance responsibility for Provider Management services in the event MAXIMUS is no longer the O&M Contractor. At least twelve months prior to the end of the contract, MAXIMUS will provide an initial turnover plan that details how we manage the completion and closure of all work for the contract. This includes delivering project artifacts, including deliverables, data, and anything needed for a smooth transition that it seamless to the providers and maintains the integrity of the programs and systems. The turnover plan includes plans specifically for transition from our SaaS solution to the State or another vendor.

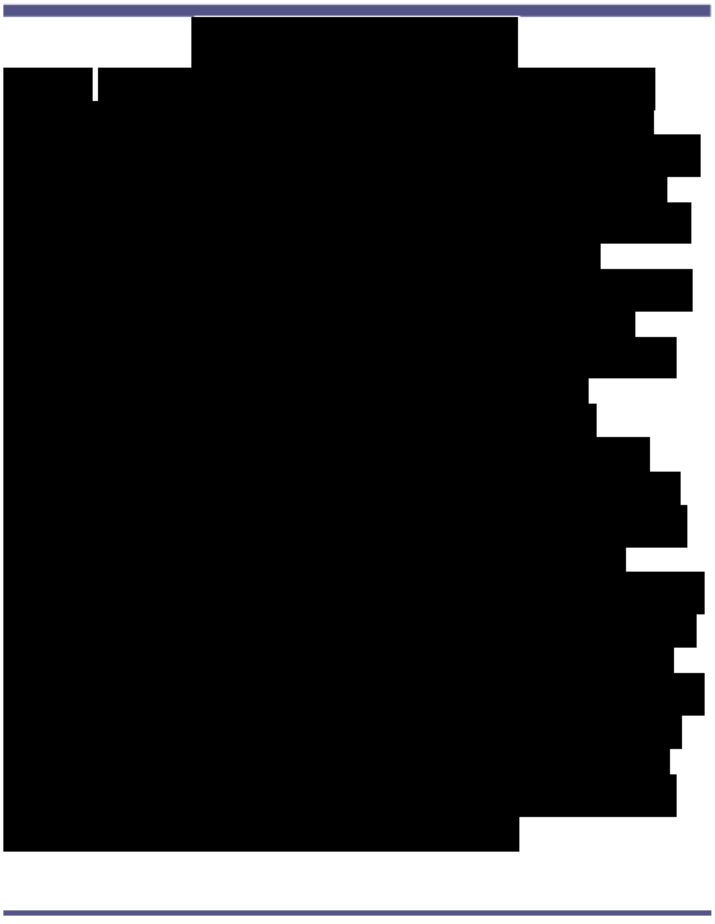
As any major government contractor knows, contracts inevitably end through normal expiration, transfer back to the client, or transfer to a successor contractor. At the end of the contract, MAXIMUS coordinates

CONFIDENTIAL

with all stakeholders to effectively transfer operations and all the requisite data to the State or a successor contractor. We develop a Turnover Plan at the end of the contract period in accordance with the State's timetable. Our Plan includes:

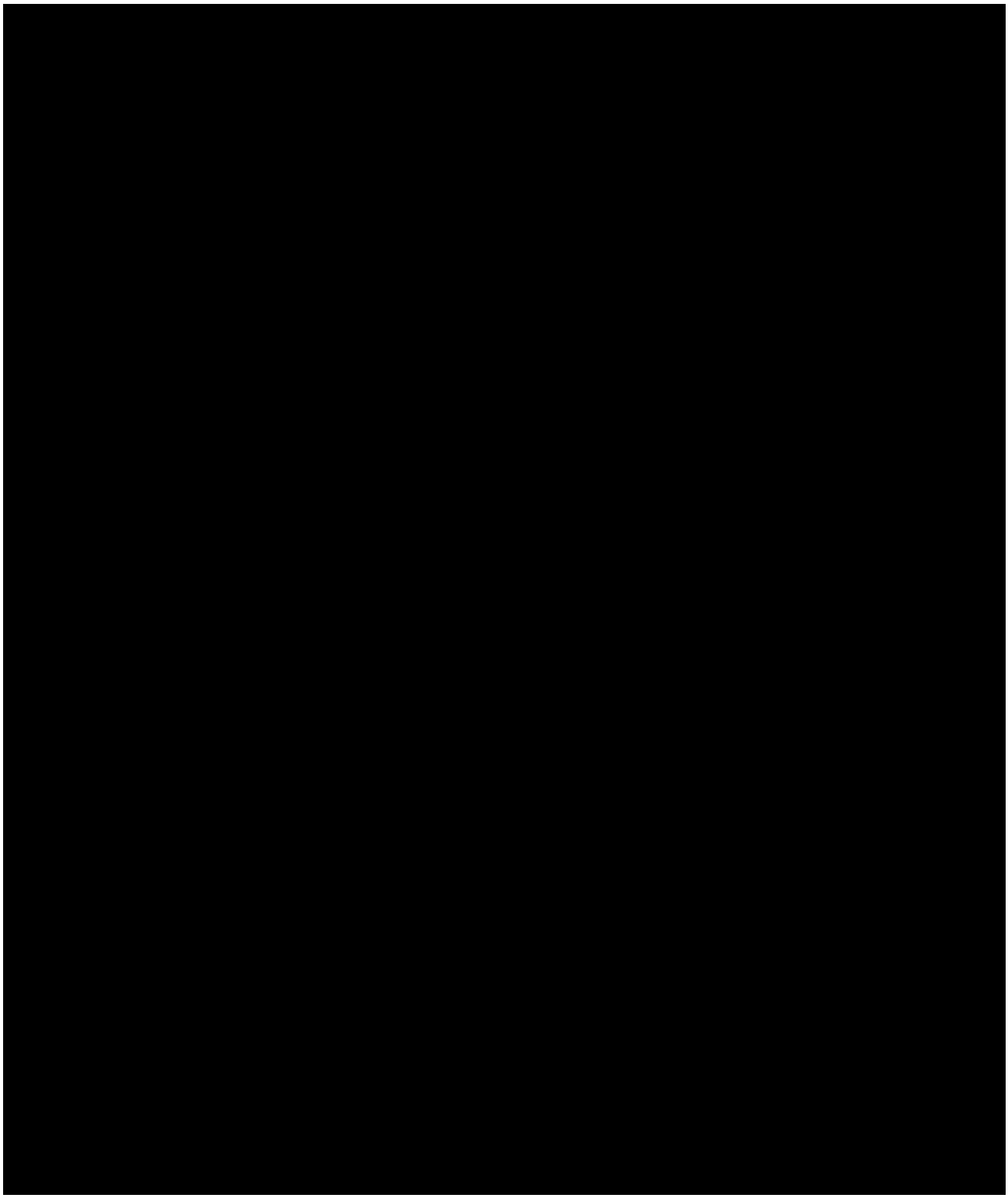
- **Schedule:** The schedule is created in Microsoft Project using a Gantt chart in much the same way that the Project's implementation schedule is created. The schedule indicates dependencies, beginning and ending dates, total duration of each task, milestones, and deadlines.
- **Activities/Tasks:** All activities/tasks are defined in the Plan, with start and finish dates associated with each task, as well as the resources needed to complete the task.
- **Resource Requirements:** Our Turnover Team members are assigned to tasks according to their roles and responsibilities as determined at the beginning of the turnover phase. The Turnover Manager closely tracks the status and progress through regular team meetings and reports.
- **Data and Documentation:** As a SaaS solution, information regarding Project operations and the MAXIMUS Provider Services solution are transferred in a manner, format, and media defined in the Plan and approved by the State.

We approach project turnover with the same meticulous planning, best practices, and communications strategies that we do for project start-ups. Our detailed Turnover Plan guides our operations and maintenance team members and the new support team through the training and oversight activities necessary to transition or "close-out" MAXIMUS responsibilities for O&M. This manual includes detailed procedures that address turnover and communication protocols we follow when working with our clients. *Exhibit 3.10.6-2: Turnover/Close-Out Checklists* summarizes some of the activities associated with closing out and turning over a project. We tailor our closeout activities to build a complete Turnover Plan unique to each project such as that for Montana.



CONFIDENTIAL

CONFIDENTIAL

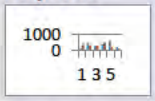


As part of our turnover planning process, we work with the State to agree upon deliverables and sign-off procedures for each so the State is satisfied with our completion of the tasks. We implement the State-approved Turnover Plan within a timeframe specified by the State.

Through our experience with contract takeovers and occasional turnovers, we have learned which components of a turnover plan are crucial to success and will result in a seamless transition. We recognize the criticality of preventing any problems that might negatively impact state Medicaid Provider registration or payment as the DPHHS transfers to a new Provider Services solution vendor. To achieve this goal, we work closely with the State and new support team to accomplish all transition activities timely and verify readiness of the new vendor to assume responsibility prior to our departure.

Transition or turnover of a contract upon completion is critical to continued successful service delivery to Providers. MAXIMUS will deliver all federal or State-funded computer applications, data, reference tables, scripts, documentation, and records required by the State or Successor Contractor to the appropriate parties. The biggest risk during any transition is an interruption in services or a degraded level of service. To help mitigate these risks, we develop a thorough Turnover Plan that fully outlines the tasks, milestones, timeframes, resources, and communications strategy for a successful turnover. Because we follow strict processes in all aspects of implementation and operations phases, we will be able to demonstrate that all contractual requirements have been met and that any operational tasks to a new Contractor and/or DPHHS have been completed.

Finally, we develop and deliver a detailed Lessons Learned document from the time of project initiation and prior to the end of the contract term. The Lessons Learned document is developed in concert with relevant staff from MAXIMUS, the State or other vendors. This document reflects the shared knowledge gained from experience so that the entire organization benefits and can apply these lessons for future projects. This includes capturing not only what did not work well, but also what did work well so those activities may be repeated.

Requirement	Approach to Turnover
Files	▪ Our application servers and computers will remain fully operational until project functions are terminated and all agreed-upon files have been transferred and received successfully ▪ The Turnover Plan defines the data that will and will not be transferred and will coordinate the timeframe and signoff procedures for acceptable data transfer ▪ We will provide all federal or State-funded computer applications, data and reference tables, scripts and other documents and records required to operate the Successor Contractor's Provider Services solution ▪ Provide all State-approved in-flight updates or replacements to business, operations, and technical materials not yet formally documented ▪ Certify in writing that any content or customizations to the State in all formats have been destroyed and all of the State's data are delivered in a format that accessible ▪ Adhering to State and federal information security standards, purge all State data from the MAXIMUS Provider Services solution and backups when the State has confirmed in writing the receipt and usability of all data. Guarantee that the data is unrecoverable by any known means
Reports 	▪ We will prepare and distribute special status reports during the turnover phase of the project to aid in managing close-out activities, timeline, deliverables, and acceptance ▪ Prepare and deliver the Turnover Results Report to document completion of all turnover activities
Procedures	▪ We will review procedures with the State to determine which ones, if any, might be transferrable in accordance with our agreed upon Plan and deliverables

Requirement	Approach to Turnover
Materials	▪ User training materials developed for this project will be transitioned per the Turnover Plan ▪ Any materials provided by the State during the course of the contract will be returned in a timely manner in an agreed upon method of hand-off described in the Turnover Plan
Documentation	▪ MAXIMUS will transfer the appropriate documentation to the State or its designated successor Contractor as defined in the approved Turnover Plan ▪ The State and MAXIMUS working together will agree on the timeframes for gathering all relevant non-proprietary documentation and distributing it to appropriate parties. All applicable HIPAA and other confidentiality requirements will remain in place and will govern the manner of data and information transfers.
Training	▪ MAXIMUS will provide reasonable training for the State and/or successor contractor. The training provided will be agreed upon during the development of the Turnover Plan and may include topics such as workflows, processes, and valuable lessons learned, and other key aspects that will facilitate a smooth turnover of services

Exhibit 3.10.6-3: Plan for Turnover. *We collaborate with the State and successor contractor, as needed, to determine the most appropriate procedures for successful transfer of applications, data, and other materials related to providing screening and enrollment services to providers.*

MAXIMUS will assist the State in the orderly transfer of contract responsibilities and the continuity of screening and enrollment services for providers to another organization if the State requests this in writing. Our assistance in this type of turnover includes:

- **Paper Originals and/or Electronic Documents and Records:** As described in *Exhibit 3.10.6-3: Plan for Turnover*, we work with the State and other stakeholders to arrive at the best format and timeline for transferring appropriate and agreed-upon original paper and/or electronic documents and records to state Medicaid per contractual requirements.
- **Discontinue Services on Specified Date:** MAXIMUS agrees to discontinue providing services or accepting additional assignments under the terms of the contract, on the date specified by the State. In this way, all services associated with the contract will be completed prior to the expiration of the contract.
- **Provide a Turnover Results Report:** When all turnover activities have been completed, MAXIMUS provides a Turnover Results Report to document the completion and results of each step of the turnover plan. Any issues encountered, as well as timeframes for completion, are included in the Results Report.

Project Closeout and Turnover Requirements

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

ID	Project Closeout and Turnover Requirement	MAXIMUS Summarized Response
PTO01	The Contractor shall provide a turnover approach and the services required for the transition of operations, services and module components.	Our thorough and comprehensive Turnover Plan includes all aspects of the contract necessary for a smooth transition. This includes the transition of operations, services, and module components.
PTO02	At least six (6) months prior to the final Contract year (including option years that have been exercised) and at least six (6) months prior to the end of any contract extension(s), the Contractor shall provide the following: a. An updated Turnover Plan. b. Complete and update system and user documentation. c. Statement of the resources that would be required by the Department or another contractor to fully take over solution, technical, and business functions outlined in the Contract(s). This includes quantity and types of resources and volume of tasks to support the scope of work. d. Operational tasks and procedures as necessary to support ongoing operations of the solution. e. Lessons learned report. f. List of incomplete tasks, such as system defects, modifications or enhancements, mass adjustments, reference updates, and configuration requests. g. A detailed description of the services that would be required by another Contractor to fully take over system, technical, and business functions outlined in the Contract. The Department reserves the right to request this information at any time throughout the Contract.	The Turnover Plan accounts for knowledge transfer to State staff or to any State designee. According to the six (6) months prior to the final Contract year and at least six (6) month prior to the end of any contract, as well as upon request at any time throughout the contract, MAXIMUS agrees to the following: a. An updated Turnover Plan b. System and user documentation will be maintained throughout the life of the project. These will be provided to the State as requested c. MAXIMUS plans for Turnover activities that include necessary resources from the State or from another contractor. We will provide a statement that includes requirements for the Department or another contractor to fully take over the solution, technical, and business functions, including quantity, types of resources and volume of tasks. d. Maintaining ongoing operations is paramount to a smooth transition. We will supply the operational tasks and procedures as necessary to support the ongoing operations. e. We will document and provide to the State a project lessons learned. f. In the event there are ongoing updates or implementations in progress during the transition period, we will provide updated documentation to the State. g. We appreciate the potential for service disruption that can occur from any contractor transition. We will provide a detailed description of services of the required services for another contractor to fully take over system, technical and business functions to minimize service disruptions.
PTO03	The Contractor shall provide a Monthly Turnover Report reflecting transition activities during the turnover period.	During the Turnover period, MAXIMUS will provide to the State regular, monthly at a minimum, updates of all transition activities.
PTO04	The Contractor shall provide operational procedures that describe how maintenance is performed for the solution.	The Turnover Plan accounts for knowledge transfer to State staff or to any State designee. This includes operational procedures that describe how maintenance is performed for the MAXIMUS Provider Services solution.
PTO05	The Contractor shall cooperate with the successor contractor while providing all required turnover services. This will include meeting with the successor and devising work schedules that are agreeable for both the Department and the successor contractor.	We are dedicated to providing a turnover of operations that is smooth and seamless to the State and transparent to providers. MAXIMUS commits to comply with the approved Turnover Plan and cooperate with the succeeding vendor as necessary for a straightforward and uncomplicated continuation of services. This includes meeting with the successor and developing work schedules that are agreeable for both the Department and the successor contractor.
PTO06	The Contractor must transfer solution and services documentation and all data requested by the State to the State.	We work diligently to provide all non-proprietary federal or State-funded computer applications, data and reference tables, scripts, and other documentation to the State.
PTO07	The Contractor shall deliver a Turnover Results Report that documents completion of each step of the Turnover Plan.	After the turnover is completed, MAXIMUS provides a Turnover Results Report. This report will document the completion and results of each step of the turnover plan. Delivery of this report marks the completion of the project.

3.10.7 Project Deliverables and Documentation

3.10.7 Project Deliverables and Documentation

The documentation deliverables outlined in Table 3.10.7 have been identified for this scope of work. DPHHS will review deliverable requirements and make changes to required deliverables based on Commercial-Off-the-Shelf (COTS)/Software-as-a-Service(SaaS) versus non-COTS/Non-SaaS software. For each documentation deliverable, the Contractor shall follow the guidelines outlined in the Documentation Standards in the Procurement Library. The Contractor will submit documents that meet the specific deliverable acceptance criteria as outlined in the Deliverable Expectation Document for the specific deliverable. All deliverables must be approved by DPHHS. Project artifacts and information will be shared on the CMS Reuse Repository. The Offeror must describe their approach to meet each of the Documentation requirements defined in Attachment F, Requirements Matrix.

Table 3.10.7 Documentation Deliverables

Deliverable	Delivery and Update Frequency	Requirement Number	Deliverables Expectations Document Required?
Project Management Plan	As scheduled in approved PWP, updates as necessary	PMT18	Yes
Project Work Plan	Project initiation, updates as approved.	PMT19	Yes
Communication Plan	As scheduled in approved PWP, updates as necessary	DOC15	Yes
Quality Management Plan	As scheduled in approved PWP, updates as necessary	DOC16	Yes
Risk Management Plan	As scheduled in approved PWP, updates as necessary	DOC38	Yes
Issue Management Plan	As scheduled in approved PWP, updates as necessary	DOC40	Yes
Change Management Plan	As scheduled in approved PWP, updates as necessary	DOC18	Yes
Defect Management Plan	As scheduled in approved PWP, updates as necessary	DOC22	Yes
Staffing Plan	As scheduled in approved PWP, updates as necessary	DOC24	Yes
Data Management, Conversion, and Migration Plan	As scheduled in approved PWP, updates as necessary	DOC03	Yes
Application, Configuration, and Maintenance Plan	As scheduled in approved PWP, updates as necessary	DOC04	Yes
User Interface Style Guide	As scheduled in approved PWP, updates as necessary	DOC46	Yes
User Documentation	Project initiation, updates as necessary	DOC07	Yes
Operations Procedure Manual	As scheduled in approved PWP, updates as necessary	DOC42	Yes
Business Continuity and Disaster Recovery Plan	As scheduled in approved PWP, Annually	DOC08, DOC09, DOC10	Yes
Operations, Maintenance and Configuration Plan	As scheduled in approved PWP, updates as necessary	DOC12	Yes
Turnover Plan	12 months prior to final Contract year	DOC37	Yes
Updated Turnover Plan	6 months prior to final Contract year	PTO02	No
Technical Documentation	Project initiation, updates as necessary	DOC19	Yes
System Design Documentation	As scheduled in approved PWP, updates as necessary	DOC14	Yes
System Documentation	Project initiation, updates as necessary	DOC29	Yes
Master Test Plan	As scheduled in approved PWP, updates as necessary	DOC26	Yes
Training Plan	As scheduled in approved PWP, updates as necessary	DOC27	Yes

Deliverable	Delivery and Update Frequency	Requirement Number	Deliverables Expectations Document Required?
System Test Plan	As scheduled in approved PWP, updates as necessary	DOC28	Yes
Module Implementation Plan	As scheduled in approved PWP, updates as necessary	DOC13	Yes
Solution Architecture Document	As scheduled in approved PWP, updates as necessary	DOC21	Yes
Attachment - L- Technology Matrix	Upon initial proposal, Annually	DOC44	No
Turnover Results Report	Upon completion of turnover activities	PTO07	Yes
Monthly Status Report*	Monthly	PMT17	No
System Security Plan	As scheduled in approved PWP, updates as necessary	DOC01	Yes
CMS Information Security Program Plan of Action and Milestones (POA&M)	Conditional upon security risk assessment findings	SEC55	No
Risk Assessments	Annually and As Needed	SEC11	Yes
Requirements Traceability Matrix (RTM)	As scheduled in approved PWP, updates as necessary	RQM06	Yes
CMS Certification Checklists	As scheduled in approved PWP, updates as necessary	CERT02	Yes
Certification Plan	As scheduled in approved PWP, updates as necessary	DOC02	Yes
Operational Readiness Review Checklist	As scheduled in approved PWP date	IA06	Yes
Operation Readiness Test Results	As scheduled in approved PWP date	IA04	Yes
Penetration Test Report	Annual and 6 months prior to implementation	SEC15	Yes
Performance Test Results	As scheduled in approved PWP, updates as necessary	TEST04	Yes
System Test Results	As scheduled in approved PWP, updates as necessary	TEST04	Yes
Parallel Test Results	As scheduled in approved PWP, updates as necessary	TEST04	Yes
Regression Test Results	As scheduled in approved PWP, updates as necessary	TEST04	Yes
Integration Test Results	As scheduled in approved PWP, updates as necessary	TEST04	Yes
Disaster Recovery/Business Continuity Test Report	Annual	OMC03	Yes
Monthly Turnover Report	Monthly, during Turnover Period	PTO03	Yes
Subcontractor Usage Report	Annual	SUB05	Yes
System Enhancement Pool Report	Monthly	PMT29	Yes
Business Rules Catalog	Project initiation, procurement of each MPATH module and updates as necessary	BR03	Yes
Certification Crosswalk	As scheduled in approved PWP, updates as necessary	CERT01	Yes
Personnel Background Check Attestation*	As necessary	KR19	No
Interface Control Documents (ICD)	As scheduled in approved PWP, updates as necessary	INR07	Yes

Deliverable	Delivery and Update Frequency	Requirement Number	Deliverables Expectations Document Required?
Deliverable Review and Acceptance Process	Project initiation, updates as necessary	PMT15	Yes
Data Dictionary	As scheduled in approved PWP, updates as necessary	DM11	Yes
Conceptual Data Model	As scheduled in approved PWP, updates as necessary	DM55	Yes
Implementation Letter	As scheduled in approved PWP	IA01	No
Security Audit Report	Annually on September 30	SEC22	No
Service Organization Control (SOC) 1 Type II Reports	Annually	SEC73	No

MAXIMUS will submit all project deliverables as specified in RFP Table 3.10.7 Documentation Deliverables. MAXIMUS has a repository of project deliverable templates and past work products that are consistent thus significantly reducing the development and review time for clients. MAXIMUS will reformat our deliverables to comply with the RFP attachment, MPATH Documentation Standards. This includes the cover letter, the table of contents, and all naming and storing conventions.

3.10.7.1 Deliverable Expectations Document

MAXIMUS will submit a Deliverable Expectations Document (DED) that contains a draft outline and annotated table of contents (ATOC) for all deliverables. Shortly after submission of the ATOC and before work on a deliverable begins, we will meet with DPHHS to discuss and agree upon the content to verify everyone has a common expectation of each deliverable. The DED is initially built based on the requirements outlined for each deliverable in Attachment F-Requirements Matrix. Our goal is to make the deliverable review process less rigorous by submitting a deliverable format and content that is familiar to DPHHS. This approach eliminates the need for rework and potential schedule delays. We believe that the deliverable expectations of MAXIMUS and DPHHS need to be in full agreement well in advance of the deliverable development and submission.

Each deliverable is submitted with a deliverable review form, as shown in *Exhibit 3.10.7-1: Project Management Plan Review Form*. This allows DPHHS to provide specific feedback on the document and allows MAXIMUS to use this same form to make changes and to respond to comments from DPHHS. MAXIMUS also supports feedback, comments, and questions provided in the deliverable document as revisions (MS Word / Track Changes).

Deliverable: PROJECT MANAGEMENT PLAN					
ID	Comment	Reviewer	Doc Ref	Document Text	Response
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					

Exhibit 3.10.7-1: Project Management Plan Review Form. *We submit our deliverables with a review form.*

Based on the State's request, we will store each document on the States and/or Systems Integration Services collaboration site. This will allow our deliverables and documentation to be accessible by the State, MAXIMUS and any external vendors that are granted access to the site. MAXIMUS updates documents and deliverables throughout the life of the project either as required by project changes or as required by the RFP. Deliverables are shared on the CMS Reuse Repository as well.

3.10.7.2 Project Management Documentation

MAXIMUS has Project Management documentation that describes in detail how the project is managed from start to finish. The Project Management Plan is the overarching plan that defines the methodology used to manage the MPATH project. The Project Management Plan includes several other plans that define the detailed workings of the management of the MPATH project. These include the Communication Plan, the Risk Management Plan, the Quality Management Plan, Project Status Reporting (weekly and monthly) information, Change Management Plan, the Staffing Management Plan, and the Issue Management Plan. 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.

3.10.7.3 Design Documentation

MAXIMUS has system business and design documentation that describe in detail how the system achieves the requirements and requirement gaps identified during the Requirements Review. The Provider Data Management System product demonstration and associate base system documentation are the starting points for the gap assessment. The MPATH versions of the SDD documents will show a high-level system design of the system architecture that shows the application components and infrastructure. The SDD documents are detailed design specifications for each application component. Updated SDD documents that reflect DPHHS specific needs will be the basis for the MAXIMUS software developers to

make coding changes and testers to create the system test scripts. Each SDD describes the purpose of the application component, includes a screen shot or report simulation, and has mappings of the web page and report data fields to the associated database tables and attributes. The field descriptions include edits and error messages, calculations and any special processing requirements.

Similar documentation is created for the conversion and interfaces analysis and design efforts. However, rather than screen and report designs, data file mappings for the extraction, transformation and loading are described. The Interface Control Document contains all of the specifications for all external data exchanges. The Data Management, Conversion, and Migration Plan contains a high level design that shows all of the conversion data sources, extract files, staging tables and transformation and load process that will be used to complete conversion.

Test script development starts with the creation of user stories and use cases during the design phase. These user stories, in conjunction with the SDDs are used to create test cases and test scripts. Test scripts are reviewed and confirmed by MAXIMUS Business Analysts, Software Developers, and DPHHS Subject Matter Experts to confirm that the expected results of each test match the expectations of everyone involved.

3.10.7.4 User Documentation

MAXIMUS develops user documentation during the initiation phase. This documentation is then updated and revised as necessary throughout the life of the project. MAXIMUS user documentation is written at a level that will allow a novice business user to successfully learn and navigate the system.

MAXIMUS documentation is written in a procedural step-by-step format that helps users understand the purpose and operation of the application components for each business process and major program/functional area. Acronyms and abbreviations are qualified and described to be consistent with windows, screens, reports, and the data element dictionary. User documentation includes system navigation, online help, and policies and procedures. All documentation is available to users on-line, with key word search capability and context-sensitive help.

We deliver most documentation in PDF format, but for those documents in a different format, PDF versions can be created upon request. SharePoint provides version control to retain historical versions of documentation and allow users to clearly see revisions. MAXIMUS writes and organizes User documentation so that novice users can learn how to access the on-line windows/screens, read reports, and perform all other user functions from reading the documentation. All user manuals and deliverables contain a table of contents and an index. Whenever possible, we try to define codes once and reference them throughout the document to build in consistency. Similarly, we describe error and system messages with an explanation of what system or user action generates the message and all potential actions the user may take to resolve the message.

3.10.7.5 Technical Documentation

MAXIMUS technical documentation is essential to our maintenance of three state applications, each with common and unique characteristics. We made creation of good documentation a priority so that we can more easily support multiple implementations. Our software is documented at the code level and matched for consistency with the SDD documents to verify that business and technical design documentation are in agreement. The technical documentation includes a description of all environments to include

development and unit test, system test, integration test, conversion and interfaces test, training, user acceptance test, production and additional environments as needed. The technical documentation includes unit test checklists, procedures for version control, release builds, and migration. In addition, the procedures used for smoke testing and backing out a release are described.

The high-level architecture documentation is contained in the Solution Architecture Document. The Solution Architecture Document includes a technical explanation of all aspects of the solution including detailed architectural diagrams, data flows, technical specifications, SaaS specifications, COTS products descriptions, and maintenance/upgrade schedules and hosting environment details. We use a method very similar to the Architecture Tradeoff Analysis Method (ATAM) method for evaluating the proposed platform architecture relative to the enterprise goals to identify risks that would inhibit the achievement of Agency's business goals.

3.10.7.6 Testing Documentation

We create and submit two primary test planning deliverables to the Department that 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. Second, the System Test Plan will conform to the requirements as set forth in Appendix 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.

Test script development starts with the creation of user stories and use cases during the design phase. These user stories, in conjunction with the SDDs are used to create test cases and test scripts. Test scripts are reviewed and confirmed by MAXIMUS Business Analysts, Software Developers, and DPHHS Subject Matter Experts to confirm that the expected results of each test match the expectations of everyone involved.

3.10.7.7 Certification Documentation

MAXIMUS certification preparation begins with a full list of certification tasks that we integrate into the larger System Implementation plan. To finalize the list of certification tasks, MAXIMUS will review the certification plan tasks with the State to validate the tasks, work products, schedule dates, task dependencies and both State and MAXIMUS responsibilities.

The Certification Plan provides the roadmap for achieving federal certification within State timeframes. Not only do we develop a thorough and detailed Certification Plan, we also incorporate certification steps into other plans, such as the Test Management Plan and Implementation Plan. The tasks and activities involved in our certification approach are guided by the project’s Certification Plan. This required deliverable will be submitted to the Department according to the PWPW and outlines the tasks and planning activities required to achieve federal certification. Our submitted Certification Plan will contain the required content as specified in requirement DOC02 as specified in Appendix F.

3.10.7.8 Operations and Maintenance Documentation

MAXIMUS will develop and maintain an Operations, Maintenance, and Configuration (OM&C) Plan for the Department's approval that contains the necessary documentation and procedures that describe the MPATH architecture and hosting. O&M procedure documentation contained in this plan includes all the procedures for monitoring and reporting daily operations, system performance, and SLAs. It also discusses the regularly scheduled and ad hoc maintenance procedures, and maintenance for system, training, and end user documentation.

The OM&C Plan is the central source of information for all O&M activities that describes how the system will be implemented and maintained for years to come. MAXIMUS is not proposing an incremental implementation. On prior system implementations in Nebraska and the District of Columbia, we implemented over 90 percent of the planned functionality in the initial release. This "big bang" implementation approach was possible as a result of extensive application, conversion and interface testing, followed by carefully executed operational readiness and implementation planning. In addition to the documentation previously discussed, the OM&C Plan describes all of the post implementation activities:

- The rollout approach and implementation schedule
- Post implementation production deployment process and activities
- Data exchange and integration approach
- Approach to continuous integration of other modules or data from other data providing entities
- MAXIMUS, State and Other Contractor and Stakeholders roles and responsibilities
- Production staff support roles and responsibilities as well as any on-call requirements
- Technical support desk response requirements and timelines

MAXIMUS documents additional O&M activities in other project deliverables. Specifically:

- The proposed implementation schedule (Project Work Plan)
- The rollback strategy (Disaster Recovery Plan)
- Communication and Contractor support procedures (Communication Plan)
- The go/no-go decision and system acceptance criteria
- All critical tasks that are required for cutover (Operational Readiness Review Checklist and Project Work Plan)
- Tools and processes to deliver overall quality (Quality Management Plan)

3.10.7.9 Documentation Requirements

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

ID	Documentation Requirement	MAXIMUS Summarized Response
DOC01	The Contractor shall develop, execute, maintain and deliver for the State's approval, a System Security Plan (SSP) that will document the current level of security controls within the module scope of work that protects the confidentiality, integrity and availability (CIA) of the solution and its information. This is a living document and will be updated no less than annually and when new vulnerabilities are identified and mitigated and when additional functionality and/or components are implemented. The System	MAXIMUS will develop, execute, and maintain a system security plan. The SSP contains all of the topics defined by the RFP. This document is a living document and is updated annually at a minimum. MAXIMUS will not move any state data into the solution until this plan is approved by the State.

ID	Documentation Requirement	MAXIMUS Summarized Response
	Security Plan must be approved before any State data is transferred or entered into the solution. The State must approve all revisions of the System Security Plan. If the Contractor's solution is hosted by the State, the State will provide supporting information to the Contractor to complete the SSP. The SSP must address the following topics: • Adherence to the State's requirements outlined in the "Security and Privacy Controls Requirements" document, included in the Procurement Library; • Compliance with the Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Safeguards (ARS) to assess CIA and NIST SP 800-53 Rev 4 at a "moderate" control level; • Data center physical security; • Network segmentation, access controls, and forensics; • Perimeter security; • Application security and data sensitivity classification, including Protected Health Information (PHI) and Personally Identifiable Information (PII); • End-point protections such as multiple redundant firewalls and host-based intrusion detection systems; • Identification and prevention of the use of prohibited functions, ports, protocols, and services; • Network, firewall, server and other security-related configurations and changes; • Intrusion detection and prevention; • Network scanning tools; • Host hardening; • Internet filtering; • Remote access; • Encryption of data at rest and in transit; • User authentication and directory services; • Interfaces and exchange of data with external entities; • System penetration testing; • Management of operating system and security patches; • Anti-Virus and malware detection and email gateways; • Assessment and testing of system and code modifications; and • Allowable internal and external communication protocols. • Compliance with the Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance or documented NIST 800-53 rev 4 at a "moderate" system risk assessment designation for Contractor hosted solutions; • Compliance with Statement on Standards for Attestation Engagements (SSAE-16) SOC 1 Type 2; • Compliance with Statement on Standards for Attestation Engagements (SSAE-16) SOC 2 Type 2.	Refer to *Section 3.10.1–Architecture* for more information on the System Security Plan (SSP).
DOC02	The Contractor shall develop and maintain a Certification Plan that defines the contractor's approach to CMS certification. It must describe the processes and procedures that will be used to manage Certification requirements. The Certification Plan must comply with the most current MECT process to ensure the system will meet all certification requirements.	MAXIMUS develops and maintains a Certification Plan that defines the MAXIMUS approach to CMS certification. This plan confirms that the system meets all MECT processes and checklists for certification. MAXIMUS has managed the certification process in Nebraska and District of Columbia, and is experienced in working with these checklists to deliver a certification package. Refer to *Section 3.10.3–Certification* for more detail on the Certification Plan.
DOC03	The Contractor shall develop, submit, and maintain a Data Management, Conversion and Migration Plan to include the following:	MAXIMUS develops, delivers, and maintains a Data Management, Conversion and Migration plan. This plan meets all of the requirements defined in the

ID	Documentation Requirement	MAXIMUS Summarized Response
	a. A data management strategy that will support integration, optimization, quality, stewardship, standards, and governance of data. b. description of appropriate skill sets, processes, technologies/tools, and any naming conventions followed. c. Approach to conversion, cleansing and migration. d. Approach to risk management for data conversion effort. e. Approach for testing migration or converted data; f. Approach to reporting the number of records successfully converted vs. errors or exceptions. g. Approach for cleansing data to prepare it for loading to the proposed solution that is refined as necessary. h. Approach to resolving data conversion errors and issues. i. Approach for supporting the Department validation of converted data. j. Tasks, timelines, and responsible parties for all conversion and migration tasks. k. Entrance and exit criteria for each phase of the effort.	RFP. MAXIMUS has managed data and conversion on each system they have developed. The approach is defined in *Section 3.10.2.5–Data Management*.
DOC04	Prior to beginning design and configuration/build activities, the Contractor must develop and submit to the State an Application Configuration and Maintenance Plan that describes the Contractor's approach to applications configuration and enhancements including: a. Approach to conducting design sessions or walkthroughs. b. Approach to conducting sprints or iterations. c. Configuration management. d. Schedule of major and minor releases. e. Tasks, timelines, and responsible parties for design and configure/build tasks. f. Approach to system enhancements g. Programming and coding standards The plan must be maintained through the system implementation. Revisions must be approved by the State.	MAXIMUS develops and delivers an Application Configuration and Maintenance Plan. This plan defines how design sessions, walkthroughs, iterations, etc. are completed. It defines the solution's configuration management and MAXIMUS maintains the plan throughout the life of the system. For more information on the MAXIMUS approach, see *Section 3.10.2.4–Design, Configuration Build Approach.*
DOC07	The Contractor shall provide during the initiation phase of the project and maintained throughout the project user documentation. The State requires User Documentation for use by a novice business user to understand the automated system or application from a business function perspective. The Contractor shall provide comprehensive, well-organized user documentation. The Contractor's User Documentation shall include at a minimum: • Written in a procedural step-by-step format. (Instructions for sequential functions must follow the flow of actual activity). • Manuals that helps users understand the purpose and operation of the module/module component(s) for each business process/major program/functional area. • Acronyms used in user instructions must be identified and must be consistent with windows, screens, reports, and the data element dictionary. • Cover system navigation, online help, and policies and procedures. • The documentation must be available on-line and provide an on-line search capability with context-sensitive help. • Provide the ability to produce a PDF version upon request • Use version control to retain historical versions of documentation and revisions must be clearly identified. • User documentation must be written and organized so that novice users can learn from reading the documentation how to access the on-line windows/screens, read reports, and perform all other user functions. • User manuals must contain a table of contents and an index.	MAXIMUS provides user documentation during the initiation phase. This documentation is then maintained throughout the project. The documentation is written at a level that would allow a novice business user to navigate the system. Refer to Section *3.10.7.4–User Documentation*.

ID	Documentation Requirement	MAXIMUS Summarized Response
	• Definitions of codes used in various Sections of a user manual must be consistent. • Descriptions of error messages for all fields incurring edits must be presented and the necessary steps to correct such errors must be provided. • Abbreviations must be consistent throughout the documentation. • Each user manual must contain a Section describing all reports generated within the subsystem, which includes the following: A narrative description of each report. The purpose of the report. Definition of all fields in the report, including detailed explanations of calculations used to create all data and explanations of all subtotals and totals. Definitions of all user-defined, report-specific code descriptions; and a copy of representative; and pages of each report. Instructions for requesting reports or other outputs must be presented with examples of input documents and/or screens. • Instructions for making on-line updates must clearly depict which data and files are being changed.	
DOC08	The Contractor shall develop and maintain annually, a Business Continuity and Disaster Recovery Plan that must be in place before any Department data is transferred or entered into the solution. The Plan must contain procedures for data backup, restoration, and emergency mode operations in the event of: a. Hardware or Software Failures; b. Human Error; c. Natural Disaster; and/or d. Other unforeseeable emergencies. The Business Continuity and Disaster Recovery Plan must be approved by the Department.	MAXIMUS will develop and maintain a Business Continuity and Disaster Recovery Plan. This plan is in place before any Department data is transferred or entered into the solution. This plan is submitted for review and approval by the Department. This plan discusses the disaster recovery testing that will be performed by MAXIMUS prior to go-live, and how these will be completed. Refer to *Section 3.10.2.8–Implementation and Acceptance*.
DOC09	The Contractor's Business Continuity portion of the plan must include the following: a. Identification of the core business processes involved in the production solution. For each core business process include: 1) Identification of potential failures for the process; 2) Risk analysis; 3) Impact analysis; and 4) Definition of minimum acceptable levels of service/output. b. Definition of triggers for activating contingency plans. c. Procedures for activating any special teams for business continuity. d. A plan for recovery of business functions, units, processes, human resources, and technology infrastructure. e. Communication protocols and process for restoring operations in a timely manner.	The Business Continuity plan includes the following information: ■ Identification of the core business processes ■ Triggers for activating contingency plans ■ Procedures for activating special teams ■ Plan for recovery of business functions, units, processes, human resources and technology infrastructure ■ Communication protocols and processes for restoring operations Refer to *Section 3.10.2.8–Implementation and Acceptance*.
DOC10	The Contractor's Disaster Recovery portion of the plan must address, at a minimum: a. Retention and storage of backup files and software; b. Hardware backup for critical solution components; c. Facility backup; d. Backup for any telecommunications links and networks; e. Backup procedures and support to accommodate the loss of any online communications; f. A detailed file backup plan, procedures, and schedules, including rotation to an off-site storage facility.	The Disaster Recovery plan includes the following information: ■ Retention and storage of backup files and software ■ Hardware backup for critical solutions components ■ Facility backup ■ Backup for any telecommunications links and networks ■ Backup procedures and support to accommodate the loss of online communications ■ Detailed backup plan, procedures and schedules

ID	Documentation Requirement	MAXIMUS Summarized Response
	g. The off-site storage facility must provide security of the data stored there, including protections against unauthorized access or disclosure of the information, fire, sabotage, and environmental considerations. h. An enumeration of the prioritized order of restoration for Contractor's proposed solution. i. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	▪ Off-site storage facility security information ▪ Prioritized order of restoration ▪ Availability of a short term power supply to allow for a systematic shut down of the system Refer to *Section 3.10.2.8–Implementation and Acceptance.*
DOC11	The Contractor shall update all project documentation (e.g., system design documentation, user and training documentation) as necessary throughout all phases of the project.	MAXIMUS updates all project documentation throughout the life of the project. We submit each update to the Department for approval. Refer to *Section 3.10.7–Deliverables.*
DOC12	The Contractor shall provide and maintain an Operations, Maintenance and Configuration Plan for the Department's approval that describes post-implementation processes for areas such as: a. Architecture/hosting operations. b. Monitoring daily operations performance. c. Performing routine maintenance. d. Maintaining user documentation. e. Online help approach and documentation, as appropriate. f. Configuration and change management. g. Approach to enhancements and other new requirements. h. Maintaining system documentation. i. Maintaining training documentation. j. Archiving requirements. k. Tasks, timelines, and responsible parties for design and configure/build tasks. l. Reporting status against relevant Service Level Agreements (SLAs) m. Schedule of major and minor releases. The Department must review and approve all revisions of the Operations, Maintenance and Configuration Plan.	MAXIMUS builds and maintains an Operations and Maintenance and Configuration that addresses all the elements of Operations and Maintenance to include batch processing schedules, change control and maintenance procedures, build/release procedures and schedule, training documentation maintenance and SLA monitoring and reporting. Refer to *Section 3.10.2.8–Implementation and Acceptance.*
DOC13	The Contractor shall develop a Module Implementation Plan in conjunction with the State that describes, at a minimum: a. The rollout approach, including phased implementation, if necessary. b. Overall integration approach c. Approach to continuous integration of other modules or data from other data providing entities. d. The proposed implementation schedule. e. The rollback strategy. f. Communication and Contractor support procedures. g. Contractor and State roles and responsibilities. h. Operational Readiness Checklist(s) that defines, in advance, the go/no-go decision, and all aspects of Contractor, solution, and State readiness. i. All critical tasks that are required for cutover. j. Post cutover monitoring. k. The onsite and offsite user support provided by the Contractor and State during the initial solution implementation. l. Solution acceptance procedures. m. Tools and processes to ensure overall quality. n. Describe post implementation production deployment process and activities.	MAXIMUS develops and delivers a Module Implementation Plan that meets the requirements outlined in the RFP. This plan indicates 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 that there are critical issues that need to be pulled out of the most integrated system. The plan identifies all of the steps to be made toward receiving a go/no-go decision from the Department, including Roles and Responsibilities for all stakeholders. Refer to *Section 3.10.2.8–Implementation and Acceptance* for additional discussion about the implementation approach.
DOC14	The State defines System Design Document (SDD) as documentation that describes how the functional and nonfunctional requirements recorded in the	MAXIMUS develops and delivers System Design Documentation for each module. This documentation

ID	Documentation Requirement	MAXIMUS Summarized Response
	Requirements Response Matrix transform into more technical system design specifications from which the system is configured and built. The SDD documents the high-level system design and the low-level detailed design specifications. The SDD describes design goals and considerations, provides a high-level overview of the system architecture, and describes the data design associated with the system, as well as the human-machine interface and operational scenarios. The high-level system design is further decomposed into low-level detailed design specifications for each system component, including hardware, internal communications, software, system integrity controls, and external interfaces. The SDD documents and tracks the necessary information required to effectively define architecture and system design in order to give the development team guidance on the architecture of the system to be developed. Design documents are incrementally and iteratively updated during the system development life cycle and includes proprietary contractor material (this excludes proprietary information related to COTS products). Its intended audience is the project manager, project team, and development team. The Contractor shall provide and maintain system design documentation that includes at a minimum: • A description of each component, their purpose, including basic functions and the business areas supported • User stories/use cases • User interface design • Physical database design • A module system diagram, including all components, identifying all business process diagrams, data flows, systems functions, and their associated data storage • Configurations • Job streams within each module, identifying programs, inputs and outputs, control, job stream flow, operating procedures, and error and recovery procedures. • A network schematic showing all network components and technical security control • Listing of the edits and audits applied to each input item and the corresponding error messages. • Interface Control Documentation • Narrative descriptions of each of the reports and an explanation of their use must be presented. • Definition of all fields in reports, including a detailed explanation of all report item calculations.	includes all of the information required to define the functional and technical details of each module involved in the solution. For more information regarding system design, see *Section 3.10.7.3–Design Documentation* and *Section 3.10.2.4–Design Configuration Build.*
DOC15	The Contractor shall develop and maintain a Communication Plan. The purpose of the Communication Plan is to provide a description of the communication that will occur on the project and how it will be managed. This includes details about various types and means of communication, communication channels, communication flow within the organizational structure, escalation, guidelines for meetings, dissemination of knowledge, and communication effectiveness. The Communication Plan shall ensure that the communication approach addresses communication across multiple vendors. Effective communication is a key element for the success of the project.	MAXIMUS develops and maintains a Communication Plan and communication matrix. This plan describes the communication types that will occurs on the project and how communication will be managed. The Communication a matrix describes each communication event, who initiations the communication, the method(s) of communication and who, primary and secondary recipients that will receive the communication. Refer to *Section 3.10.2.1.1–Communication Plan.*
DOC16	The Contractor shall develop and maintain a Quality Management Plan. The Quality Management Plan identifies the quality standards for the project and how quality standards are measured. It includes the process steps and quality tools that will be used (e.g., templates, standards, and checklists).	MAXIMUS develops and maintains a Quality Management Plan that identifies the quality standards for the project and how they are

ID	Documentation Requirement	MAXIMUS Summarized Response
		measured. Refer to *Section 3.10.2.1.5–Quality Management Plan.*
DOC18	The Contractor shall develop and maintain a Change Management Plan. The Change Management Plan must include the following elements. a. Tools to support change management b. Change management process steps c. Escalation process d. Training e. Roles and Responsibilities	MAXIMUS develops and maintains a Change Management Plan that meets the requirements identified in the RFP. Refer to *Section 3.10.2.1.3–Change Management Plan & WBS.*
DOC19	The Contractor shall provide and maintain Technical Documentation including written description of module component(s) design, function and architecture that will provide guidance to system developers. Additionally, the Contractor must include a detailed list of all environments, each environments' IT technologies including software, middleware, hardware, utility applications, development tools, testing tools, and provides detailed information on the programming languages and protocols used.	MAXIMUS provides and maintains Technical Documentation including component design, function, and architecture. It also includes a definition of each environment. Refer to *Section 3.10.1–Architecture* and *Section 3.10.7.5–Technical Documentation.*
DOC21	The Contractor shall provide a Solution Architecture Document. The Solution Architecture Document includes a technical explanation of all aspects of the solution including detailed architectural diagrams, data flows, component specifications, SaaS, COTS products and hosting environment details. The document will include architectural tradeoffs using the Architecture Tradeoff Analysis Method (ATAM) method or other suitable method for evaluating the proposed platform architecture relative to the enterprise goals to identify risks that would inhibit the achievement of Agency's business goals.	MAXIMUS delivers and maintains a Solution Architecture Document that explains all aspects of the solution. Refer to *Section 3.10.1–Architecture* and *Section 3.10.7.7–Technical Documentation.*
DOC22	The Contractor shall develop and maintain a Defect Management Plan that describes the process of submitting, monitoring and resolving defects. The plan will detail the following: a. Approach and tools utilized to assign, identify, prioritize, track, resolve, and test system defects. b. Approach to defect severity categorization using an industry standard methodology. c. Approach to reporting and documenting defects. d. Describe how the Contractor will work collaboratively with other State healthcare programs enterprise vendors. e. Describe the defect management processes related to all test types and levels in the RFP (e.g., the relationship between defect resolution and the coordinated test case execution). f. Describe the defect management processes after implementation.	MAXIMUS develops and maintains a Defect Management Plan that details how defects are prioritized, tracked, assigned, and worked. Refer to *Section 3.10.2.6–Testing.*
DOC24	The Contractor shall submit and maintain a Staffing Plan as part of the Project Management Plan. The Staffing Plan must include: a. Identify the roles and responsibilities by resource type throughout all phases of the contract, including identifying key and non-key personnel as well as FTE allocation for all personnel. b. Staffing Levels (estimated by resource type by phase for the duration of the project) to be reported in the Resource Allocation Matrix. c. Detail how the staffing levels shall achieve consistent, dependable service regardless of changes that may influence work volume. d. Detail differentiated by Proposer staff, subcontractor staff, if applicable, and State project staff. e. Identify total hours to be expended, per phase or effort, and for the entire project, by Proposer staff and by State project staff. f. Tools and processes used to screen available staff and fill positions. g. Expectations regarding onsite time for contractor resources h. Process for temporarily and permanently replacing vacancies in key personnel and other manager/lead positions consistent with staffing SLAs.	MAXIMS provides and maintains a Staffing Plan as part of the Project Management Plan. This plan includes roles and responsibilities, staffing levels, sub-contractor staff, hours to be expended by phase, processes for filling positions, expectations for onsite time, and process for replacing vacancies. Refer to *Section 3.10.2.1.4–Staffing Management Plan.*

ID	Documentation Requirement	MAXIMUS Summarized Response
DOC26	The Contractor shall develop, submit and maintain a Master Test Plan that describes the Contractor's plan for all testing activities, processes, types and levels. Testing must be as automated and self-documenting as possible (e.g., continuous unit testing). At a minimum, the Master Test Plan must address the following: a. Overall testing strategy for the following testing types: unit testing, system testing, integration testing, regressing testing, parallel testing, performance and load testing, manual and automated and/or scripted testing, disaster recovery and end-to-end integration testing of COTS products if any. b. Approach to planning and preparing the test/staging environment c. Approach to conducting each test level. d. Approach for supporting UAT. e. Approach for testing nonfunctional requirements. f. Approach to test documentation (e.g., test cases, test scripts, test case matrices added as design progresses). g. Approach to quality control/quality assurance. h. Approach to bi-traceability to requirements and design. i. Tools, techniques, and methods. j. Reporting mechanisms, traceability and metrics. k. Defects and defects resolution. l. Entrance and exit criteria for each test level including alignment with industry standards. m. Configuration management for each test level n. Testing roles and responsibilities o. Acceptance Criteria shall include but is not limited to; no high or critical defects in code released to production and production releases will not be promoted if more than 5% of requirements have an open defect	MAXIMUS develops and maintains a Master Test Plan that defines the process for each level of testing and how it is supported and managed. Refer to *Section 3.10.2.6–Testing*.
DOC27	The Contractor shall develop and submit a Training Plan that, at a minimum, addresses the following: a. Summary of training approach that focuses on the train-the-trainer methodology, objectives, and desired outcomes. b. Training needs analysis, including an assessment of the target audience and their knowledge and skills. c. Recommendations on type and delivery approach based on training needs analysis. d. Summary of proposed training materials and documentation in addition to hands-on training. e. Approach to maintaining training documentation and accompanying materials. f. Approach to providing training necessary to support new functionality and/or major software releases that materially change the user interaction. g. Approach to processing for incorporating feedback to improve train the trainer effectiveness over the course of the Contract.	MAXIMUS develops and delivers a Training plan that identifies the training methodology and approach. The plan is written to meet all of the requirements identified in the RFP. Refer to *Section 3.10.2.7–Training*.
DOC28	The Contractor shall develop in collaboration with the Department, a System Test Plan that describes the Contractor's System Testing approach and includes at a minimum the following: a. Test Coverage b. Walkthroughs and Inspections c. Test Data Considerations d. Entrance Criteria e. Exit Criteria f. Configuration Management g. Testing Documentation h. Process Steps i. Inputs to System Testing	MAXIMUS delivers a System Test Plan that describes our approach to system testing. It identifies the process for system test as well as the test cases that are to be included. Acceptance Criteria is met before System Test is considered complete. Refer to *Section 3.10.2.6–Testing*.

ID	Documentation Requirement	MAXIMUS Summarized Response
	j. Outputs for System Testing k. Metrics l. Pass/Fail Criteria m. Suspension Criteria and Resumption requirements n. Testing Deliverables o. Testing activities p. Resources, Roles and responsibilities q. Testing Tools r. Meetings and Communication s. Acceptance Criteria shall include but is not limited to; no high or critical defects in code released to production and production releases will not be promoted if more than 5% of requirements have an open defect.	
DOC29	The Contractor shall provide during the initiation phase of the project and maintain throughout the project, system documentation that at a minimum includes: • A description of each component, their purpose, including basic functions and the business areas supported • User stories/use cases • Screen layouts, report layouts, and other output definitions, including examples and content definitions • Physical database design • A module system diagram, including all components, identifying all business process diagrams, data flows, systems functions, and their associated data storage • Configurations • Job streams within each module, identifying programs, inputs and outputs, control, job stream flow, operating procedures, and error and recovery procedures. • A network schematic showing all network components and technical security control • Listing of the edits and audits applied to each input item and the corresponding error messages. • As applicable, listing and description of all control reports • Interface Control Documents • Narrative descriptions of each of the reports and an explanation of their use must be presented. • Definition of all fields in reports, including a detailed explanation of all report item calculations. • Operations Procedure Manual • Data Dictionary	MAXIMUS provides system documentation during the initiation phase of the project. The system documentation includes: ■ A description of each component, their purpose, including basic functions and the business areas supported ■ User stories/use cases ■ Screen layouts, report layouts, and other output definitions, including examples and content definitions ■ Physical database design ■ A module system diagram, including all components, identifying all business process diagrams, data flows, systems functions, and their associated data storage ■ Configurations ■ Job streams within each module, identifying programs, inputs and outputs, control, job stream flow, operating procedures, and error and recovery procedures. ■ A network schematic showing all network components and technical security control ■ Listing of the edits and audits applied to each input item and the corresponding error messages. ■ As applicable, listing and description of all control reports ■ Interface Control Documents ■ Narrative descriptions of each of the reports and an explanation of their use must be presented ■ Definition of all fields in reports, including a detailed explanation of all report item calculations ■ Operations Procedure Manual ■ Data Dictionary Refer to *Section 3.10.2.4–Design Configuration and Build.*
DOC37	At least twelve (12) months before the start of the final Contract year (including option years that have been exercised) the Contractor shall provide, a Turnover Plan to the Department. The Plan will include: a. Proposed approach to turnover. b. Tasks and subtasks for turnover. c. Schedule for turnover. d. Updated operational tasks and procedures during turnover.	MAXIMUS provides a Turnover Plan 12 months prior to the start of the final contract year. We write the plan to meet RFP requirements. Refer to *Section 3.10.6–Turnover.*

ID	Documentation Requirement	MAXIMUS Summarized Response
	e. Description of vendor coordination activities that will occur during the turnover task and implementation of the activities to ensure continued system and services as deemed necessary by the Department. f. List of incomplete tasks, such as system defects, modifications or enhancements, mass adjustments, reference updates, and configuration requests. g. A detailed description of the services that would be required by another Contractor to fully take over system, technical, and business functions outlined in the Contract. The description shall also include an estimate of the number and type of personnel required to support the technical platform and supporting services. h, The data and documentation shall be organized in a format required by the State (e.g., by provider unique ID and provider name).	
DOC38	The Risk Management portion of the Project Management Plan must describe at a minimum: a. Proactive identification and analysis of risks before they become issues. b. Development of risk avoidance, transfer, mitigation or management strategies. c. Approach to monitoring, communicating, reporting of risk status including procedures for documenting, resolving, and reporting issues and risks identified by the Contractor, the Department or other project contractors. d. Approach to root cause analysis. e. The appropriate methods, tools, and techniques for active and ongoing identification and assessment of project risks. f. Describe how risks will be quantified and qualified.	MAXIMUS develops a Risk Management Plan as part of the Project Management Plan. This plan is written to include at a minimum, the following: ■ Identification and analysis of risks before they become issues ■ Description of risk avoidance, transfer, mitigation, or management strategies ■ Approach to monitoring, communicating, reporting of risk status including procedures for documenting, resolving, and reporting issues and risks identified by the Contractor, the Department or other project contractors ■ Approach to root cause analysis ■ The appropriate methods, tools, and techniques for active and ongoing identification and assessment of project risks ■ Description of how risks will be quantified and qualified Refer to *Section 3.10.2.1.6–Risk Management.*
DOC40	The Issues Management Plan portion of the Project Management Plan must describe at a minimum: a. Approach to issue management. b. Issue management process steps including: -Approach to prioritizing, tracking, escalating, communicating, reporting issues -Approach to documenting, reporting, and resolving issues identified by the Contractor, the Department or other module contractors. -Approach to impact analysis. c. Tools, and techniques for active and ongoing identification and monitoring of project issues. d. Roles and responsibilities. e. Describe how issues will be quantified and qualified.	MAXIMUS delivers an Issues Management Plan as part of the Project Management Plan that describes at a minimum: ■ Approach to issue management ■ Issue management process steps including: • Approach to prioritizing, tracking, escalating, communicating, reporting issues • Approach to documenting, reporting, and resolving issues identified by the Contractor, the Department or other module contractors • Approach to impact analysis ■ Tools and techniques for active and ongoing identification and monitoring of project issues ■ Roles and responsibilities ■ How issues will be quantified and qualified Refer to *Section 3.10.2.1.7–Issue Management Plan*
DOC41	The Contractor shall provide a Deliverable Expectations Document (DED) for each deliverable that describes the purpose, content, applicable MECT minimum required content and industry standards (e.g., PMI, IEEE/ISO, CMS XLC) that are satisfied for each Deliverable. Each DED is a deliverable.	MAXIMUS provides a Deliverable Expectations Document for each deliverable in accordance with the Documentation standards. Refer to *Section 3.10.7.1–Deliverable Expectation Document.*
DOC42	The Contractor shall develop a comprehensive Operations Procedure Manual which shall provide guidelines for the operation and use of the module and/or module component(s). At minimum the Operations Procedure	MAXIMUS delivers an Operation Procedure manual to provide guidelines for the operation and use of

ID	Documentation Requirement	MAXIMUS Summarized Response
	Manual shall contain policies, processes and workflows for the module and/or module component(s).	modules. Refer to *Section 3.10.2.8–Implementation and Acceptance.*
DOC44	The Contractor shall maintain Attachment L- Technology Matrix, and deliver annually for the Department for review.	MAXIMUS maintains *Attachment L–Technology Matrix* and delivers it to the Department annually.
DOC46	The Contractor shall provide a User Interface Style Guide or equivalent document defining the design standards for user interfaces. The User Interface Style Guide must demonstrate how the solution meets the most current MECT user interface requirements including: a. User ability to customize or make adjustments (e.g. language support, font size) to portal presentation. b. Users utilizing scripting languages and/or assistive technology have the ability to access the information, field elements, and functionality required for electronic form or page completion and submission including directions and cues. c. User Interface organization so documents are readable without requiring an associated style sheet. d. User Interfaces identifying row and column headers for data tables. e. User Interfaces informing users when a timed response is required and given sufficient time to indicate more time is required. f. User Interfaces providing a method that permits users to skip repetitive navigation links. g. User Interfaces provide text titles for frames to facilitate frame identification and navigation. h. User Interfaces use markup to associate data cells and row/header cells for data tables that have two or more logical levels of row or column headers.	MAXIMUS provides a user interface style guide to define the standards for user interfaces. This style guide demonstrates how the solution meets the MECT user interface requirements. We assembled documentation to demonstrate compliance during the R3 certification review for the State of Nebraska. We will consolidate these and other artifacts into a User Interface Style Guide to define the standards for user interfaces. This Style Guide can be used as an artifact as the State prepares for R2 and R3 milestone reviews with CMS. Refer to *Section 3.10.3.2 Certification Support Activities.*

3.10.8 Performance Standards

3.10.8 Performance Standards

Performance standards for phases of the project are defined in Attachment F – Requirements Matrix. Performance standards as well as associated liquidated damages for unmet standards are also defined in Attachment J, Service Level Agreement Requirements. The Offeror must describe their approach to meet the Performance Standards requirements defined in Attachment F, Requirements Matrix and Attachment J, Service Level Agreements.

MAXIMUS understands that liquidated damage penalties may be assessed if the performance measures in Attachment J – Service Level Agreements Requirements are not met.

MAXIMUS will employ a Service Level Management (SLM) process to capture the SLAs and provide monitoring and reporting as depicted in *Exhibit 3.10.8-1: Service Level Management*. This process begins with definition of the SLM Framework that contains the underlying service contract along with the contractual and performance standards. The next step is to develop documentation of the service requirements. Documentation for each requirements includes definition of the methods for measurement, acceptance criteria, the reporting method, and the process for corrective action. Once the SLAs are clearly defined, the next SLM process is to "perform" the services required. The monitoring step captures the metrics throughout the performance period and provides the data that will be analyzed and reported at the end of the reporting period. In the reporting step, the performance metrics are compared to the contract SLA targets and the pass/fail results are then circulated to all parties responsible for SLA oversight. In the event one or more SLA targets are missed or at risk of missing future targets, corrective actions are defined, tested and implemented as soon as possible.

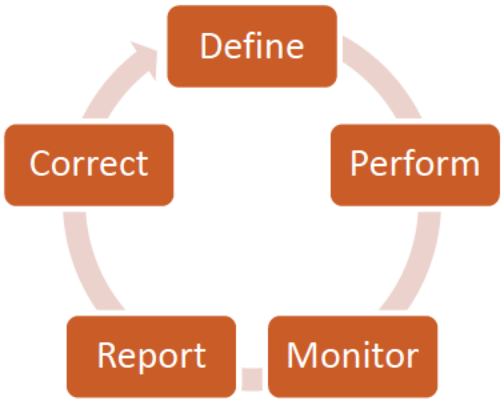


Exhibit 3.10.8-1: Service Level Management. *Our SLM process is a circular approach that continues to identify performance improvement opportunities and implement them throughout the life of the contract.*

During the DDI phase of the project, an automated dashboard is used for tracking all project contract compliance SLAs. The SLA dashboard, an excerpt of which is shown in *Exhibit 3.10.8-2: MPATH SLA Dashboard*, will be easily accessible, 24x7, by all parties with DPHHS authorized access. Responsible MAXIMUS team members will record and upload the performance data to the register within 24 hours of when an SLA event has occurred, or whenever the performance evaluation period (e.g. monthly) has ended. Some metrics will be updated based upon data captured from third party COTS applications and subsequently imported into the dashboard for automated calculation and evaluation. System test results and defect reporting data are examples of performance data that is continuously collected in JIRA and must be sampled and extracted to evaluate the SLA compliance standards. Other SLAs are manually tracked events such as submission of meeting agendas and distribution of the associated meeting minutes. These SLAs and other similar SLAs will need to be updated manually in the dashboard data repository. As the performance data for an SLA is entered or uploaded to the dashboard, the calculations in the dashboard are triggered and automatically compared to the performance standards to determine whether the SLA has been met. The SLA compliance result is instantaneously reflected on the dashboard.

CONFIDENTIAL

During Operations and Maintenance, MAXIMUS uses industry standard COTS tools that automatically track and report system response time and system availability. MAXIMUS relies on a product named Pingdom for capturing the data and providing accurate performance reporting of the system availability statistics. Pingdom is a service that tracks the uptime, downtime, and performance of websites. Pingdom monitors websites from multiple locations so that it can distinguish genuine downtime from routing and access problems.

Option B Operational performance metrics are tracked within the CRM component of our Provider Services Solution.

Performance Requirements

The following table includes Attachment F Performance Requirements for the Base and Option A. Responses to Option B Performance Requirements are documented in our response to 3.10.14 Option B Services .Below we provide our summarized response to each requirement.

ID	Performance Requirement	MAXIMUS Summarized Response
PRFM01	The Contractor shall develop a method for maintaining performance compliance with Service Level Agreements (SLA).	MAXIMUS will use a Service Level Management process to comply with the Service Level Agreements.
PRFM04	The Contractor shall meet Service Level Agreements and integrate tools for monitoring system and component performance and create the necessary reports or supply a dashboard to support SLAs.	MAXIMUS will use both automated and mechanical monitoring methods to inform the reports and dashboards necessary to give visibility to the achievement of the performance standards.

ID	Performance Requirement	MAXIMUS Summarized Response
PRFM05	The system shall track performance measures for each SLA requirement using predefined and ad hoc reporting methods	As part of the SLM process, MAXIMUS will define the reporting methods necessary to track performance for each SLA.
SLA01	Contractor must meet the due date for Acceptance of each Deliverable, as indicated in the Work Plan (excludes Implementation Acceptance as defined in Performance Standard #67).	MAXIMUS acknowledges that the due dates for Acceptance of each Deliverable are established to maintain the schedule integrity of the project and MAXIMUS will meet the specified due dates.
SLA02	Contractor shall ensure there are no more than two submissions of any Deliverable to gain Acceptance by the Department using the process defined in Section 7.3 of the Contract. A Deliverable that is not compliant with the Acceptance Criteria as defined in the applicable Deliverable Expectation Document (DED) will not gain Acceptance.	MAXIMUS acknowledges that we are allowed no more than two submissions of any deliverable to gain acceptance by the Department using the process defined in Section 7.3 of the Contract. The MAXIMUS team will maintain close communication with the Department to prevent avoidable misunderstandings or miscommunication that could lead to rejection of deliverables. MAXIMUS also has a well-established process for internal deliverable review prior to submission, which verifies deliverables that are well-written, thorough, and error-free.
SLA03	Contractor shall distribute meeting agendas to invitees at least 24 hours before the start of a scheduled meeting involving project stakeholders. Scheduled meetings include any reoccurring project meetings, meetings identified in the Work Plan or any meeting requested by the Department with at least 48 hours' notice. Contractor shall distribute meeting minutes to meeting attendees within two business days of the scheduled meeting.	The MAXIMUS project management team will distribute meeting agendas to invitees at least 24 hours before the start of a scheduled meeting involving stakeholders. MAXIMUS will distribute meeting minutes to meeting attendees within two business days of the conclusion of the scheduled meeting.
SLA05	Contractor's Key Personnel positions may not be vacant for more than 10 Business Days without a qualified substitute (temporary replacement). A qualified substitute must be in place no more than 10 Business Days after the separation date of the vacating resource. The definition of a qualified substitute is someone meeting the requirements of the RFP and Contract Section 4.	MAXIMUS acknowledges that Key Personnel positions may not be vacant for more than 10 business days without a qualified, temporary substitute. MAXIMUS has 18,000 employees worldwide and deep program expertise in Medicaid, which allows us to quickly identify qualified substitutes if a Key Personnel position becomes vacant.
SLA06	Contractor will have 60 calendar days from the vacancy date to fill a Key Personnel position with a permanent replacement (a position is considered vacant even with the substitute replacement serving in that role).	MAXIMUS acknowledges we will have 60 calendar days from the vacancy date to fill a Key Personnel position with a permanent replacement. MAXIMUS has a robust recruitment function designed to quickly identify and onboard candidates. Along with this recruiting capacity, MAXIMUS encourages the professional growth of its employees and makes positions available to internal candidates.
SLA09	Contractor shall ensure that 100% of all critical Priority tickets, (Enhancements, Deficiencies, Maintenance, Research, Configuration and Mass Adjustments) are completed and Implemented by the Required Implementation Date.	MAXIMUS uses Jira software for issue management. MAXIMUS will use reports and or a customized JIRA dashboard to monitor where in the process the critical tickets are. Each ticket can be given a due date and/or a planned release date.
SLA10	Contractor shall ensure that 80% of all high Priority tickets (Enhancements, Deficiencies, Maintenance, Research, Configuration and Mass Adjustments) are Implemented by the Required Implementation Date. Contractor shall ensure that 100% of all high Priority tickets (Enhancements, Defects, Maintenance, Research, Configuration and Mass Adjustments) are Implemented within five business days of the Required Implementation Date.	MAXIMUS uses Jira software for issue management. MAXIMUS will use reports and or a customized JIRA dashboard to monitor where in the process the critical tickets are. Each ticket will be given a due date and/or a planned release date to make sure that 80% of all high priority tickets are implemented on time and 100% of all high priority tickets are implemented within five business days of the required implementation date.
SLA11	Contractor shall ensure that 75% of all medium Priority tickets (Enhancements, Deficiencies, Maintenance, Research, Configuration and Mass Adjustments) are Implemented by the Required Implementation Date. Contractor shall ensure that 100% of all medium Priority tickets (Enhancements, Deficiencies, Maintenance, Research, Configuration and Mass Adjustments) are Implemented within 10 business days of the Required Implementation Date.	MAXIMUS uses Jira software for issue management. MAXIMUS will use reports and or a customized JIRA dashboard to monitor where in the process the critical tickets are. Each ticket will be given a due date and/or a planned release date to assure that 75% of all medium priority tickets are implemented on time and that 100% of all medium priority tickets are implemented within 10 business days of the required implementation date.

ID	Performance Requirement	MAXIMUS Summarized Response
SLA12	Contractor shall ensure compliance with all licensing agreements, required to support the proposed Solution and Services. Compliance is defined as the maintenance of licenses and appropriate permitted usage.	MAXIMUS will comply with all licensing agreements required to support the proposed solution and services.
SLA13	Contractor shall turn over any applicable Solution related licenses to the Department within 30 calendar days of the request.	MAXIMUS will turn over any applicable solution-related licenses to the Department within 30 calendar days of the request.
SLA14	Contractor shall thoroughly test the Solution and demonstrate proof of successful Contractor Testing for 100% of the Specifications defined for each Implementation. Contractor can demonstrate proof of successful Contractor Testing by providing Documentation such as system, integration or parallel test results or demonstration of the Specifications including Interfaces/APIs. All Specifications must be tested through the use of testing procedures, verification procedures and other testing methodologies identified in Contract Section 7, Section 3.10.2.6 of the RFP, and the associated testing requirements.	MAXIMUS will thoroughly test the entire Provider Services solution along with the specific modifications and enhancements. We will demonstrate proof of successful testing for 100% of the Specifications defined for each Implementation. MAXIMUS will create a Requirements Traceability Matrix (RTM) to indicate what types of tests are required, whether tests can be automated or manual, and the extent of the regression testing required. The RTM will be used to assess test coverage and test all specifications. Our Test Plan will document all items to be tested and will cross-reference the RTM for each release. The Test Plan will also indicate features and services that are excluded from testing.
SLA15	Contractor shall maintain environments as mutually agreed upon to perform System validation, integration testing, and Data migration to determine overall production readiness. Each environment must include all of the components to support the intended purpose of that environment. Any component not replicated in a designated environment must be disclosed to the Department and a written explanation as to why this will not affect the inherent use of the environment for its intended purpose.	MAXIMUS will establish and maintain all environments required, and mutually agreed upon, to perform system validation, integration testing, and data migration to determine production readiness. Each environment will include all of the components to support the intended purpose of that environment. Any component not replicated in a designated environment will be disclosed to the Department with a written explanation of why this will not negatively affect the use of the environment for its intended purpose.
SLA16	Contractor shall document all business rules applicable to the functioning of the Module and document any new or changed business rules within 10 Business Days of the implementation of a change.	MAXIMUS will document all business rules applicable to the functioning of the Provider Services module and document any new or changed business rules within 10 business days of the implementation of a change. Business rules are initially captured and documented in narrative format in the detailed design specification for the specific component within the application. The rules could be edit rules that relate to the entry/validation of data through the user interface, or a backend rule that relates to actions the system should take under certain conditions. Once the rules are documented and approved in the detailed design specification, we enter (or update) these rules in the Corticon Business Rules engine. To create rules that are easily understandable and human readable, MAXIMUS has put extensive effort into creating a vocabulary set. This vocabulary contains 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 technical business analysts 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, thereby creating documentation as changes are made to the rules.

ID	Performance Requirement	MAXIMUS Summarized Response
SLA17	Contractor's Solution shall ensure 100% of all Data Interfaces identified for the Enterprise Service Bus (ESB) integration are managed and orchestrated by the ESB.	MAXIMUS will ensure 100% of the data interfaces identified for the ESB integration are managed and orchestrated by the ESB.
SLA21	Contractor shall document 100% of all Configuration items applicable to the Solution and update Documentation within 10 Business Days of the Implementation of a change.	MAXIMUS will document 100% of the configuration items applicable to the solution and update the documentation within 10 business days of the implementation of a change.
SLA22	Contractor shall ensure that the Data integrity error rate and routing errors of any transaction is less than .001%.	MAXIMUS will ensure the data integrity error rate and routing errors of any transaction is less than .001%. MAXIMUS will using monitoring tools
SLA25	Contractor's Solution shall ensure Data received from real-time Interfaces will be accessible in the Module within three seconds at least 99% of the time; excluding batch interface updates. Performance is measured by a predefined sample measuring timestamp Data was received to the time the Data is available to query in the Module database or presented to the user via a Module user interface.	MAXIMUS will ensure that data received from real-time interfaces are accessible in our Provider Services module within three seconds at least 99% of the time, excluding batch interface updates.
SLA26	Contractor's Solution response time for user-initiated functionality related to the Data store including simple queries shall not exceed three seconds and for complex queries whose output is greater than 10,000 rows shall not exceed 30 seconds. Performance is measured by a predefined sample measuring from the user initiating simple query until return of accurate output. Also predefined sample measuring from the user initiating a complex query until the return of accurate output.	The Provider Services Solution response time for user-initiated functionality related to the Data store including simple queries will not exceed three seconds and for complex queries whose output is greater than 10,000 rows will not exceed 30 seconds.
SLA27	Contractor's Solution shall accommodate a user interface response time of two seconds or less per discrete transaction.	The Provider Services solution will accommodate a user interface response time of two seconds or less per discrete transaction.
SLA28	Contractor's Solution response time for adding, updating, or deleting Data from operational components shall not exceed three seconds per action. Performance is measured by a predefined sample measuring individually the adding, editing and deleting of Data. Measure from action to completion of process. Validate 1) appropriate action to Data was completed. 2) Review action history for timing.	The Provider Services Solution response time for adding, updating, or deleting Data from operational components will not exceed three seconds per action.
SLA29	Contractor must ensure all of the required Interfaces for the Module operate in accordance with the Specifications, without degradation in performance.	MAXIMUS will ensure all of the required interfaces for the Provider Services module will operate in accordance with the specifications, without degradation in performance.
SLA31	"Contractor must ensure all production reports will be available on line for review by the Department pursuant to the following schedule: A. Daily or Weekly Reports – by the end of the Business Day following the end of the reporting period. B. Monthly Reports – by the third Business Day following the end of the reporting period C. Quarterly or Annual reports – by the fifth Business Day following the end of the reporting period."	MAXIMUS will ensure all production reports will be available online for review by the Department in compliance with the following schedule: A. Daily or Weekly Reports – by the end of the Business Day following the end of the reporting period. B. Monthly Reports – by the third Business Day following the end of the reporting period C. Quarterly or Annual reports – by the fifth Business Day following the end of the reporting period."
SLA33	Contractor shall ensure 99% of all responses from redundant site storage are received within 10 seconds.	MAXIMUS will ensure 99% of all responses from redundant site storage are received within 10 seconds.
SLA34	Contractor must, in the event of an unscheduled Module Downtime, restore Availability, using procedures approved in the Business Continuity and Disaster Recovery Plan within four hours from the start of the unscheduled Downtime.	MAXIMUS will recover the Provider Services module within four hours from the start of the unscheduled down time. The BCDR plan will outline the procedures to be used, notification requirements, and recovery window for each type of recovery effort.

ID	Performance Requirement	MAXIMUS Summarized Response
SLA35	Contractor shall provide an alternate business site if Contractor's primary business site becomes unsafe or inoperable. The alternate business site must be fully operational within two Business Days of the primary business site becoming unsafe or inoperable.	MAXIMUS staff are primarily mobile-workers who have the ability to work from a variety of locations when necessary. For Option B business operations, our SOA model of delivery is complete with fail-over to one of our many alternate sites. For the Montana implementation, our Glendale, Colorado location is the primary business site with Hampton, VA as the backup location. MAXIMUS is using Amazon Web Services hosting solution. In this environment, a redundant site is kept online and available for recovery of the system. In all cases, business operations will resume within two business days.
SLA36	Contractor shall provide detailed Disaster Recovery Plan test results annually to the Department within 30 days of test completion	MAXIMUS will conduct annual DR testing and provide results to the Department within 30 days of test completion.
SLA38	Contractor shall provide file restoration within six hours of Department request.	MAXIMUS does not archive system files or documents, hence, all files are available without need for restoration.
SLA39	Contractor shall request any planned Downtime due to scheduled upgrades or Maintenance, outside the normal Maintenance Window, to the Department five Business Days prior to Downtime. The Department must approve the planned Downtime.	MAXIMUS will make requests for planned down time due to scheduled upgrades or maintenance, outside the normal maintenance window, to the Department no more than five business days prior to the down time. MAXIMUS acknowledges that the Department must approve the planned down time.
SLA40	Contractor shall notify the Department of any emergency Deficiencies, as defined by the Department causing severe financial or productivity impacts, including Module Downtime, within one hour of the initial Deficiency or within fifteen minutes of becoming aware of the issue, whichever is earlier. Contractor shall provide its plan for resolution within two hours of the notification of the Deficiency to the Department and resolve the Deficiency within 24 hours of the notification of the Deficiency to the Department.	MAXIMUS will notify the Department of any emergency deficiencies within one hour of the initial deficiency or within fifteen minutes of becoming aware of the issue; whichever is earlier. MAXIMUS will provide our plan for resolution within two hours of the notification and resolve the deficiency within 24 hours of the notification.
SLA41	Contractor shall notify the Department of any Major Deficiencies, as defined by the Department, causing serious disruption to Operations and Services where there is no alternative or work around, within one hour of becoming aware of the issue. Contractor shall provide its plan for resolution within four hours of the notification of the Deficiency to the Department and resolve the Deficiency within 36 hours of the notification of the Deficiency to the Department.	MAXIMUS will notify the Department of any major deficiencies within one hour of the initial deficiency or within fifteen minutes of becoming aware of the issue; whichever is earlier. MAXIMUS will provide our plan for resolution within four hours of the notification and resolve the deficiency within 36 hours of the notification.
SLA42	Contractor shall notify the Department of any Moderate Deficiency, as defined by the Department, it identifies that affects a small number of users, causes inconvenience, or delays business or prevents use of a fully supported Service within 24 hours of becoming aware of the issue.	MAXIMUS will notify the Department of any moderate deficiencies within 24 hours of becoming aware of the issue.
SLA44	Contractor shall work collaboratively with the Department to gather, analyze and report findings to the Office for Civil Rights (OCR) for any HIPAA or HITECH incident involving Contractor that affects a population of 500 members or more. Sufficient technical evaluation will be completed by the Contractor to verity the number of member potentially affected.	The MAXIMUS Privacy Official will work with the Department to gather, analyze, and report findings to the OCR for any HIPAA or HITECH incidents involving MAXIMUS that affect a population of 500 members or more. The MAXIMUS security team will provide the technical evaluation to identify the number of members potentially affected.

ID	Performance Requirement	MAXIMUS Summarized Response
SLA46	Contractor shall adhere to applicable State and Federal laws, rules, regulations, guidelines, policies, and procedures relating to information systems, information systems security and privacy, physical security, PHI confidentiality and privacy. Contractor must work with the Department to define and identify that the proposed Solutions or Services meet applicable compliance requirements. If Contractor is out of compliance, a mitigation plan to regain compliance is due to the Department within 10 business days with mitigation and testing to be completed in the timeframe defined in the mitigation plan.	MAXIMUS will adhere to applicable State and Federal laws, rules, regulations, guidelines, policies, and procedures relating to information systems, information systems security and privacy, physical security, PHI confidentiality and privacy. We will work with the Department to define and identify that the Provider Services solution meets applicable compliance requirements. We will develop a mitigation plan to address any compliance issues within 10 business days of discovery of the compliance issue.
SLA47	Contractor shall prevent any user or system administrator from having a shared account.	MAXIMUS privacy and security policy prohibits use of shared accounts for any system. MAXIMUS staff undergoes annual refresher training on privacy and security topics and Project Management personnel emphasize project standards with all project staff. No MAXIMUS user or system administrator will utilize a shared account.
SLA48	Contractor shall have an acceptable documented risk mitigation plan submitted to the Department within 5 business days of risk identification for 100% of high or critical risks. The Department will determine the level of criticality of each risk.	In the event a high or critical risk is identified by either MAXIMUS or the Department, MAXIMUS will submit an acceptable risk mitigation plan to the Department within 5 business days of risk identification for 100% of the identified risks. MAXIMUS acknowledges the Department will determine the level of criticality for each risk.
SLA50	Contractor shall conduct annual HIPAA and security training with Contractor staff. This training will also be part of the onboarding processes and the documentation will be consolidated and submitted annually to the Department.	MAXIMUS conducts mandatory annual HIPAA and security training for all staff members. Documentation of completion of the annual training will be submitted to the Department annually.
SLA51	Contractor will ensure that Module Federal Certification is achieved retroactive to the first day of Operations and continued throughout the Operations Phase. The Contractor is responsible for meeting the Federal standards, conditions and business requirements, formally published by CMS on the date the RFP closes, necessary to ensure initial and continued federal Certification for the operation of the Module and Department to receive full Federal Financial Participation (FFP) and the Federal Medical Assistance Percentage (FMAP) funding. In addition, the Contractor is responsible for meeting any new or modified Federal standards necessary to ensure initial and continued federal Certification, provided that to the extent those standards or requirements are not outside the scope of the RFP and do not result in a material cost impact on Contractor, otherwise the Contractor shall only be required to meet them if and to the extent the parties agree to do so through the Change Order process. Contractor will provide all support requested by the Department during Certification and any recertification conducted by CMS and by the Department. The support will include assisting the Department and CMS in developing artifacts and evidence to support the Certification review. This includes developing the Certification presentation and participation in the Certification review.	Having been through a modular certification effort, MAXIMUS understands the certification requirements as well as the effort involved in preparing for the CMS reviews. MAXIMUS is familiar with the MECL, as well as both the 2.1 and 2.2 versions of the MECT checklists. We appreciate the developing nature of the CMS requirements as the approach to modular certification continues to evolve. As CMS introduces new standards, we agree to meet any new or modified standards and if those standards fall outside the scope of the RFP, we will pursue a change order according to the Change Order process. Based on our familiarity with the requirements, we are confident our solution meets the Federal standards, conditions, and business requirements and will continue to do so to support initial and continued federal certification. As a result of achieving federal certification, the State will receive full FFP and FMAP funding. Based on our certification experience in other states, we understand the enormous undertaking of preparing for and participating in the CMS gate reviews for modular certification. As laid out in our certification plan, MAXIMUS intends to collect artifacts, supply evidence and develop the certification presentation, including a full system demonstration of the solution during the certification review.

ID	Performance Requirement	MAXIMUS Summarized Response
SLA52	Contractor shall work cooperatively with all other contractors and offer timely support in integrating Solutions within the State's healthcare programs enterprise. Timely shall be defined as scheduling of a meeting within five business days, review of applicable documentation within five business days and scheduling of testing within five Business Days and ensuring the appropriate Contractor staff is participating. Days begin based on a request by the Department or another contractor.	MAXIMUS will work cooperatively with all other contractors and offer timely support for the integration of solutions within the State's healthcare programs enterprise. MAXIMUS acknowledge the following: ▪ Meetings shall be scheduled within five business days ▪ Review of documentation occurs within five business days ▪ Scheduling of testing occurs within five business days ▪ Ensuring appropriate MAXIMUS staff are participating in these activities
SLA53	Contractor shall ensure that 99% of all Data converted is correctly mapped and usable by the scheduled completion date in the Work Plan.	MAXIMUS confirms that 99% of all converted data will be correctly mapped and usable by the scheduled completion date in the work plan.
SLA54	Contractor is required to maintain a Data dictionary, accessible electronically, that shall be updated within 10 Business Days of any change.	MAXIMUS will maintain an electronically accessible data dictionary which will be updated within 10 business days of any change to the database.
SLA57	Contractor shall ensure accurate processing in accordance with the applicable Specifications of all electronic data interchange (EDI) transactions.	MAXIMUS will ensure accurate processing in accordance with the applicable specifications for all EDI transactions.
SLA60	Contractor shall maintain up to date System Design Documentation and System Documentation. Documentation shall be updated within 10 business days of the Implementation of a change.	MAXIMUS will maintain up to date system design documentation and system documentation. We will update the documentation within 10 business days of the implementation of a change.
SLA61	Contractor shall maintain up to date functional Documentation including both User Documentation and the Operations Procedures Manual. Documentation shall be updated within 10 business days of the Implementation of a change.	MAXIMUS will maintain up to date functional documentation, including user documentation and the operational procedures manual. We will update the documentation within 10 business days of the implementation of a change.
SLA62	Contractor's Solution shall ensure access for the required number of concurrent users, according to the Specifications, necessary for the administration of the Department's business functions without limitation of user access and compliance with Performance Standards.	MAXIMUS ensures access for the required number of concurrent users according to the specifications.
SLA63	Contractor shall perform patching and corrections related to security vulnerabilities of a critical nature within three Business Days and those of a major nature within 10 Business Days. The Department will determine the level of criticality in consultation with the Contractor.	Upon identification of a security vulnerability, MAXIMUS will apply patching and corrections to resolve the vulnerability within three days for critical issues and within ten days for major issues. MAXIMUS acknowledges that the Department will determine the level of criticality in consultation with MAXIMUS.
SLA64	Subject to receiving the Department's approval as provided in contract Section 25.28, Contractor will provide a statement indicating approval by the Department for any publicity concerning the Contract, including, but not limited to, notices, information pamphlets, press releases, research, reports, signs, and similar public notices prepared by or for Contractor. The Department will provide Contractor with the applicable statement.	MAXIMUS will comply with the requirements in Section 25.28 for prior approval for any publicity concerning the Contract and will provide a statement indicating approval by the Department; which shall be provided by the Department.
SLA65	Damages may be assessed if Contractor fails to meet other contract and RFP requirements. The performance criteria will have a performance measure and scoring mechanism established in this Contract through negotiation with Contractor.	MAXIMUS acknowledges that damages may be assessed if MAXIMUS fails to meet other contract and RFP requirements. Performance criteria, measurement, and scoring will be established in the Contract through negotiation with MAXIMUS.
SLA66	Contractor shall provide accurate responses to all Department Change Requests for Enhancements including proposed Solution and pool hours/cost within 10 days for low complexity projects, 20 days for medium complexity projects or 30 days for high complexity projects, from submission of a Department Change Request for an Enhancement. The Department will determine the level of complexity.	MAXIMUS will respond to the Department's Change Requests for Enhancements within 10 days for low complexity projects, 20 days for medium complexity projects and 30 days for high complexity projects. MAXIMUS acknowledges that the Department will determine the level of complexity. However, MAXIMUS recommends that the Department consult MAXIMUS for input in determining the level of complexity.

ID	Performance Requirement	MAXIMUS Summarized Response
SLA67	Contractor must receive Implementation Acceptance from the Department for each scheduled Implementation no later than the Acceptance Date in the Work Plan.	MAXIMUS acknowledges that we must receive Implementation Acceptance from the Department for each scheduled Implementation no later than the acceptance date in the work plan. Per answers provided in the Q&A board, if the Department does not provide acceptance, the Department will provide information to the vendor detailing why acceptance has not been provided. Additionally, the Department may choose to waive the liquidated damages if it is in the best interest of the State.
SLA68	Contractor shall notify the Department within one hour following the identification of any potential or actual Security Incident, including any physical or system breach, any attack, or the introduction of any disabling device, related to the System. Contractor shall take corrective action to mitigate the potential or actual major or minor Security Incident within two hours following the identification of each potential or actual Security Incident.	MAXIMUS will notify the Department within one hour of identification of any potential or actual security incident. MAXIMUS will take corrective action to mitigate the potential or actual incident within two hours following the identification of the incident. The MAXIMUS Security Team will assist with the identification, corrective action plan and implementation of the security fixes.
SLA69	Contractor shall provide a written report and assessment to the Department within 12 hours following the identification of any Security Incident detailing all actions taken concerning the incident, including the type of incident, the current status, and any potential impact(s).	The MAXIMUS Security Team will provide a written report and assessment to the Department within 12 hours following the identification of any security incidents. The report will detail actions taken, type of incident, status, and potential impact(s).
SLA98	The Contractor's Solution shall ensure that the maximum amount of time between the initiation of a transaction and the confirmation receipt of the transaction by the Enterprise Service Bus (ESB) will not exceed two seconds.	MAXIMUS confirms that the maximum amount of time between the initiation of a transaction and the confirmation receipt of the transaction by the ESB will not exceed two seconds.
SLA101	Contractor's performance monitoring dashboard must have Availability 99% of the time, 24 hours a day, seven days a week, excluding Department approved planned Downtime. Availability is calculated as follows: Availability percentage = unplanned Downtime (Total Downtime-approved Downtime) divided by Total time (24X7).	The MAXIMUS performance monitoring dashboard will be available 99% of the time, 24 hours a day, seven days a week, excluding Department approved down time. The dashboard is integrated with our real-time performance monitoring reporting tool.
SLA102	Contractor's Solution must have Availability 99.5% of the time, 24 hours a day, seven days a week, excluding Department approved planned Downtime. Availability is calculated as follows: Availability percentage = unplanned Downtime (Total Downtime-approved Downtime) divided by Total time (24X7).	The MAXIMUS Provider Services solution will be available 99.5% of the time, 24 hours a day, seven days a week, excluding Department approved planned Downtime. System monitoring tools will alert support staff when the system experiences any full or partial outage. Support staff will initiate the appropriate recovery processes.

3.10.9 Subcontractors

> 3.10.9 Subcontractors
>
> The highest scoring Offeror will be the Prime Contractor if a contract is awarded and shall be responsible, in total, including for all work of any subcontractors. Nothing contained within this document or any contract documents created as a result of any contract awards derived from this RFP shall create any contractual relationships between any subcontractor and the State. The Offeror must describe their approach to meet the Subcontractor requirements defined in Attachment F, Requirements Matrix.

The MAXIMUS subcontractor management approach ensures effective control of all subcontracted activities. These management processes and procedures are based on industry best practices and include a comprehensive governance framework, allowing us to select and manage companies that offer the State quality and seamless performance, regardless of the company performing the work.

We understand and will comply with all subcontracting requirements provided in the RFP, including using a subcontractor for no more than 40 percent of the scope of work included in the contract. In

addition, we understand that any contracts awarded to MAXIMUS as a result of this proposal does not create a contractual relationship between the State and Microassist. 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.

We intend on subcontracting with Microassist who will provide training materials and develop the training plan. Microassist has completed a number of similar training engagements for MAXIMUS and brings knowledgeable resources and repeatable processes. We discuss Microassist in further detail in Section 3-10-02-7: Training. Microassist is the only subcontractor MAXIMUS will use for the MPATH project.

In keeping with MAXIMUS corporate contracting procedures, our standard subcontract contains a detailed statement of assigned tasks and responsibilities, a disclosure of business relationships, certification to comply with all applicable laws and regulations, and a statement that the subcontractor is subject to the requirements of the prime contract including any adjustment in work activities or negotiated contract terms. Our subcontract requires subcontractors to comply with all applicable privacy and security requirements, performance requirements in the RFP related to the functional areas within their scope of work and adhere to an established system of accounting and financial controls.

Microassist was selected for specialty skills, performance records, and proven ability to work in an integrated partnership environment. Our process to ensure that their training efforts are coordinated and integrated across our team is shown in *Exhibit 3.10.9-1: MAXIMUS Subcontract Management Workflow*.

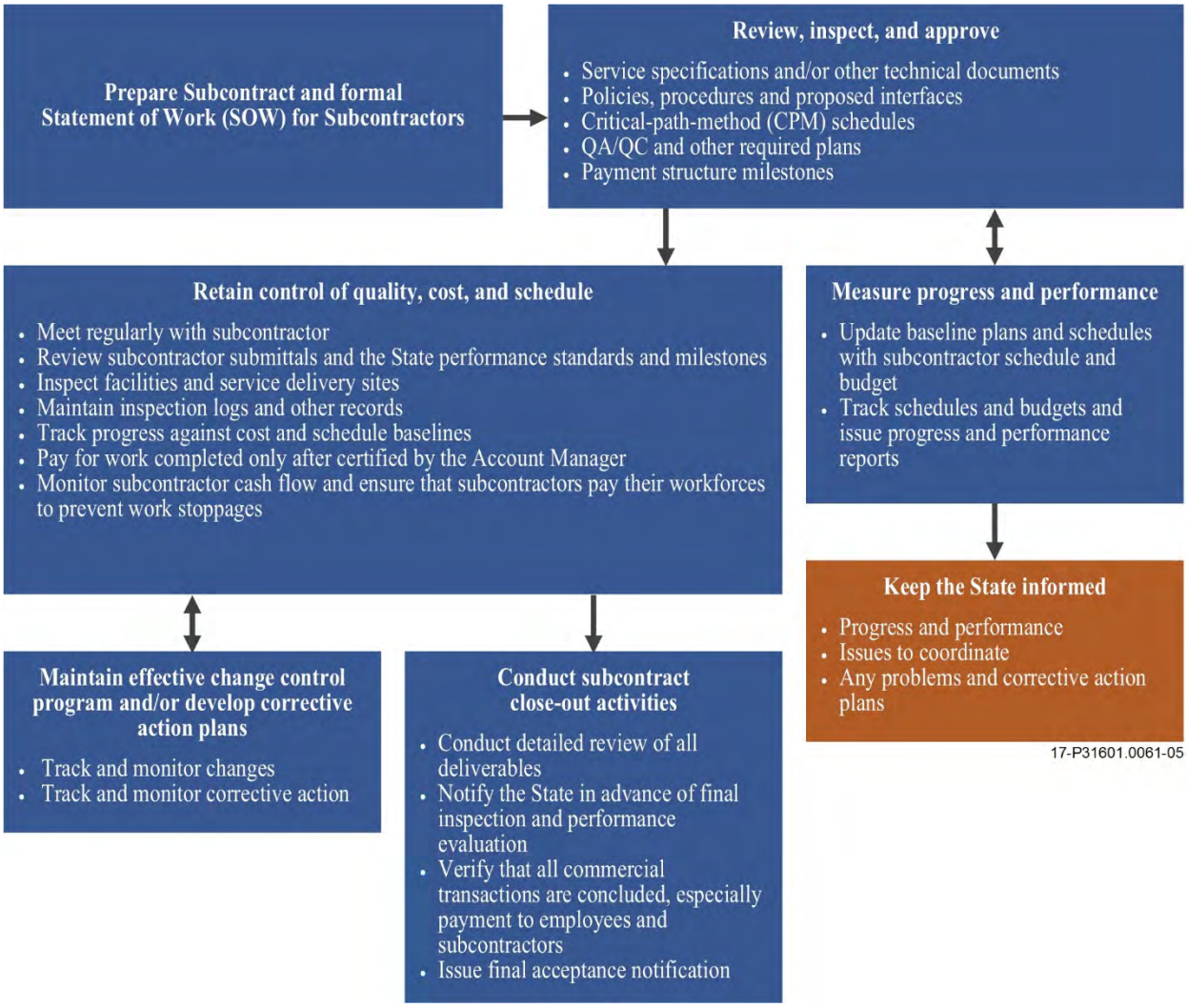


Exhibit 3.10.9-1: MAXIMUS Subcontract Management Workflow. *Our subcontract management process is used successfully on existing MAXIMUS projects.*

Subcontractor Requirements

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

ID	Subcontractor Requirement	MAXIMUS Summarized Response
SUB01	The Contractor may use subcontractors for no more than forty percent (40%) of the scope of work included in the contract. The subcontractor 40% will be determined using the highest proportional value among the following factors: subcontract dollar value relative to the overall contract value, subcontractor FTE's relative to the total contract FTE's, subcontractor hours relative to the total contract hours. If the proposed solution to meet the core functional requirements (e.g., core product) is a commercially licensed COTS or SaaS product (e.g., the State will receive a commercially available license for the product), the specific product that satisfies this condition can be excluded from the 40% subcontractor calculation. In Attachment L - Technology Matrix, the vendor must include "Commercially Licensed" in the column titled "Other" for the specific line item. This exclusion does not apply to infrastructure software or software that supports the core product.	Microassist is the single subcontractor MAXIMUS will use to perform the scope of work. Microassist's role is limited to providing the training materials as specified in Attachment F. This work amounts to less than 40 percent of the scope of work included in the contract.
SUB02	If the Contractor transfers resources required to fulfill the contract to a third party, the third party is considered a sub-contractor and the transfer will be subject to the 40% subcontractor limitation.	MAXIMUS does not intend to use third parties to fulfill contractual obligations. However, we understand that if we transfer resources to fulfill the contract to a third party, the third part is considered a sub-contractor and the transfer is subject to the 40 percent subcontractor limitation.
SUB03	The Contractor shall list all subcontractors, if any, in the proposal.	The sole subcontractor MAXIMUS intends to use in the MPATH scope of work is Microassist.
SUB04	The Contractor shall provide a detailed description of all work to be subcontracted to third parties.	Microassist will provide the training plan, documentation, user and training manuals, and web-based training modules for Option A. For a more detailed description on Microassist's scope of work, see Section 3.10.2.7 Training.
SUB05	The Contractor must submit to the Department annually, a Subcontractor Usage Report on the use of subcontractors and certify that all subcontractors are in compliance with the employment practices mandated by federal and State statutes and regulations. The Subcontractor Usage Report must at a minimum contain the total subcontract dollar value, total subcontractor FTE's, total subcontractor hours.	We submit to the Department a Subcontract Usage Report on the use of our subcontractors and certify that all subcontractors are in compliance with the employment practices mandated by federal and State statutes and regulations.
SUB06	The subcontractor will be required to enter into a signed Business Associate Agreement (BAA) as a part of the contract, that is in compliance with the Privacy and Security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) prior to start of work. The BAA is included in the contract template found in the Procurement Library	Part of the subcontract with Microassist includes a signed Business Associate Agreement, using the contract template contained in the Procurement Library
SUB07	The Contractor shall allow Department personnel direct access to all subcontractor or third-party personnel serving in critical roles on the project and shall not act as an intermediary between the Department and such parties for questions about the proposed solution or operation of the proposed solution. The Department reserves the right to discuss design, configuration, implementation, operation, routine maintenance, and enhancement of the proposed solution(s) directly with any subcontractors or third parties involved in performing work for the Department.	Open and accessible communications with each entity with a scope of work in the MPATH project is essential to project success. MAXIMUS supports the Department's direct access to all subcontractor or third-party personnel serving in critical roles on the project and we do not act as an intermediary between the Department and Microassist for questions about the proposed solution, including details around all aspects of the training.
SUB08	The Department shall have the right to review and approve any subcontracts through the Contractor.	We agree with the Department's right to review and approve any subcontracts MAXIMUS executes.

3.10.10 Enrollment

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, revalidations, and updates 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

> 3.10.10 Enrollment
>
> This section addresses provider enrollment requirements. The Provider Services module will support a web-based tool for providers to electronically enroll with Montana Healthcare Programs which includes an automated tool for screening activities that must be completed in accordance with State and federal statutes, policy, mandates as well as industry standards required for the Contractor's Scope of work. The Offeror must describe their approach to meet each of the Provider Enrollment requirements defined in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution is designed to maximize Provider use of the web portal. The solution's web portal functionality includes validation of field input, user validation, an electronic signature, and a record of the application receipt date. The flexible workflow engine within our solution 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, if required. By configuring our business processes to match the Department's requirements, we are confident in our solution's ability to assist the Department in processing all Provider applications accurately, and in an expedited timeframe.

Exhibit 3.10.10-1: Functional Features of MAXIMUS Provider Services solution shows the key functional components of our solution and the benefits they offer to DPHHS and Providers engaged in the screening and enrollment process.

Screening/ Enrollment Component	MAXIMUS Provider Services solution Functionality	Benefits to the State, Providers & Trading Partners
Application Submission	▪ Web-based design supports data entry of the full application (based on Provider type) including data related to ownership and convictions ▪ Providers can register online and enter data through the portal using wizard-style forms for complete and correct data entry ▪ Paper applications can be entered directly into the system and follow the same workflow process ▪ Application is pre-populated with conversion data for existing providers	▪ Ease of data entry and faster approval time encourages Providers to apply via the web portal ▪ Providers can start, save, continue, and complete applications at times that are convenient for them
Application Fee	▪ Seamless integration with Bill2Pay allows for an integrated payment function as part of the online application process ▪ Providers can pay required application fees via e-Check, paper check, or credit card ▪ Workflow allows Providers to request a waiver of the application fee on a hardship basis or based on previous payment to Medicare or another state	▪ Application fees from institutional Providers collected as required by statute. ▪ Screening process initiated once receipt of payment verified ▪ Department has a work queue for viewing waiver requests

Screening/ Enrollment Component	MAXIMUS Provider Services solution Functionality	Benefits to the State, Providers & Trading Partners
License Verification	▪ Automated source validation using clearinghouse or single database search ▪ Integrated automated and manual verification functions if required ▪ Dashboard tracking for all license verification statuses	▪ The system enforces verification in all jurisdictions where the Provider claims to be licensed ▪ The Department has a work queue for viewing Providers that fail license verification process
Risk Profiling	▪ Automated calculation of risk based on CMS and DPHHS policy ▪ Integrated workflows create tasks for Department and operations staff to perform next steps, including rechecking databases on a periodic schedule and scheduling on-site visits	▪ The Department has a dashboard to track status of database checks, background checks, and site visits completed on moderate- and high-risk Providers
Database Checks	▪ Automated checking of all required databases during initial enrollment, revalidation, and monthly based on Provider risk levels	▪ The Department is automatically notified of adverse findings on Providers that fail required database checks
Site Visits and Fingerprint-based Background Checks	▪ Integrated workflows move enrollments into site visit categories and finger print-based background check categories based on risk level ▪ Functionality to support the full array of data required to be documented as well as the checklist to be used	▪ The Department has a dashboard to track site visit status, completion of checklist, photo documentation, and other site visit activities ▪ All allowable documentation received on Fingerprint-based background checks is stored in the system
Provider Communication	▪ Automated communication channels allow users to be proactive with Providers ▪ "Return to Provider" functionality allows Enrollment Specialists to inform Providers of issues in their application or screening process without the need for paper	▪ Providers using the web portal are prompted to update their information ▪ Communication with Providers is based on their preferred contact method
Online Provider Directory	▪ Robust search functionality that includes a public facing search function and an internal search function only accessible by Department authorized users. ▪ Search functions offer a variety of search parameters all of which are configurable to meet any unique requirements of the Department.	▪ Intuitive search capability gives all Montana stakeholders ability to find Providers and know their status ▪ Provides a consolidated view of Providers, their programs and networks

Exhibit 3.10.10-1: Functional Features of MAXIMUS Provider Services solution. *Our combination of people, process, and technology offers the Department and Providers a screening and enrollment solution that is optimized for efficiency.*

3.10.10.1 Enrollment Submission

The MAXIMUS Provider Service solution provides full system functionality to allow Providers to enter new enrollments, re-enrollments, revalidations and updates electronically via the web portal. The configurable workflow engine and user interface in our solution allows us to implement the enrollment processes to meet the requirements and policy set forth by DPHHS. Providers will also have the option to submit paper versions of these documents via regular mail. In our current configuration, the solution supports the scanning and indexing of paper enrollment forms and data updates submitted on paper and stores them in the Hyland OnBase document repository. The imaging component is directly integrated into the online solution and is used to capture uploaded documents necessary for Providers to complete their enrollment. If Montana chooses not to procure our Option B services, MAXIMUS can offer this functionality to the Fiscal Agent vendor or we can link received and stored images scanned by the State's Fiscal Agent to the Provider's profile in the system. Our solution provides a paper application workflow that allows the Data Entry staff to enter the paper enrollment applications directly into the system through the web portal. The web portal allows authorized users access to the system dashboard, which provides a history of every application that has been received electronically and by mail, along with the status of each application.

To submit electronic applications online in our solution, Providers must first establish an account on the web portal. Our solution uses a combination of the Provider's Tax ID (EIN or SSN) and NPI as the primary identifiers to set up the account. Existing Providers that are converted from the MMIS will be required to supply additional information to establish their initial account. The additional information will depend on the type of Provider, but may include their Taxonomy code, Medicaid ID, and zip code/zip extension for a specific practice location where the Provider is currently enrolled.

Once the Provider's initial profile information is captured, the system requests the user's contact and account security information. As part of the request for contact information, the system captures the email address of the Provider or the Provider's credentialing agent. We use this email address to communicate the status of the application with the Provider and to request additional information and/or corrections based upon the submission. The system can be configured to capture any number of security questions, based on the requirements of the Department.

Once the user has logged into the web portal, the user is taken to the Provider home page. The home page displays all the existing Providers that the user is authorized to manage and allows the user to create a new Provider record. *Exhibit 3.10.10.1-1: Provider Home Page* shows the initial screen the user sees when logging into the system.

CONFIDENTIAL

The system displays alerts and messages to the Provider on the homepage, notifying them of important actions that may need to be taken (e.g., a license is due to expire within 30 days). Users can select from the available list of Providers displayed on the screen, or add a new Provider if required. Once logged in and viewing the homepage, Providers are able to view the status of any in progress enrollments, revalidations, or updates.

Once the user selects an action to take on a Provider, the system contains edits and validations throughout the application workflow to help confirm that Provider-submitted data meets CMS and Department requirements prior to initiating the internal screening process. The system contains a wizard-based data entry flow that guides Providers through the enrollment/re-enrollment process. The system prevents Providers from submitting applications that have missing, incomplete, or conflicting information. These front-end edits in the web portal are configured to meet any of the unique rules and policies required by the Department. Information on existing Providers is converted and loaded into the system during data conversion, prior to implementation of the new screening and enrollment process. Providers are only required to validate the converted information from the MMIS for accuracy via the web portal rather than beginning their application anew. *Exhibit 3.10.10.1-2: Wizard-Based Enrollment Flow* shows how the system guides providers through the enrollment process and provides a visual status of where they are at within the flow.

CONFIDENTIAL

CONFIDENTIAL

As shown in *Exhibit 3.10.10.1-2*, the enrollment screen shows a 'Progress Tracker' section that tells the user which screens they have completed and which screens remain to be completed for the enrollment. The user is able to navigate through the enrollment by simply pressing the 'Next' button or they can directly navigate to the desired screen by scrolling within the Progress Tracker. Screens where data has been entered and the screen edits have passed show as green check marks. If the user exits the enrollment process and returns at a future time, they will be able to continue the enrollment from where the point where they last saved.

During enrollment, the system allows Providers to select and to opt out of any State-defined programs. Our solution will also allow the Provider to return to the portal and provide them the option to enroll in additional programs later. The system tracks the eligibility spans for all programs that the Provider may be enrolled and allows users to search on these programs, as needed. We send these program enrollment spans to the MMIS as a part of the MMIS interface, as required.

An important edit that is triggered during the new enrollment process detects when a Provider may be attempting to create a duplicate Provider in the system. In our experience, the definition of a duplicate Provider varies from state to state, but the system is configurable to fit whatever definition is required for Montana. When submitting a new enrollment, the Provider user is required to submit initial identifying information to initiate the enrollment process. This initial information consists of Provider Type, Tax ID (EIN or SSN), Name, NPI, primary Taxonomy code, and Zip code/zip extension of the primary practice location. Once the Provider enters this information, the system validates that the Provider does not already exist in the system, per Department defined rules. If the system detects a duplicate Provider exists, an error message is returned to the Provider and the system does not allow the Provider to proceed with the new enrollment. The online help and enrollment guide is available to Providers to assist them in determining the next steps to take with their enrollment.

CONFIDENTIAL

3.10.10.2 Atypical Provider Enrollment

Different States use different rules for enrolling Atypical Providers. In our most recent implementation for the District of Columbia, the District required an NPI 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 or not required. We make this simple rule change to the system once we confirm the requirements for each State. For the Montana implementation, the default configuration will not require NPI for the Atypical Providers, but this can be changed per Department policy.

3.10.10.3 Provider Notification – Receipt of Enrollment Application

Providers are able to use an electronic signature to submit their enrollment application on the Agreements screen. The Agreements screen is configured to meet the Department requirements for the viewing and signing of Provider agreements. Once the Provider activates the electronic signature, the Provider can then submit their new enrollment or re-enrollment for review and screening. The system generates a printable PDF that captures all the information entered by the Provider during the enrollment process. The system also sends an email notification to the Provider, notifying them that their application has been received and is ready for processing. *Exhibit 3.10.10.3-1: Application Receipt Notification* gives an example of the Provider notification that is sent in our implementation for the District of Columbia.

Our solution can also be configured to send different types of application receipt notifications based on Provider type and based on the Provider's risk level. For example, the additional screening requirements required for moderate and high-risk Providers can be included in the email notification, making these Providers aware of additional steps that may be required to complete their enrollment.

From: DCMedicaidPDMS@maximus.com [mailto:DCMedicaidPDMS@maximus.com]
Sent: Monday, April 10, 2017 1:46 PM
To: [redacted]
Subject: DC Medicaid Provider Application Received

District of Columbia Provider Screening& Enrollment Customer Service Center
PO BOX 34086
Washington DC, 20043 – 4086
844-218-9700 Phone
844-436-8333 Fax

[redacted]
2000 15TH ST
Suite 600
ARLINGTON, VA 22201-2220

Legal Name: [redacted]
NPI: 1053367151
Taxonomy: 207L00000X
Effective Date: 10/01/2015

04-10-2017
Dear Provider:

This notice acknowledges receipt of your application to join the District of Columbia Medicaid Program. The District's agency that oversees the Medicaid and Alliance programs, Department of Health Care Finance (DHCF), is pleased that you have chosen to join with those providers who serve the healthcare needs of our residents enrolled in the District of Columbia Medicaid Program.

MAXIMUS staff will review your application for completeness and will verify the information you provided. As a limited risk provider type, credentialing could take up to 30 days to complete. If additional information is requested, the process could take longer.

Thank you for your participation and your efforts to maintain and improve the health of District of Columbia residents.

If you have questions, please contact the MAXIMUS Provider Screening and Enrollment Customer Service at [redacted] or email at [redacted]

Regards,

MAXIMUS Provider Screening and Enrollment Customer Service

Exhibit 3.10.10.3-1: Application Receipt Notification. *The system automatically notifies Providers in real-time that that their application has been received.*

3.10.10.4 Enrollment Review

Once a Provider submits an application through the web portal, the system creates a task in the Provider Enrollment Specialist work queue. The Provider Enrollment Specialist retrieves the Provider's application from the work queue and initiates the review and screening process. The Provider Enrollment Specialist reviews the electronic application to identify whether any required forms are missing, incomplete, or contain conflicting information. The system requires all applications to be reviewed by the Provider Enrollment Specialists for missing, incomplete, or conflicting information.

The MAXIMUS Provider Services solution workflow engine guides the Provider Enrollment Specialist through the application review, screening, and approval process. If additional information is required, the Provider Enrollment Specialist is able to return the application to the Provider by using the "Return to

CONFIDENTIAL

Provider" function, which generates an email that lists the additional information required. Generation of these emails is immediate once the Provider Enrollment Specialist has taken the action to return the application to the Provider. This functionality eliminates the paper correspondence trail typically associated with the enrollment review and allows for timely and accurate processing of all required Provider applications and revalidations. Examples of the actions the Provider Enrollment Specialist can take when reviewing a Provider application are shown in *Exhibit 3.10.10.4-1: Return to Provider*.

Exhibit 3.10.10.4-1 shows a list of reasons the Provider Enrollment Specialist may determine that a Provider's application requires additional or corrected information to be processed. In the current configuration, the system requires the Enrollment Specialist to review the entire application and to identify all potential deficiencies before taking the action to return to Provider. This process decreases any potential back and forth with the Provider and makes sure the Provider is aware of all corrections that need to be made before submitting their updated enrollment. Once the "Return to Provider" action is taken, a system-generated email is sent alerting the Provider to make the necessary updates to the application on the web portal. The status of the application is changed to "Return to Provider" and the workflow engine tracks the time lapsed from the initial application submission. The robust front-end screen edits on the web portal also significantly reduce the likelihood that an application needs to be corrected as these will be caught by the system during initial Provider data entry. The list of

The "Return to Provider" function is extremely efficient because it eliminates the paper trail of requests and the back-and-forth between the Provider and the State's Provider enrollment support team.

CONFIDENTIAL

"Return Reasons" is a configurable item within the system and can be tailored to meet any unique needs of the Department.

Our solution tracks the timeliness of processing of the completed Provider application after receipt of required information to resolve any deficiency from the previously supplied information. The system dashboard displays aging statistics on Providers that have submitted applications, including those Providers that have resubmitted applications for missing information. The system records each event that occurs during a workflow and records the date-time stamp of that event. For example, if the application is returned to the Provider for a deficiency, the system will know how long it has taken for the Provider to return the required information. All workflow actions and events are tracked, and the duration between events can be viewed within the system, via on demand reports, and through real time system dashboards.

3.10.10.5 Provider Screening

The MAXIMUS Provider Service solution contains built-in mechanisms to support the full range of Provider enrollment and screening requirements mandated by the ACA. State visibility into the status of Provider activity is available through the dashboard, Provider search, and robust reporting capabilities in the Provider Services system. Our solution provides a data extraction module that is used in connecting to a number of data sources for purposes of downloading data. When possible we download an entire verification source into the system so that we have flexibility in how we process initial and on-going screening. Our Provider Services Screening module is configured to validate Provider information using both automated and manual methods.

During Design, we will identify each screening source required by the Department and determine who owns the data, how we will access the data, and what keys are available in the data for matching purposes. In our experience, we have found there to be only minimal configuration required for implementing the screening functionality, generally being limited to including a new data source that may be unique to a particular State. 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 3.10.10.5-1: Screening Verification Sources* shows the list of data sources that are used currently in our 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	Automated
SAVE	Systematic Alien Verification for Entitlements Program	Manual
License Verification	Search the State's License Database	Manual

Database	Description	Method
Sexual Offender Registry	Search Sexual Offender Registry	Manual
DEA	DEA Verification	Manual
Controlled Substance Verification	Controlled Substance Verification	Manual

Exhibit 3.10.10.5-1: Screening Verification Sources. *We identify the full list of screening sources during design based on Department requirements and configure each verification source based on how the data is accessed.*

Provider screening and enrollment are key components of the enrollment requirements included in the ACA. Categorizing Providers by risk profile, re-enrolling Providers using the screening requirements, and verifying licenses and other key Provider data place operational and system challenges on Medicaid agencies as they move continue to implement the ACA provisions. These requirements call for operational staff to interact with the Provider Services system to execute and track compliance, as well as additional system functions for data sharing, workflow management, and reporting. Our Provider Services solution meets these requirements and we will configure the screening processes to align with any of the unique requirements for the Department.

New Enrollment and Revalidation Screening

For newly enrolling providers and revalidating providers, once the submitted application is approved by the Enrollment Specialist, the system initiates the screening checks against the required screening sources for the State. In our current configuration, if a Provider, owner, managing employee, or entity fails a required database check during the initial screening process, the Provider Enrollment Specialist uses the system to forward the provider to the State Program Integrity work queue for further review and disposition by the State. Likewise, if a Provider fails the initial license verification, the Provider Enrollment Specialist will forward the provider to the State Program Integrity work queue. *Exhibit 3.10.10.5-2: Initial Screening Results* shows the screen the Enrollment Specialist uses to review the initial screening on a newly enrolling or revalidating provider.

CONFIDENTIAL

As shown in *Exhibit 3.10.10.5-2*, the Enrollment Specialist is able to view the status of each required screening category and take actions based on the results for each category. The system automatically checks for potential matches for the automated screening categories. The system alerts the user to potential matches on a screening category. The Enrollment Specialist is then able to drill-down on the screening category and find further information on the results of the match. The screening categories displayed on the screen are configurable based on the provider's type, category (Individual versus Organization) and risk level.

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.

Monthly Database Checks

Our solution is configured currently to perform monthly database checks with OIG LEIE, EPLS/SAM, and SSDMF. Additional automated screening checks can be added to this list based on the Department's request. The system performs the monthly database checks for all enrolled Providers, group members, and any individuals or entities identified as owners or managing employees by the Provider during the enrollment process. The timing of periodic database checks is also a configurable parameter in the system.

CONFIDENTIAL

CONFIDENTIAL

The system exposes all required Providers, owners, and managing employees to the monthly database checks and records the matching results. Tasks are created in the work queue for our Provider Enrollment Specialists to review and take action on any matches that may require exclusion of the Provider from the State's Medicaid program. If a Provider fails a monthly database check, findings and supporting attachments (viewable through the system) are forwarded to State Program Integrity for further review and disposition. In our current configuration, the State Program Integrity worker can review the information and, if appropriate, issue a termination letter and handle any subsequent appeal made by the Provider.

The monthly database checks reveal the potential matches with the various exclusion databases required for screening and enrollment. *Exhibit 3.10.10.5-3: Provider Screening Results Page* is a screen shot from our system showing matches and available data from a SAM/EPLS match and an OIG match on the List of Excluded Individuals and Entities (LEIE) database. *Exhibit 3.10.10.5-3* provides an example of the screening results an Enrollment Specialist can view to determine potential matches and recommend approval, denial, or termination of the Provider from the program.

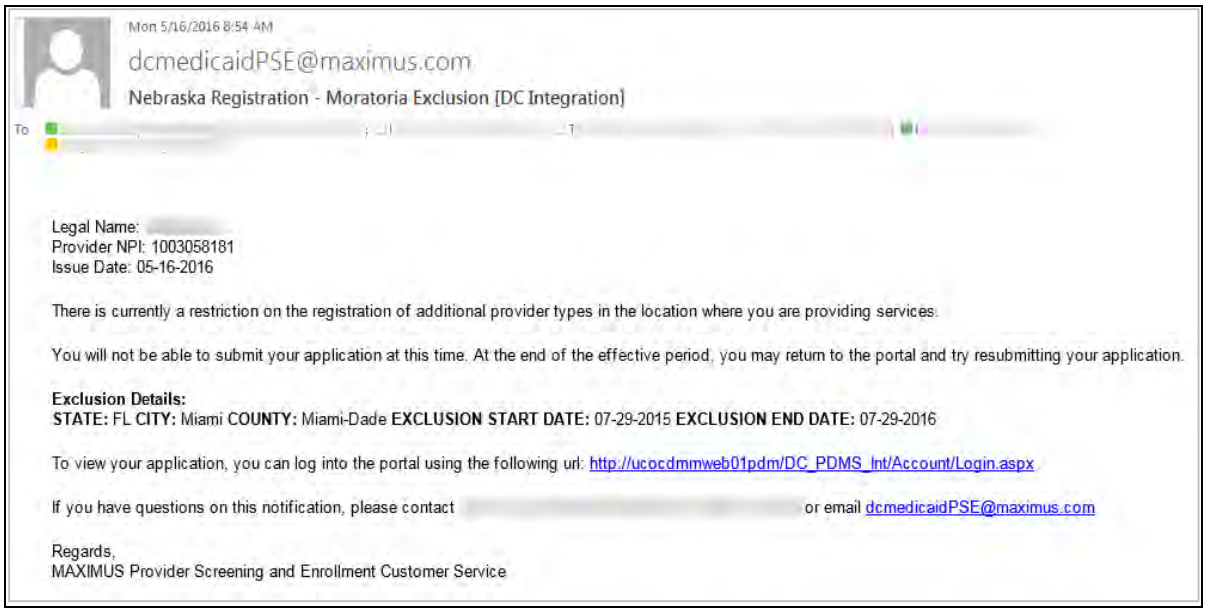
The screening results for all Providers are available for review by all authorized users of the system. State Program Integrity staff and other Department staff are able to view screening results for all Providers. Because many of the data sources do not have key data such as SSN, we configure the system to require a manual review in the cases where key data searches are not available. We will work with the Department to determine how best to configure the system in Montana.

CONFIDENTIAL

Moratoria

Through the data conversion process and subsequent new enrollments and revalidations, our system will contain a complete list of all active Providers within the State's Medicaid program. The system has a configurable moratoria component that identifies, by Provider type, any types of moratoria that may be active based on each individual Provider type. This component allows us to receive requests from the State, update the system moratoria parameters, and begin imposing moratoria for certain types of Providers based on the time parameters imposed by the U.S. Department of Health and Human Services and/or the State. Moratoria are imposed for an initial six-month period and may be extended in additional six-month increments.

Once the moratoria parameters have been entered into the system, our system begins to enforce them through Provider enrollments initiated via the web portal as well as paper applications processed by operations staff. For any Provider that fails the screening process due to a temporary moratorium, our solution places the application in the 'Enforce Moratoria' workflow step and sends an email notification to the provider that their application is suspended due to the current Moratoria restriction in place for their Provider type and location. *Exhibit 3.10.10.5-4: Moratoria Notification* provides an example of the email notification we send to the Provider in the case where their submitted enrollment is impacted by Moratoria.



Mon 5/16/2016 8:54 AM

dcmedicaidPSE@maximus.com

Nebraska Registration - Moratoria Exclusion [DC Integration]

To

Legal Name:
Provider NPI: 1003058181
Issue Date: 05-16-2016

There is currently a restriction on the registration of additional provider types in the location where you are providing services.

You will not be able to submit your application at this time. At the end of the effective period, you may return to the portal and try resubmitting your application.

Exclusion Details:
STATE: FL **CITY:** Miami **COUNTY:** Miami-Dade **EXCLUSION START DATE:** 07-29-2015 **EXCLUSION END DATE:** 07-29-2016

To view your application, you can log into the portal using the following url: http://ucocdmmweb01pdm/DC_PDMS_Int/Account/Login.aspx

If you have questions on this notification, please contact or email dcmedicaidPSE@maximus.com

Regards,
MAXIMUS Provider Screening and Enrollment Customer Service

Exhibit 3.10.10.5-4: Moratoria Notification. *Our solution is fully ACA compliant with all screening requirements, including Moratoria enforcement.*

The system is configurable to adjust the workflow steps once the Provider has been identified as being impacted by Moratoria. In our Nebraska implementation, we send the notice to the Provider as shown in *Exhibit 3.10.10.5-4* above. In our District of Columbia implementation, the client preference was to refer the Provider to District Provider Services staff (the system takes this action automatically). District Provider Services staff can then take the action to keep the Provider in the Moratoria workflow step, or override the Moratoria and allow the provider to proceed into further review and screening

CONFIDENTIAL

In addition to moratoria, our solution can be configured to set a limit or cap to the number of Providers that can be actively enrolled in the Medicaid program at any given point in time based on significant potential for fraud, waste, or abuse or other factors. Once the cap or limit has been set by the State and communicated to our support team, the system tables will be updated and the system will begin to systematically enforce the limits.

3.10.10.6 Streamlined & Expedited Applications

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 3.10.10.6-1: 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 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.

3.10.10.7 Application Fee Processing

MAXIMUS configures the application workflow to require certain institutional Providers to submit an application fee prior to initiating the review and screening process. Configuration will be based on CMS and DPHHS regulations for the collection of application fees, which are required for prospective, re-enrolling, and reactivating institutional Providers. Institutional Providers are required to pay an application fee unless they are

CONFIDENTIAL

already enrolled in Medicare or they have already paid the application fee to Medicare or another state program.

The amount of the application fee will be a system parameter that we update in the system on an annual basis per the CMS published rate. Providers will have the ability to submit an electronic payment online via a link in the web portal, or by paper check through the mail.

Collect Application Fee When Applicable

The system is configured to request the application fee from Providers when applicable and track receipt of the fee before initiating any screening and enrollment activities. *Exhibit 3.10.10.7-1: Application Fee* illustrates the application fee screen that is activated in the workflow when a Provider requires collection of the application fee.

Our solution validates that Providers requesting a waiver of the fee will have previously attested to the fact that they have already paid the fee via Medicare or through another state Medicaid agency. The system is configured to only request payment from those Provider types that are required to submit the application fee. If Providers opt to pay the fee online, the system will navigate the Provider to the Bill2Pay payment submission screen. This automated link to Bill2Pay streamlines the application fee collection process. Bill2Pay's specialty is customized electronic payment processing and remittance processing solutions for governmental, commercial, and financial billers. Required identifying information (for example, the unique application ID) will be sent to Bill2Pay for tracking purposes.

Providers can pay application fees through the web portal's link to the Bill2Pay using an e-Check or credit card, or they can submit their payment via a paper check. The application fee screen will be changed to inform the Provider as to the lockbox location for the Montana implementation. Regardless of the payment options selected by the Provider, the system tracks and verifies that the payment has been received prior to initiating internal review and screening processes for the Provider.

CONFIDENTIAL

The system does not retain or maintain any confidential financial information for the Provider when making a payment. Any sensitive financial information will be collected and retained by Bill2Pay. Once a Provider's application fee has been successfully processed by Bill2Pay, they will notify the Provider Services module of the successful payment transaction.

Process Application Fee Waiver Requests from Providers

A Provider may request a waiver of the application fee on a hardship basis by submitting a waiver request through the Department to CMS in writing. If CMS approves the hardship exception, a copy of that notification must be attached to the Provider's enrollment application that is submitted. In the current configuration, once the hardship approval is received from CMS, the approved hardship exception is attached to the Provider’s file by the Department reviewer.

The system allows Providers to request a waiver of the application fee. In this situation, Providers will not be prompted to enter their payment information through the web portal. The application will be submitted and the workflow will be configured to place the application in the status of "Waiver Requested."

If submitting the waiver request through the web portal, Providers will be required to use the document upload function to upload a signed form requesting the waiver. Provider Enrollment Specialists will initiate a verification process with PECOS for those Providers that have indicated their fee has been paid through Medicare. In this process, the system automatically checks the Provider’s Application Fee status in PECOS and indicates if a match was found using the available identifying information of the Provider.

CONFIDENTIAL

If the system can confirm that the Application Fee has paid, the Enrollment Specialist can advance the provider into the review step of the workflow and process the application. If payment of the fee cannot automatically be confirmed on PECOS, the Enrollment Specialist is required to perform a manual search on PECOS to confirm the payment. Provider Enrollment Specialists then record the results of the PECOS verification on the Provider file in the system.

Authorized Department users are able to view hardship waiver requests in their work queue. We can configure the workflow to send an email notification to Department user(s) when a hardship waiver has been requested. Authorized Department users will then navigate to the web portal to review the waiver request (including the signed form submitted by the Provider) and take an action to either approve or reject the waiver request. If approved, the authorized Department user will change the status of the waiver to "Approved" and can send the waiver request to CMS for final approval. Once approved by CMS, the Department user can update the waiver status to "CMS Approved." The application will then be automatically placed in the Provider Enrollment Specialist work queue for further processing.

Our solution tracks the aging of all such waiver requests, and the aging statistics are viewable by both the Department and other project staff through the web portal dashboard. Aging parameters in the system are configurable to allow for potential future changes in DPHHS policy.

3.10.10.8 Provider Revalidation

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. The system also will be 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 Provider type.

Our solution has a configurable Revalidation Monitoring workflow that governs the revalidation process for Providers, from initial notification through update, review, screening, approval, and potentially, termination.

Revalidation Due Notices

The system maintains an end date (revalidation due date) for each Provider in the system. In the current configuration, the initial revalidation notice is sent to the Provider 90 days in advance of their current revalidation due date in the system. This is a configurable parameter that can be easily updated within the system to meet DPHHS requirements. Providers that navigate to the web portal and begin an update process are automatically placed in the revalidation workflow if their due date is within 90 days of the current date. The system can also be configured to perform a ‘staggered’ revalidation schedule based on DPHHS defined rules.

The Revalidation Monitoring workflow creates notifications to Providers regarding the predetermined eligibility end date and that their enrollment is due for revalidation. The system can send a paper notice to the Provider (if the Provider is a converted Provider and may not yet have an email address on file) or most preferably via email in the case where we have a valid email address on file. The system can also be

configured to send both a paper notice and email depending on the Department's preference. The Revalidation notices contain the following types of information:

- Information and instructions regarding all screening and enrollment activities required for their Provider type
- A listing of all required forms, attachments, and addendums
- The date on which their current eligibility will end based on their current enrollment eligibility span
- The address and/or website for submitting forms, attachments, and addendums
- The Provider Services Call Center's telephone number and hours of operation

The system tracks all notices sent to Providers and can generate follow up notices at predetermined intervals, based on Department defined rules.

Revalidation Reminder Notices

The system is currently configured to send Revalidation notices as shown in *Exhibit 3.10.10.8-1: Frequency of Provider Revalidation Reminders*. As mentioned, the timing and sequencing of these notices are configurable within the system.

Notice Type	Timeframe	Reason
Initial Notice	90 days prior to the eligibility end date	Stating the need for the Provider to re-enroll to remain an active Provider
Notice of Intent to Terminate	60 days from the eligibility end date	No response from Provider to Initial Notice
Final Notice of Termination	30 days from the eligibility end date	No response from Provider to Notice of Intent to Terminate

Exhibit 3.10.10.8-1: Frequency of Provider Revalidation Reminders. *Our solution sends reminder notices to all Providers due for revalidation based on a schedule approved by the DPHHS.*

If the Provider fails to take the required action within each defined timeframe, the system creates a task in the work queue for a Provider Enrollment Specialist to review the Provider file and take appropriate action. If the next appropriate action is to forward the Provider file to the DPHHS for termination, the referral will include copies of all notices and documentation of all Provider contact throughout the 90-day period. Optionally, the system can be configured to auto-terminate the Provider if they have not taken any action to revalidate within their required timeframe.

Revalidation Completion Notices

If the Provider successfully completes revalidation, the system generates a written confirmation notice via email to the Provider. The email notice indicates that the Provider's information has been successfully revalidated, and includes the following information:

- Provider Identification Number (Medicaid ID)
- New enrollment eligibility dates
- Instructions on how to update Provider information prior to the next revalidation
- The Provider Services Call Center's telephone number and hours of operation
- Addresses for the Department and other project websites

3.10.10.9 Suspending Enrollments

In addition to the Revalidation Monitoring workflow discussed in the previous section, our solution is packaged with other enrollment monitoring workflows that can be configured for the Montana implementation to auto-suspend or cancel open enrollments based on defined rules. Other monitoring workflows within the system include the Enrollment Cancellation Process, License Monitoring Process, and Reactivate/Re-Open Provider Enrollments process.

Enrollment Cancellation Process

Our solution is packaged with an Enrollment Cancellation workflow that auto cancels new enrollments submitted by Providers if the Provider does not submit the electronic application within a period specified by the Department. The current configuration allows the Provider 10 days to submit their enrollment. This timeframe is configurable within the system. The monitoring process begins when the Provider initially clears the NPI and Duplicate check steps within the application entry process. The Provider receives a message at this point indicating that they have 10 days to submit their enrollment or their enrollment will be cancelled. For the Montana implementation, we will configure the notice to occur in a timeframe based on Department-identified auto-closure date(s). If DPHHS policy does not require the cancellation, we will turn off this service for the Montana implementation.

License Monitoring Process

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 navigate to the web portal to provide a new expiration date for 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.

If the State's License Board is capable of providing a web service or interface to the Providers Services module for purposes of validating license, our preference would be to handle the license monitoring via the interface. In this model, the system would request current license information (number and expiration date) from the Licensing Board and automatically update the system with renewed license information.

Reactivate/Re-Open Provider Enrollments

Authorized users have an online admin function that allows a user to reactivate or re-open a Provider's enrollment that may have been previously terminated or suspended. In our experience, reactivations are not typically done in bulk but are more of a one-off update based on request of the Department. However, the system does have a Reactivation workflow process that can be configured to reopen or reactive applications that had previously been suspended or closed. This process is configurable based on Department defined rules.

3.10.10.10 Maintaining Provider Agreements

Our solution displays Provider Agreements on the Agreements screen, which is the last screen the Provider sees prior to submitting a new enrollment or revalidation. The Department typically provides the

CONFIDENTIAL

agreements to MAXIMUS as PDF files and the agreement is posted as a link to the website for the Providers to view. Once the Provider reviews the Agreement and agrees to its conditions (by checking a checkbox on the screen) the Provider is then able to give their electronic signature and proceed with submitting the enrollment.

Our solution is configurable to display different agreements and contracts on the Agreements screen based on Provider type. The system is also aware, based on rules contained in the Corticon rules engine, as to which Providers require which type of agreement.

3.10.10.11 Storing and Viewing Provider Documents & Attachments

The MAXIMUS Provider Services solution maintains a full electronic record of data and documents as part of the Provider's complete enrollment profile. This includes attachments for documents that are required to be submitted by a Provider during the enrollment process. For example, if DPHHS policy requires a Provider to submit proof of NPI/Taxonomy (via NPPES) with their enrollment, the system will prompt the Provider to upload the NPI document. *Exhibit 3.10.10.11-1: Documents and Attachments* provides an example of the actions a Provider will take to upload proof of NPI.

All paper documents submitted by Providers are time-stamped, stored in our OnBase imaging and document repository, and linked to the Provider's enrollment profile for the entire lifetime of the Provider in the system.

CONFIDENTIAL

CONFIDENTIAL

3.10.10.12 Provider Search and Workflow History

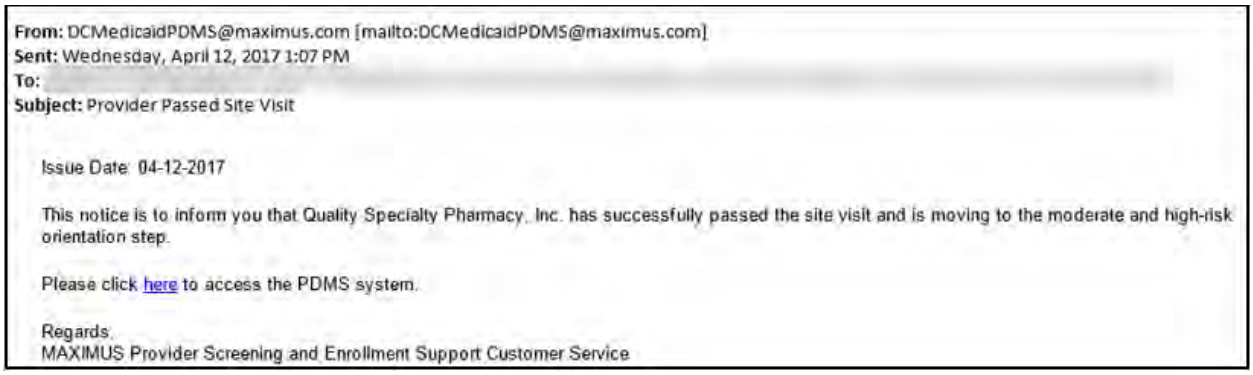
Our solution provides the functionality to allow a Provider to submit multiple application types and tracks the outcome of each submitted application. The system is packaged with a robust search function, a system dashboard that allows drilldown capabilities, and numerous on demand reports. *Exhibit 3.10.10.12-1: Provider Search* illustrates the types of search options a user has on-demand for finding a Provider in the system. These search and reporting capabilities allow users to search applications and trace the system and user actions that have been taken for each Provider submitted application.

In addition to searching for Providers in various statuses, our solution also contains automatic alerts and notices that can be generated to a target email address/user group based on Department defined rules. These email notifications are trigged by rules within the workflow engine for Providers that have reached a certain step in the workflow or where a specific type of action has been taken in the workflow. An example of this is the 'Provider Passed Site Visit' notice that is sent to an internal user group (configurable based on rules) notifying the user group that a specific Provider has passed the Site Visit.

The system contains several system-generated notices that perform functions similar to the Site Visit notice shown in *Exhibit 3.10.10.12-2: Site Visit Notification.* Our solution is configurable to use Department-defined criteria to automatically identify Providers and notify specific users when a Provider has previously submitted an application and whether the Department has returned a recommendation(s) for approval or denial of enrollment for that Application. All actions taken by any user in the system are recorded and searchable within the system. Furthermore, all eligibility spans and enrollment history are

CONFIDENTIAL

available in the system and the presence/absence of certain events for the Provider can trigger a notice to be sent to a user.



From: DCMedicaidPDMS@maximus.com [mailto:DCMedicaidPDMS@maximus.com]
Sent: Wednesday, April 12, 2017 1:07 PM
To:
Subject: Provider Passed Site Visit

Issue Date: 04-12-2017

This notice is to inform you that Quality Specialty Pharmacy, Inc. has successfully passed the site visit and is moving to the moderate and high-risk orientation step.

Please click here to access the PDMS system.

Regards,
MAXIMUS Provider Screening and Enrollment Support Customer Service

Exhibit 3.10.10.12-2: Site Visit Notification. *Our solution sends automatic notices to targeted users based on defined rules.*

3.10.10.13 Ownership Disclosure & Individuals Associated with an Application

The system captures all required information for each enrollment application, based on what is required by the Department for that Provider type but also what is required by ACA for screening purposes. In each of our implementations we have a screen in the enrollment flow related specifically to collecting Ownership and Disclosure information for the Provider. The form that is used to capture this information varies from State to State, but typically the system is required to capture the certain types of ownership information for the Provider, as shown in *Exhibit 3.10.10.13-1: Ownership and Disclosure Information.*

In addition to the information displayed in the summary Ownership grid, the system also captures the SSN, Birth Date, and Address for each of the owners and managing employees associated with the Provider. All Individual owners and managing employees with a 5% or greater ownership interest are subjected to the screening step within the new enrollment and revalidation workflow. These individuals are screened against OIG LEIE, SAM/EPLS, and SSDMF. Similarly, all owners are subjected to monthly screening against the same three (3) data sources.

During the internal review process, the Enrollment Specialists are required to review the Ownership information submitted by the Provider. If additional information is required, or if the Provider did not properly disclose all required Ownership information, the Enrollment Specialist can return the application to the Provider, requesting full disclosure of all Ownership information.

CONFIDENTIAL

Our solution is compliant with individual owners requiring fingerprints as part of the application process. All new and re-enrolling high-risk Providers and owners with a 5 percent or greater ownership interest are subject to a fingerprint-based criminal background check. While Medicare has defined two of these Provider types (home health agencies and durable medical equipment) as high risk, states are free to designate additional Provider types as high risk. In addition, states have the flexibility to lower the risk level of high-risk Provider types once they complete an initial background check. Other Provider types may also be elevated to the high-risk category if one of the following occurs:

- Credible allegation of fraud, waste or abuse
- An overpayment of $1500 or greater
- The Provider has been excluded by the OIG or another state's Medicaid program in the last 10 years
- The Provider type has been subject to a moratoria within the last six months

The system allows the Admin role to change a Provider's risk level that will automatically kick-off the background check workflow. Once identified as high risk, the Enrollment Specialist is prompted to check PECOS. If the Provider or owner has already passed a background check with Medicare or another state, the Enrollment Specialist records the information in the system, including the date of the background check and a screen print as evidence of the background check. If the background check is still required, the system identifies those individuals and sends a notice listing the locations where the fingerprints can be taken and also the date by which they must be received. Providing fingerprints and obtaining background check results requires coordination with the Department depending on what entity is being used to conduct the background checks, such as the state patrol, or a private background check vendor.

CONFIDENTIAL

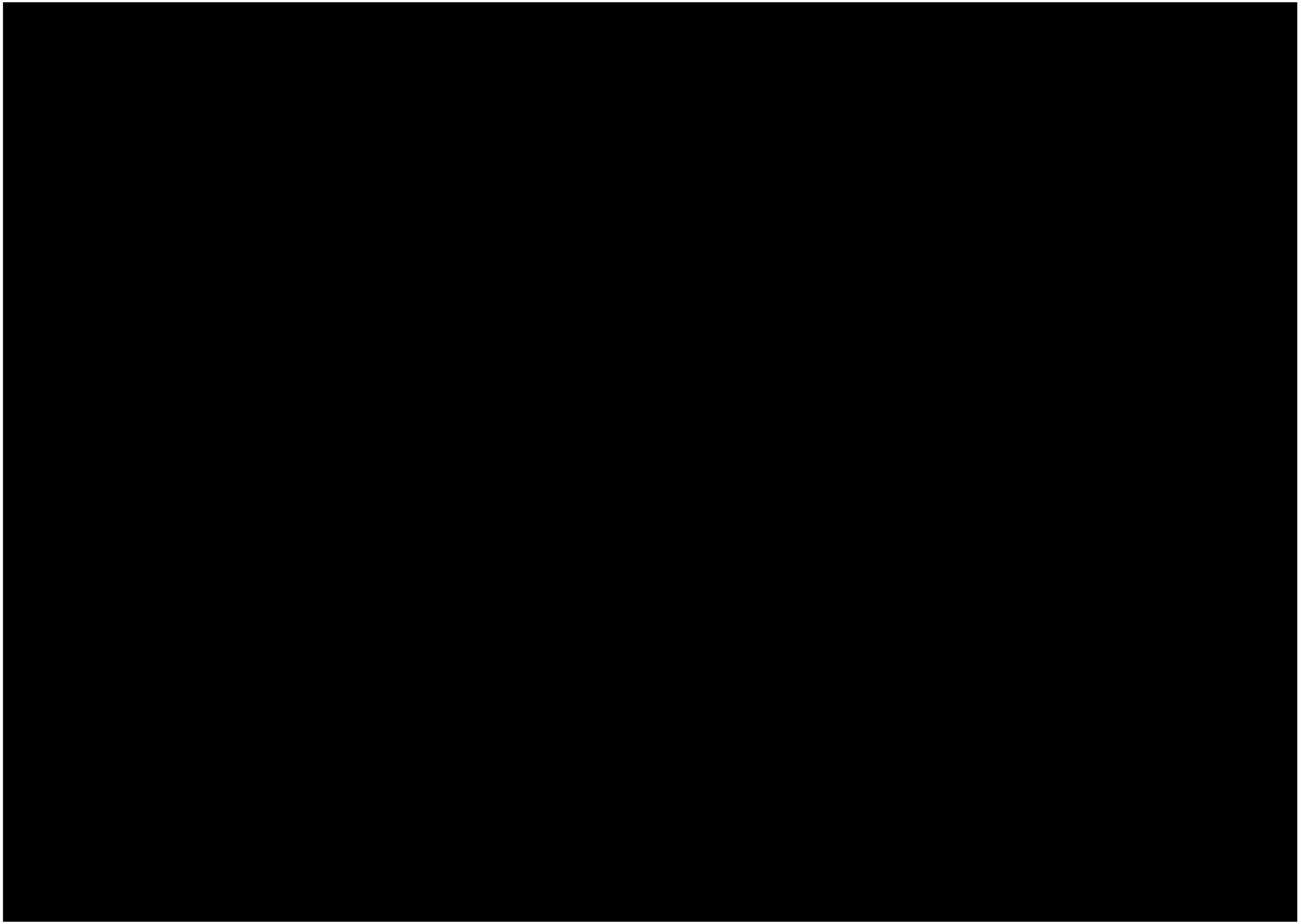
The Enrollment Specialist updates the system with the background check results and the system moves to the next step in the workflow.

3.10.10.14 Tracking Multiple Types of Enrollments

Our solution contains multiple configurable workflows to support all types of applications that the Department requires. Our solution contains a flexible Workflow Engine, working in concert with the Corticon Business Rules Engine, to support multiple processing workflows based on the type of enrollment application or form submitted. *Exhibit 3.10.10.14-1: Re-Enrollment Workflow* provides a visual representation of one of the many workflows within our solution.

The system's Workflow Engine can be configured to change the process flow to fit the needs of Montana DPHHS. The workflow tasks and steps are stored and displayed to reflect the real-time status of an application. The Workflow Engine stores all the information on the tasks for every application in the system.

CONFIDENTIAL



CONFIDENTIAL

New Enrollment Workflow

New Providers that enter a new enrollment through the web portal are placed in to the New Enrollment workflow. The New Enrollment workflow can take separate paths depending on the type of application being submitted (e.g., Fee-for-Service, Ordering/Referring). The system's Workflow Engine governs the path the Provider will take through the submission, review, and screening process and also the types of Users that will be required to take actions at various steps within the workflow. The rules engine is configured to control the types of data, documents, attachments, and screening categories the Provider will be required to complete, largely based on a combination of the Application Type and the Provider Type.

Revalidation/Re-Enrollment Workflow

Providers that initiate an update to their enrollment profile within 90 days of their enrollment renewal due date are automatically placed into the Revalidation Workflow. The 90-day window is a configurable parameter within the system. The system automatically generates Revalidation reminder notices to the Providers. Providers can click on a link in the reminder notice and navigate directly to the web portal to begin their Revalidation update.

The Revalidation Workflow behaves similarly to the New Enrollment Workflow, except the Provider is updating information that was either previously entered or was converted from the MMIS. Providers in the Revalidation workflow are subjected to the same review and screening requirements as a Provider in the New Enrollment Workflow.

Update Workflow

The MAXIMUS Providers Services solution also 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.

An example of a Provider using the portal to make an update would include a Provider who is updating/renewing their professional license. Once logged into the portal, the Provider can navigate directly to the screen to make the license update, submit the update, and exit the system. The submitted license update will be reviewed internally by the Enrollment Specialist, screened (if required) and then submitted to the MMIS via the MMIS interface. Providers can also opt to call or mail in a request for update. In this scenario, the internal Enrollment Specialist (or authorized user as determined by DPHHS) will have the authority to make the update in the system. In this scenario, the user will be required to upload supporting documentation as submitted by the Provider to provide an audit trail regarding the reason for the change.

3.10.10.15 Routing Applications to Department Program Integrity

Our solution's workflows can be configured to route applications and updates to any user at any step of the review process, per Department defined rules. In our Nebraska implementation, all applications that are approved by an Enrollment Specialist are sent directly to the MMIS, bypassing any sort of subsequent

CONFIDENTIAL

Department review. In our District of Columbia implementation, all applications are routed to the Department reviewer/approver role (whether approved or recommended for denial/termination) before being submitted to the MMIS. We will configure this workflow to meet the unique requirements for DPHHS in Montana.

Provider Integrity

In all our implementations, when the system or the Enrollment Specialist confirms a match on one of the screening databases, the Workflow refers the Provider to the Department reviewer role (or Department Program Integrity division) as required by the Department. *Exhibit 3.10.10.15-1: Adverse Actions* shows an example of the action the Enrollment Specialist will take to refer a Provider to the Department Program Integrity when a match is confirmed on a screening database.

When the Enrollment Specialist clicks on the Terminate button in the screenshot shown in *Exhibit 3.10.10.15-1: Adverse Actions* the Provider will automatically be routed to the Department Program Integrity for further review and action. The Department reviewer will be able to view all of the screening results on the Provider along with any supporting documentation (e.g., OIG Search Results) that were uploaded by the Enrollment Specialist. In the case where the application is a new enrollment, the action may be to deny the Provider, in the case where the Provider is in Revalidation, the action may be to terminate the Provider.

3.10.10.16 Tracking Site Visits

Our solution provides a workflow that is configured to require the completion of an unannounced pre-enrollment site visit by a Site Visit Specialist for moderate- and high-risk Providers once their preliminary screening and database checks have been completed and passed. The system reassigns these Providers to the Site Visit Specialist work queue and the next available Site Visit Specialist will retrieve the task and initiate the site visit process. These Providers will remain in a "Site Visit" review status until all required site visit actions are taken and the system has been updated.

CONFIDENTIAL

For providers where the system needs to validate the current Medicare enrollment status of a Provider, we use TIBCO to import the PECOS Unified Global Extract (UGE) for purposes of verifying enrolling providers. The PECOS UGE is a set of xml formatted files that contain provider enrollment data. These files contain provider information for all providers for all statuses. This includes approved as well as revoked providers. Our system provides automated checks against PECOS in the case where the system needs to validate participation in Medicare, if a site visit has been completed, whether a fee has been paid or if a sanction or background check has negative results.

Pre-Enrollment Site Visit

If the system determines that a Site Visit is required for the Provider, the system is configured to display a site visit checklist that the Site Visit Specialist must complete and sign during the site visit process. The Site Visit Specialist obtains the signature of the Provider's representative and uploads the signed checklist using the document upload function. All of these activities can be completed in the web portal while the Site Visit Specialist is performing the review at the Provider's site.

The required photograph of the Provider location's exterior, including the sign and street address can also be uploaded to the Provider file using the document upload function. These attachments remain a part of the permanent Provider record in the system.

The workflow will be configured to meet the site visit aging requirements as specified by both CMS and DPHHS policy. If the site visit cannot be completed on the Site Visit Specialist's first attempt (for example, the facility director was not in the office), the workflow will require another site visit attempt within 10 business days (or the number of days required by the Department). This task will remain in the Site Visit Specialist's work queue until all required activities have been completed for the site visit as per the checklist. *Exhibit 3.10.10.16-1: Site Visit Summary* provides an example of a pre-enrollment site visit summary that was completed for a moderate-risk Provider.

CONFIDENTIAL

Site Visit Specialists log failed site visits into the system, and the system assigns these Providers into the status of "Site Visit Fail." The next step in the workflow will be governed by the rules as specified by DPHHS. In our District of Columbia implementation, if the Provider fails the pre-enrollment site visit, the system refers the Provider application and supporting documentation to the Department Program Integrity. The Department reviews and handles appropriate follow-up, including issuing the notice of intent to terminate letter and any subsequent appeal made by the Provider. Authorized Department users are able to view all Providers with a status of "Site Visit Fail" in their dashboard and also in the work queue. Additionally, the system can be configured to bypass the Site Visit step in the workflow in the case where the site visit has already been completed by another agency, Medicare, or another state.

Post-Enrollment Site Visit

Once moderate-risk Providers have passed their initial screening and pre-enrollment site visit requirements and are approved, the system logs the initial date of enrollment and tracks the due date for the unannounced post-enrollment site visit. A task is created in the Site Visit Specialist work queue for a post-enrollment site visit to be completed within one year, but no sooner than three months, of the Provider's initial data of enrollment. The timing of these post-enrollment site visit is configurable based on DPHHS defined rules.

Once the post-enrollment site visit task is retrieved from the work queue, the Site Visit Specialist follows the same processes and procedures for the unannounced post-enrollment site visit that apply to the pre-enrollment site visit discussed previously. These processes and procedures include having the required checklist signed by both parties, taking photographs of the sign and street address, and making a second attempt to complete the site visit within 10 days of the failed first attempt. The Provider's application and

CONFIDENTIAL

supporting documentation are again referred to the Department in the case where the post-enrollment site visit has failed.

3.10.10.17 Provider Enrollment Requirements

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

ID	Provider Enrollment Requirement	MAXIMUS Summarized Response
ENR01	The Contractor's solution shall provide a unique submitter number for each billing service or submitter that transmits HIPAA X12 transactions with the State for single or multiple providers.	Our 3 previous Provider Services implementations have been Provider Services modular implementations but in all States, we are still interfacing with a legacy MMIS. Because of this, the business processes (and system functionality) for the enrollment of trading partners has remained with their EDIFECS/EDI platform. In our Tennessee Provider implementation, providers do have the ability to view X12 transactions via the self-service web portal through ESB integration with the EDIFECS platform. MAXIMUS will work with the Department to extend the capabilities of our enrollment process to track submitter numbers for billing services and other submitters for purpose of sending/receiving X12 transactions. We anticipate that the implementation of the ESB and the published services that are required to implement such functionality will be a prerequisite for implementing this functionality for Montana. During Requirements Validation for this requirement, we would like to discuss with the State the opportunity to leverage the existing (and potentially future) EDI platform to meet this requirement.
ENR02	The Contractor's solution shall receive provider applications through a web based provider self-service tool and on paper. The solution shall allow for the enrollment, re-enrollment, termination, recertification, or revalidation of providers and provide real-time notification to the providers of the receipt of the enrollment application.	Our solution accepts applications and updates by Providers via the web portal and through direct entry of applications by operations staff for paper applications. We also have a process to perform enrollment of large Pharmacy chains through import of a standardized enrollment file for Pharmacies.
ENR03	The Contractor's solution shall use automated screening and monitoring processes and tools to verify provider enrollment and eligibility based on Federal requirements contained in 42 CFR 455.436 (e.g., CMS data matching for provider screening and monitoring, Social Security Administration's Death Master File, the National Plan and Provider Enumeration System (NPPES), the List of Excluded Individuals/Entities (LEIE), the Excluded Parties List System (EPLS)).	The MAXIMUS Provider Service solution contains built-in mechanisms to support the full range of Provider enrollment and screening requirements mandated by the ACA. State visibility into the status of Provider activity is available through the dashboard, Provider search, and robust reporting capabilities in the Provider Services system. Please refer to *Section 3.10.10.5– Provider Screening* for further details on our existing screening capabilities and approach for the MPATH implementation.
ENR04	The Contractor's solution shall allow entities enrolling as trading partners with the State's healthcare programs to select the HIPAA X12 transactions they choose to submit and receive.	Please also see our response to ENR01. MAXIMUS will extend the enrollment capabilities of our Provider Services solution to allow for the enrollment and tracking of all required Trading Partner data, including the ability for the user to indicate their preferred list of HIPAA X12 transactions to submit and receive.
ENR05	The Contractor's solution shall assign a unique provider ID for all providers including atypical providers, for use in transactions with the enterprise.	Our solution assigns a unique ID to each Provider (including atypical) that establishes an account and begins an enrollment through the Provider Services web portal. This ID is referred to as the Provider's 'Registration ID'. This ID stays with the Provider throughout their lifetime as a Provider in the system.

ID	Provider Enrollment Requirement	MAXIMUS Summarized Response
ENR06	The Contractor's solution shall prompt users in the event of data entry errors, missing data or inconsistencies in the provider enrollment, maintenance, or revalidation process.	Our solution contains edits and validations throughout the application workflow to help confirm that Provider-submitted data meets CMS and Department requirements prior to initiating the internal screening process. The system prevents Providers from submitting applications that have missing, incomplete, or conflicting information. These front-end edits in the web portal are configured to meet any of the unique rules and policies required by the Department. Refer to *Section 3.10.10.1–Enrollment Submission* and other subsections for further details.
ENR07	The Contractor's solution shall allow enrolling providers to enroll in one or more program types (e.g., Care Management, waiver, CHIP, Standard Medicaid) using a single enrollment event.	During enrollment, the system allows Providers to select and to opt out of any State-defined programs when completing the Medicaid enrollment. Our solution will also allow the Provider to return to the portal and provide them the option to enroll in additional programs later. The system tracks the eligibility spans for all programs that the Provider may be enrolled and allows users to search on these programs, as needed. Refer to *Section 3.10.10.1–Enrollment Submission* and other subsections for further details.
ENR08	The Contractor's solution shall have configurable business rules to suspend or restrict the enrollment of providers, trading partners or clinics affiliated with individuals debarred by State or Federal agencies, listed in Registries (e.g., Child Abuse, Elder/Adult Abuse, Sex Offender), or do not meet requirements specified by the State.	Our solution contains robust functionality to prevent the enrollment of providers and to terminate or suspend the enrollment of existing providers based on Department defined rules. The actual action to deny or terminate a provider can occur through an automated process (e.g. failure to renew License) or through a combination of automated and manual processes (e.g. an identified match on the OIG/LEIE sanction database that has been confirmed by the Enrollment Specialist). Refer to *Section 3.10.10.5–Provider Screening* and *Section 3.10.10.15–Routing Applications to Department Program Integrity* for further details on how our solution provides this functionality.
ENR09	For enrolling and actively enrolled providers electing to participate in specific programs, the Contractor's solution shall collect and maintain the supporting data (e.g., geographic locations, number of preferred assigned members, and capacity to accept additional members), present the program agreement/contract for review, and acceptance (i.e., digital signature).	Our solution collects and maintains all supporting data required for a provider based on the provider's characteristics (e.g. Application Type, Provider Type, and Taxonomy). The system captures the Provider's office hours and its capacity to accept new members. Providers enrolling electronically via the web portal are required to provide an electronic signature when submitting their application or revalidated application. The primary practice location is required for each provider and additional practice locations can be optionally added.
ENR10	The Contractor's solution shall be configurable to allow or prevent provider enrollment based on provider characteristics.	Our solution is configured to allow or prevent enrollment based on provider characteristics. The system provides extensive automated screening capabilities to detect providers that may not be eligible for enrollment due to matches found on exclusion databases during the initial screening process and/or by the enforcement of Moratoria. Refer to *Section 3.10.10.5–Provider Screening* and *Section 3.10.10.15–Routing Applications to Department Program Integrity* for further details on how our solution provides this functionality.
ENR11	The Contractor's solution shall prevent the creation of duplicate records during enrollment application submission.	An important edit that is triggered during the new enrollment process detects when a Provider may be attempting to create a duplicate Provider in the system. In our experience, the definition of a duplicate Provider varies from state to state, but the system is configurable to fit whatever definition is required for Montana. Refer to *Section 3.10.10.1–Enrollment Submission* for further details on our approach for meeting this requirement.
ENR12	The Contractor's solution shall allow a provider to use a single enrollment application for multiple programs, specialties or service types.	During enrollment, providers are able to select from a pre-defined list (configurable) of programs where they intend to provide services. Providers are able to add multiple specialties and service types (for Waiver providers). All data is effective dated with start and end dates and a complete history is maintained by the system for the program and specialty data. During conversion, we build a complete set of reference data that relates Specialties, Taxonomies, and Service Types to Provider Types. Providers are then able to select from pre-defined lists based on their Provider Type. This reference data is configurable but initially is set up to match what is allowed on the MMIS.

ID	Provider Enrollment Requirement	MAXIMUS Summarized Response
ENR13	The Contractor's solution shall allow a single provider to enroll multiple service locations	The system requires the provider to enroll and to specify a primary practice (service) location, but the provider is also able to add additional service locations. Individual providers are able to indicate which billing providers they are associated with and billing providers (Groups, clinics) are able to add/update members to their practices. Providers are also able to enter their billing address, correspondence address, remittance address, and W9 address.
ENR14	The Contractor's solution shall collect and maintain all information needed to complete provider enrollment in compliance with all State and federal policies and regulations.	We have implemented our modular Provider Services solution in 3 different States. Each State has had different enrollment requirements, different enrollment forms, and different documentation submission requirements. By leveraging our Workflow Engine and the Business Rules Engine, we have advanced our system to be able to configure the enrollment and data collection processes to be flexible, capable of meeting any unique requirements for each State.
ENR15	The Contractor's solution shall determine provider eligibility in accordance with State and Federal policies and regulations.	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, revalidations, and updates 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
ENR16	The Contractor's solution shall provide the ability to accept and track provider enrollment fee information.	MAXIMUS configures the application workflow in our system to require Providers to submit an application fee prior to initiating the review and screening process. Configuration is based on CMS and Department regulations for the collection of application fees, which are required for prospective, re-enrolling, and reactivating institutional Providers. Unless a waiver is obtained, institutional Providers are required to pay an application fee unless they are already enrolled in Medicare or they have already paid the application fee to Medicare or another state program. Refer to *Section 3.10.10.7–Application Fee Processing* for further details on our approach for meeting the Application Fee requirements.
ENR17	The Contractor's solution shall allow providers to view status of their enrollment online.	Providers are able to view the status of their enrollments, revalidations, and updated directly from the Provider Homepage. Refer to *Section 3.10.10.1–Enrollment Submission* for further details on the Provider homepage.
ENR18	The Contractor's solution shall support real-time edits allowing providers to submit corrections to applications as needed.	Our solution contains edits and validations throughout the application workflow to help confirm that Provider-submitted data meets CMS and Department requirements. The system prevents Providers from submitting applications that have missing, incomplete, or conflicting information. During the Provider Review workflow step, if additional information is required, the Provider Enrollment Specialist is able to return the application to the Provider by using the "Return to Provider" function, which generates an email that lists the additional information required. This functionality eliminates the paper correspondence trail typically associated with the enrollment review and allows for timely and accurate processing of all required Provider applications and revalidations. Enrollment Specialists use the Return to Provider function primarily when a provider may not have uploaded the correct/required attachment with their enrollment (e.g., their W9 form was not signed, as an example). Refer to *Section 3.10.10.1–Enrollment Submission* and *Section 3.10.10.4–Enrollment Review* for details regarding system edits and return to provider functionality.

ID	Provider Enrollment Requirement	MAXIMUS Summarized Response
ENR19	The Contractor's solution shall be capable of suspending provider participation in specific programs while maintaining participation in other programs and initiate notification(s) to the provider, agency staff, and modules.	Our system provides for both automated and manual methods for suspending providers. Refer to *Section 3.10.10.6–Provider Screening* and *Section 3.10.10.16–Tracking Site Visits* for further details on the screening processes and workflows that are packaged with our solution. Our system also provides an administrative functional that allow the admin role (typically the Enrollment Specialist Manager) to take direct action on a provider to suspend their enrollment. This admin function allows the user to suspend the provider for participation in specific programs or for all programs. In all cases where the Provider's enrollment status has changed, automatic emails are generated and sent to a configurable list of recipients, based on Department defined rules. When available services are exposed through the ESB, our system can also send notifications of enrollment status changes to other modules within the MPATH enterprise.
ENR20	The Contractor's solution shall use automated screening and monitoring processes and tools to verify provider enrollment eligibility based on State regulations and policies (e.g., State licensing agencies, State exclusion lists, Provider Enrollment Chain and Ownership System (PECOS)).	The Provider Services 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. Our solution also provides for automated Provider monitoring for license expiration and enrollment expiration (failure to revalidate timely). Refer to *Section 3.10.10.5– Provider Screening* and *Section 3.10.10.9–Suspending Enrollments* for further details on our proposed screening and monitoring processes.
ENR21	The system will be able to link to training modules within the enrollment process (e.g., contractors authorizing member and provider services).	Our system provides links to training materials and user guides via the self-service web portal. The web portal provides a configurable eLearning link where all training materials and user guides can be posted to the website.
ENR22	The Contractor's solution shall support at a minimum, the following enrollment status designations or their equivalent: denied, terminated, suspended, provisionally accepted, accepted, in progress, pending, voluntarily terminated.	Our Provider Services system tracks the workflow status for each provider and also the enrollment status for each provider. We typically configure the system to match the types of enrollment statuses that are in place in the MMIS. The combination of our workflow status and enrollment status will meet this requirement for the State. Our solution provides for the statuses listed in ENR22 and can be configured to include more if required.
ENR23	The Contractor's solution shall allow users to enroll retroactively in compliance with State policy, ACA and CMS standards.	The system provides the ability for Providers to enroll retroactively. We have implemented this functionality in all 3 of our modular implementations, but each State's policy has been different (mainly in terms of which user can request the retroactive date and how the date becomes approved). The system configuration is to default the effective date for the provider to the approval date (screening completion date). In our most recent implementation in the District of Columbia, the configuration allows the provider to request a retroactive effective date, but when doing so they are required to supply an attachment that supports their claim for the retro enrollment. Enrollment Specialists review the request during provider review to determine if the retro request can be granted. In other implementations, any provider requesting a retroactive effective date is forwarded to the State Provider Services for review and approval. The system workflow automatically coordinates this transition. The system also provides an admin function where an authorized user can manually override or set the effective date to a retroactive date. In all cases, the effective date is sent to the MMIS through the MMIS interface.
ENR24	The Contractor's solution shall maintain the provider's effective date to begin administering services as of the date the provider screening process is complete as the standard effective date unless otherwise overridden and specified by the State.	The current configuration of our Provider Services module is to set the provider's effective date to the screening completion date. As mentioned in our response to ENR23, the system provides the functionality for this date to be modified or overridden.

ID	Provider Enrollment Requirement	MAXIMUS Summarized Response
ENR25	The Contractor's enrollment process shall be configurable to include trading partner enrollment within the overall provider enrollment business process.	Please also see our response to ENR01. MAXIMUS will extend the enrollment capabilities of our Provider Services solution to allow for the enrollment and registration of Trading Partners.
ENR26	The Contractor's solution shall present conditionally required resource materials and training required in order to complete the enrollment business process.	Our system provides for context sensitive online help and also provides the ability to add links to screens to describe the steps needed to complete specific enrollment functions. The links can display text, video, or both.

3.10.11 Maintenance

3.10.11 Maintenance

This section addresses provider maintenance requirements. The Provider Services module must support provider maintenance activities for external and internal users that are founded on business process driven workflow automation principles. Maintenance activities include the collection, storage, maintenance of information. It also requires ongoing automated provider monitoring necessary to support Montana Healthcare Programs business objectives and must be compliant with federal and state statues, policies and mandates. The Offeror must describe their approach to meet each of the Provider Maintenance requirements defined in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution includes a full slate of system functions and workflows that enables providers or internal users to update provider data. Our solution collects, stores, and maintains provider data that is viewable to authorized users. The database is populated with data that is provider-entered or received from the data conversion process from the MMIS. This data is reviewed and the providers screened and enrolled with data being sent to the MMIS to support other processing activities. Providers are able to update their data as regularly as necessary following an easy approach that allows the provider to navigate quickly to the data needing to be updated. In addition, internal users are also able to update provider data based on their role.

The MAXIMUS Provider Services solution employs a flexible workflow engine that routes applications through the enrollment and revalidation processes using business-defined rules. The workflow in which an application is placed is a function of application type, provider type (including risk level), and application status. Updates can be made to data at any time a provider is outside their revalidation period. When a provider must revalidate, additional workflows guide the provider through the data review and updated process. Within each workflow is a series of steps or tasks the application must pass before the workflow completes. The workflows also include rules for when to send emails to which entities, what screens to display based on provider type, and which document uploads are required. For example, a hospital will have the additional step within its workflow to display the application fee page, whereas a physician would not. A DME provider must go through the criminal background check process and the site visit process that a dental group would not. Our solution's workflows are configurable according to the State's requirements.

We are able to configure new workflows as necessary to support State requirements and based on our experience we understand that processing rules vary from state to state. For example, the District of Columbia had additional requirements for "sister agencies", such as the Department of Behavioral Health and Division of Disability Services. To accommodate this requirement, we created new user roles and configured workflows to confirm the applications flowed to these roles at the appropriate time in the process for review and approval. We also added steps in the workflows to accommodate review and

finalization steps at the District level. This flexibility verifies that our solution can accommodate the unique needs of different State Medicaid programs.

A key attribute of our system is the ability to configure workflows that monitor timelines, provider actions, and program requirements with the use of automated communications to inform providers of these items and additional processes to automatically take action if a provider does not take action. This includes things such as monitoring when a provider revalidation must occur, sending out reminder notices at various timeframes, and then terminating the provider if they do not revalidate. This could also include steps in a workflow such as informing a high-risk provider of the need to perform a fingerprint-based background check and tracking the compliance and results of this process.

Section 3.10.12–Self-Service Portal includes a detailed description of our Provider Self-Service Portal. Many of the functions required for Maintenance are also described in those system functions. The MAXIMUS solution is an integrated web-based system so the maintenance and self-service portal functions for Providers occur using the same functionality on the self-service portal. To validate we meet all requirements in the RFP, we have kept these sections separated but cross-reference areas where an explanation exists as part of the self-service portal functions.

3.10.11.1 System Workflow and Data Collection

The robust workflow options in our solution can accommodate any number of steps based on application type of provider type. *Exhibit 3.10.11.1-1: Workflow Configurations* is a snapshot of some of the scenarios currently in place in our solution. Some application types and provider types will have more workflows and steps than others due to details such as risk level, or whether an application fee should be collected. We spend time during requirements review to understand the complete workflows for the various programs and provider types.

Application Type	Provider Type	Applicable Workflows	Steps
Standard	Physician MD	▪ New or Revalidation	1. Provider Data Entry 2. Provider Review 3. Return to Provider 4. Provider Screening 5. Pending DPHHS Approval/Denial 6. Pending State Admin Approval/Denial 7. Sent to MMIS
Standard	Hospital	▪ New or Revalidation ▪ Application Fee	1. Provider Data Entry 2. Application Fee Review 3. Provider Review 4. Return to Provider 5. Provider Screening 6. Pending DPHHS Approval/Denial 7. Pending State Admin Approval/Denial 8. Sent to MMIS

Application Type	Provider Type	Applicable Workflows	Steps
Standard	DME	▪ New or Revalidation ▪ Site Visit ▪ Background Check	1. Provider Data Entry 2. Provider Review 3. Return to Provider 4. Provider Screening 5. Site Visit Review 6. Background Check Review 7. Pending DPHHS Approval/Denial 8. Pending State Admin Approval/Denial 9. Sent to MMIS
EPD Waiver	EPD	▪ New or Revalidation ▪ Site Visit ▪ LTC Review	1. Provider Data Entry 2. Provider Review 3. Return to Provider 4. Provider Screening 5. Site Visit Review 6. LTC Review 7. Pending DPHHS Approval/Denial 8. Pending State Admin Approval/Denial 9. Sent to MMIS

Exhibit 3.10.11.1-1: Workflow Configurations. *Our solution contains numerous workflows that are built with a series of steps that are triggered based on application type and provider type.*

We strive to reuse workflow steps to standardize operations to the extent possible. In addition, a workflow may direct the application to a different reviewer based on data. For example, if a provider requests a hardship waiver of the application fee, our current configuration requires a State reviewer to approve it. Therefore, while an applicant with a paid application fee will go to the operator role for review, a hardship waiver request goes directly to the State queue for review and approval before it moves to the next step.

The following sections contain several of the application screens in which providers supply enrollment information information. The application is then reviewed and screened by operators and State staff.

3.10.11.1.1 Data Entry and Maintenance

The data collection screens in the MAXIMUS Provider Services solution are simple and user-friendly with online help and field-level edits designed to expedite the provider enrollment process. Data requirements are defined at the application/program type, provider type and specialty level and data requirements are configurable to be required, optional, or to not display at all based on provider type or application type. This section provides screen shots of many of the screens contained in our solution.

CONFIDENTIAL

Account Creation

The first step in the online process is for the provider to create an account. Completing the account enables providers to create new applications for enrollment or to update their existing data that was converted from the MMIS. The provider must supply an email address during the account creation process, as shown in *Exhibit 3.10.11-2: Solution Login Screen*.

CONFIDENTIAL

CONFIDENTIAL

The account creation process triggers a validation email to be sent to the email address provided for the account. The email instructs the user to click the link to activate the account. This process verifies that the account holder has a valid email account and we tie that email account ultimately to the provider record as the processes continue. The provider may return to this screen at any time to maintain information, change a password or change security questions and answers. *Exhibit 3.10.11.1-3: Create User Account* shows how users are required to setup their account.

CONFIDENTIAL

The following email shown in *Exhibit 3.10.11.1-4: Account Creation Email* is sent to the provider to activate the account. The text in this email is configurable according to State specifications.

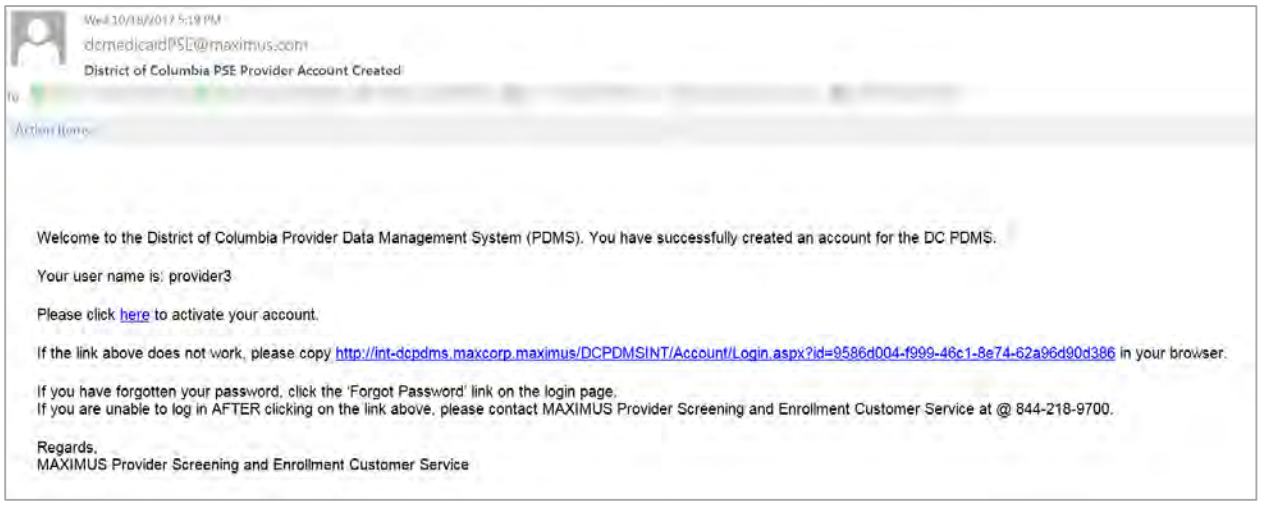


Exhibit 3.10.11.1-4: Account Creation Email. *The auto-generated confirming email to the account holder contains instruction to activate the provider account. Users must select the link to verify their email account and active the account.*

New and Existing Providers

Once an account is created and activated, the provider can log in to initiate an application or connect the user account to an existing provider already in the MMIS. In our current Provider Services configuration, the key identifier given to establish the account is the Tax ID of the Provider. This could be the SSN of an Individual Provider or the EIN of an organization/entity. If at least one Provider does exist (this could be either a converted Provider from the MMIS or a newly added Provider), then the user is required to add additional information that uniquely identifies a Provider using that Tax ID at a specific practice location. We configure the system based on the data elements that constitute a unique provider.

If the account being created belongs to an existing provider, the system enables the account to be connected to that provider. Sections 3.10.12.3 and 3.10.12.4 provide a detailed explanation of how converted providers are supported within the self-service portal. Because many of the maintenance activities are included in the self-service portal, we are trying not to duplicate the same information.

If there are no Providers existing in the system that currently use that Tax ID, the user is able to proceed in the account setup process without having to enter any additional demographic information for the Provider. The maintenance processes would then take over as described in the sections below.

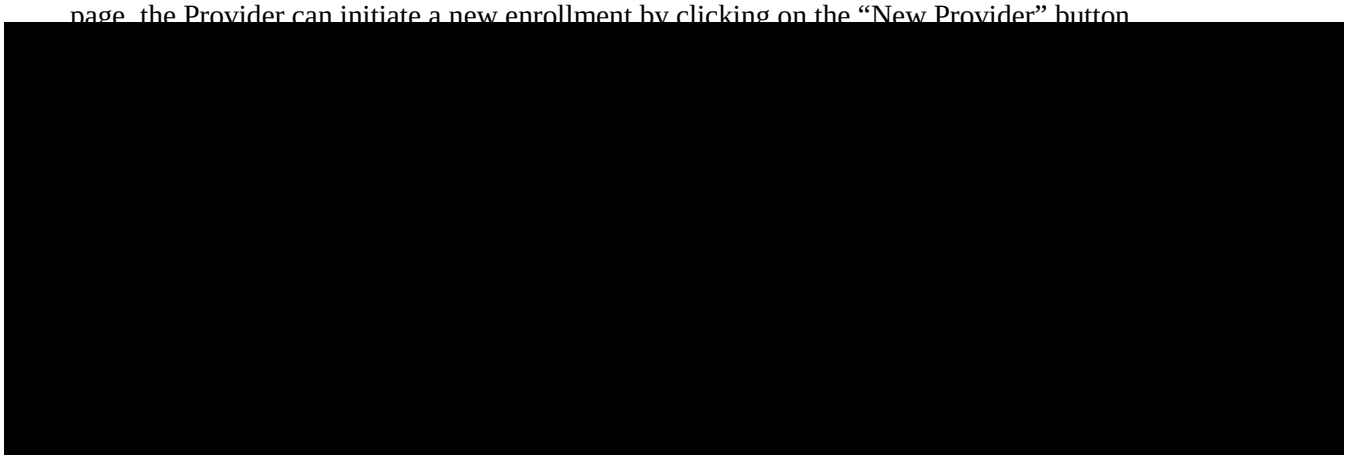
Application Type

Our solution is configured to have a variety of application types based on State requirements. We believe that the concept of application type is analogous to the concept of Program type. For example, because an ORP provider's application requires much less data than a fee-for-service provider does, the ORP provider selects the Streamlined application type. A waiver provider selects either the EPD Waiver, ADHP or HCBS Waiver application type. Once the application type is selected, the user is presented with

CONFIDENTIAL

a dynamic list of provider category configured to the application type chosen. Provider categories include individual, group, facility, or pharmacy.

Once a Provider user establishes an account on the web portal and authenticates for the first time, the user is taken to the Provider homepage as shown in *Exhibit 3.10.11.1-5: Provider Home Page*. From the home page, the Provider can initiate a new enrollment by clicking on the "New Provider" button.



After initiating the new enrollment, the Provider is then given the option to select from a pre-defined list of application/program types, as shown in *Exhibit 3.10.11.1-6: Application Types*. A provider can select multiple provider types by returning to the initial application selection screens.

CONFIDENTIAL

CONFIDENTIAL

Each application/program type has configurable predined data requirements and workflows. These application types will be configured to meet DPHHS enrollment requirements. In this example the Provider has selected the Standard Application, indicating they intend to become enrolled as a full fee-for-service Provider. *Exhibit 3.10.11.1-7: Select Provider Category* shows the next step in the new enrollment process where the Provider selects their category.

Provider Data Maintenance

As part of the configurable nature of our system, each provider and application type is configured to define required and optional data. Through this configuration, the workflow moves the provider through a series of screens that collects new data or maintains existing data. However, the data shown is specific for the provider and application type so that data that is not related is not even shown to the provider.

The sections below highlight a number of the screens that are used to collect different types of information. We provide examples of the types of providers that would need to enter the data but show the wide variety of screens to enable the State to see how data is collected and displayed.

After selecting the application type and category, our solution prompts the Provider to enter basic demographic information before launching the Provider into the new enrollment workflow. Data includes entry of first name, middle initial, and last name for indidivual providers and business entity name for groups, facilities or pharmacies. *Exhibit 3.10.11.1-8: New Enrollment Demographic Information* shows an example of the types of information the system captures for a new individual Provider beginning a new enrollment.

CONFIDENTIAL

CONFIDENTIAL

There are two (2) primary edits and checks that are triggered on this screen. First, our solution uses a real time web service call to NPPES to validate the NPI for the Provider. In the example above, the NPI entered is a Type 2 NPI (for an Entity) and the system will not allow the individual to proceed using the Type 2 NPI. The second edit that is triggered is to check whether the Provider already exists in the system. We will configure the duplicate check to match the rules specified by DPHHS for the module implementation.

As shown in *Exhibit 3.10.11.1-9: Provider Search Page*, users have access to the Provider Search screen where a user can seach on full or partial name, or a numbr of other provider identifiers. The robust search function also supports fnding applications that are in a certain status or by application tpe, category and provider type.

CONFIDENTIAL

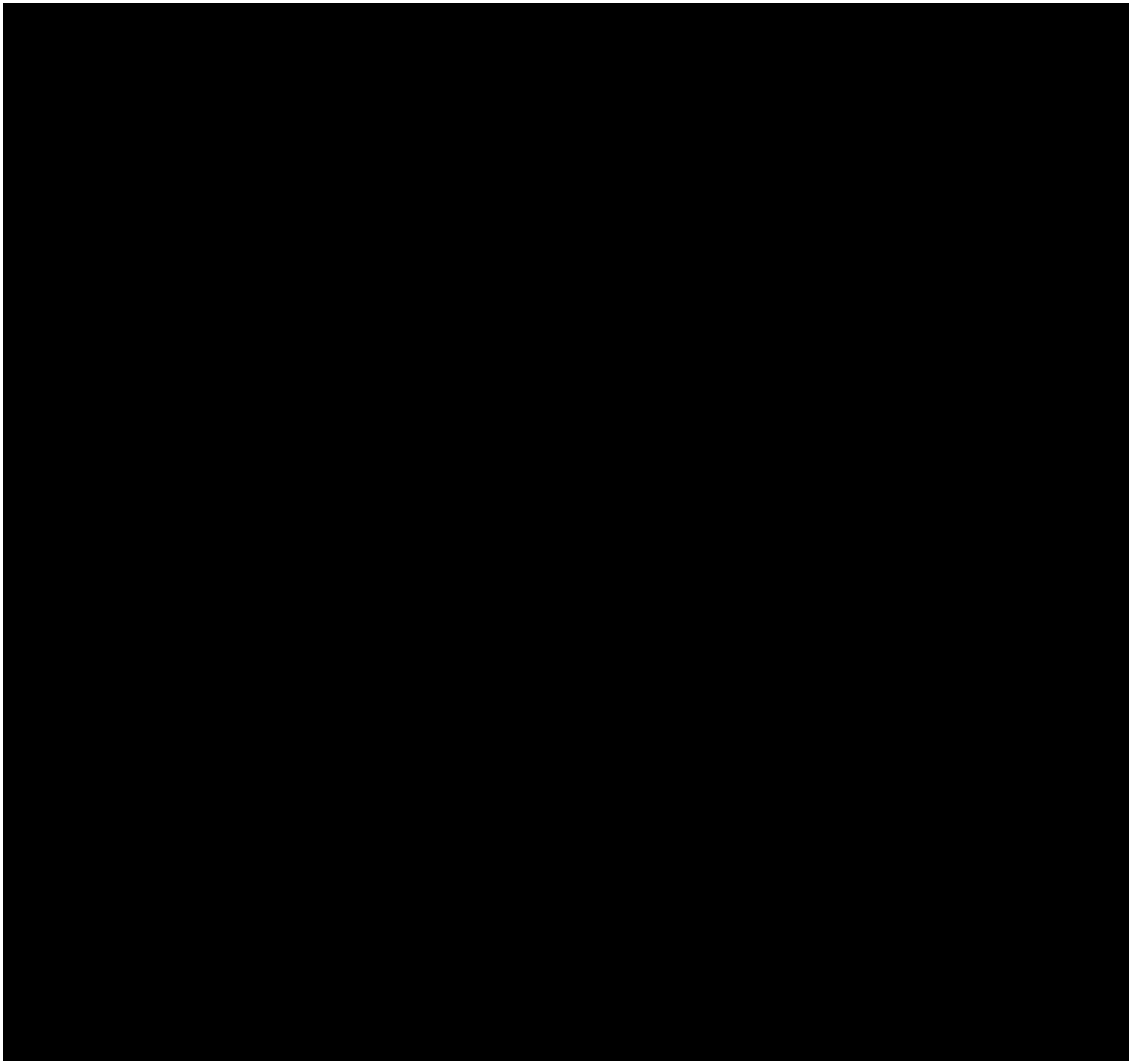
CONFIDENTIAL

Our solution contains dynamic navigation with one click access to other screens as well as additional detail within a screen. Each page provides a 'previous and 'next' button to allow users to easily navigate from one screen to the next. Our solution also has a Quick Jump drop-down feature that allows users to navigate directly to any screen within the system. *Exhibit 3.10.11.1-10: MAXIMUS Solution Navigation* shows how the other screens are accessed within a specific workflow.

Several of our solution's webpages contain icons that, with one click, display additional details about the data entered on the page. For example, when the history icon is selected on the CPR screen shown in

CONFIDENTIAL

CONFIDENTIAL



CONFIDENTIAL

CONFIDENTIAL

Demographic Information

The MAXIMUS Provider Services solution captures provider information according to the application type and the provider type. Several screens capture this data initially where it is viewable and editable by the provider or by an internal operator while the provider is in a maintenance status. Online history and audit tables are available for tracking changes on data.

Certain provider types are required to provide a professional license issued by the same State as the primary service address. The Professional License page as shown in *Exhibit 3.10.11.1-13: Professional Licenses* captures and displays licensure information, including begin and end dates, license state, license number and license type. Additional licenses can be added by clicking the “plus” sign. Clicking on the history icon displays the user name of the person who made an update as well as the date and time of the update.

CONFIDENTIAL

CONFIDENTIAL

Our solution can be configured to allow or require multiple license types. For example, like professional license requirements, some provider types are required to provide a valid DEA license that is verified during provider review. As shown in *Exhibit 3.10.11.1-14: Federal DEA Registration*, our system captures DEA information for applicable provider types. This page is configurable according to the requirements of the State to either be required, optional, or to not display at all. This page is also where the provider uploads a copy of the DEA license.

CONFIDENTIAL

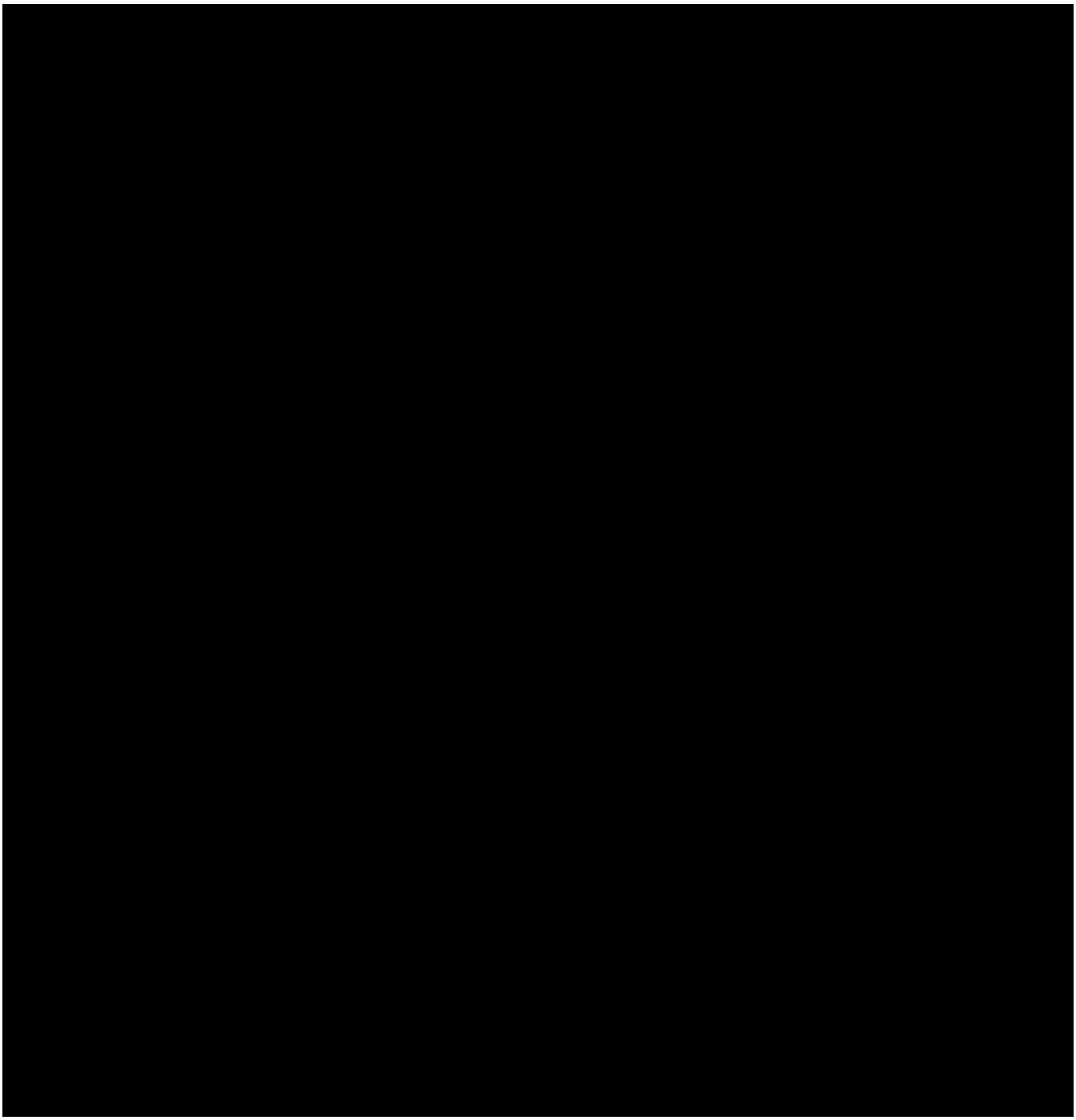
CONFIDENTIAL

Another program requirement for some provider types is a CLIA number. Like all pages within our solution, the CLIA Information page is configurable so that capturing this data is mandatory for certain provider types and does not even show up as an option for provider types where it is not applicable. *Exhibit 3.10.11.1-16: CLIA Information* shows that our system captures all required CLIA information for the provider, including the CLIA number, type, and effective date span. Online edits verify the CLIA number entered is in the correct format of two digits, followed by a D, then seven digits.

CONFIDENTIAL

CONFIDENTIAL

As an enrollment requirement, certain institutional providers must provide bed data as part of their enrollment application. The solution is configurable so this information is required only for provider types as designated by the State. *Exhibit 3.10.11.1-17: Number of Beds* shows how our system captures the total number of beds. We can also capture any number of data elements about specific practice components. MAXIMUS will work with the State to identify these additional data requirements and configure them to be collected as part of the application process.



CONFIDENTIAL

CONFIDENTIAL

Another page that captures provider certification is the CPR Certifications page. This is an optional page for individual providers and can be configured to be required per State direction and is depicted below in *Exhibit 3.10.11.1-19: CPR Certifications*.

[redacted]

DME providers in some states are required to hold accreditations based on the products and services the DME provider furnishes, as shown in *Exhibit 3.10.11.1-20: DME Page*. The current configuration also requires a document upload for verification of the accreditation.

Exhibit 3.10.11.1-20: DME Page. *This portion of the DME page captures the appropriate accreditation required for DME providers based on the services provided.*

CONFIDENTIAL

CONFIDENTIAL

Address and Contact Information

Capturing and maintaining contact information is key to ongoing communication with the provider. Our solution captures contact information at several points in the system, and the primary contact is the individual enrollment specialists should contact for application issues. The provider's contact information is captured and maintained on the Primary Contact Information page, shown in *Exhibit 3.10.11.1-21: Primary Contact Information*.

We understand that different states capture contact information in different ways. The MAXIMUS solution always requires the entry of a primary contact but we are able to configure the system to include additional contacts for the various addresses that we capture.

CONFIDENTIAL

CONFIDENTIAL

The MAXIMUS Provider Services solution requires at least one physical address for the providers. This address is used for populating the GIS map used in the public provider search function. This is also the address used for site visit purposes for moderate and high-risk providers. The provider or internal user can update this information when the application is in conversion or maintenance status. The Primary Service Address page is pre-populated with the Provider's legal name, as shown below in *Exhibit 3.10.11.1-22: Primary Service Address*.

CONFIDENTIAL

CONFIDENTIAL

All subsequent address pages contain fields for the provider to designate additional contacts for different purposes, including billing, correspondence remittance, and other. All address pages contain a copy feature that allows users to populate the form with the same address information entered on the primary service address page, shown in *Exhibit 3.10.11.1-23: Billing Address*.

CONFIDENTIAL

CONFIDENTIAL

A value-added benefit to our solution is the Address Verification function. The system provides a real time link to the USPS address verification service to validate all addresses that are entered into the system. This feature results in the standardization of all addresses in the solution as well as storing geo codes for the addresses so they can be used in maps or other value-added features. During new enrollment, all required addresses entered by the Provider (e.g., Primary Service Address, Billing Address, etc.) are validated through USPS. For converted Providers from the MMIS, the addresses are validated as the Provider goes through the initial update or revalidation in the system. *Exhibit 3.10.11.1-24: Address Verification Part 1* shows how the address verification pop-up appears for the Provider when the address is initially entered.

In *Exhibit 3.10.11.1-24* above, the Provider has entered an address into the system and clicked Save. Once this occurs, the system links to USPS web service to validate the address. The Provider can choose to accept the standard address returned from USPS or cancel and re-enter a different address. Notice in the screenshot above that the Address Line 1, County, and Zip Extension entered by the Provider are corrected in the USPS address pop-up. *Exhibit 3.10.11.1-25: Address Verification Part 2* shows the results after the Provider has accepted the corrected address.

CONFIDENTIAL

CONFIDENTIAL

As shown in *Exhibit 3.10.11.1-25* above, the corrected address fields for the Provider are moved to the page address fields. The Address Verification function also captures the geo coordinates of the address and these coordinates are stored in the system. This allows us to provide users (public and internal) the ability to view search results in GIS. Refer to *Section 3.10.12–Self Service Portal* for additional details on the GIS search function in our solution.

CONFIDENTIAL

Linking Individuals

Authorized internal users are able to link or unlink the affiliations of individual practitioners to billing providers using the same screens available to individual providers. The Group and Facility Individual Affiliation screen also captures start and dates of the affiliation. *Exhibit 3.10.11.1-26* and *Exhibit 3.10.11.1-27* show how affiliations are shown and maintained in the system.

CONFIDENTIAL

CONFIDENTIAL

Billing providers and internal users are able to add new members, end date existing members, and delete members. If we determine the affiliate is found to be unrelated to a group, our solution can automatically and manually unlink the individual from the group. In addition, if an individual's enrollment is terminated or end-dated, all affiliations with any billing provider are also terminated. For more information on linking individuals to billing providers, see *Section 3.10.12.7–Self Service Portal*.

Our solution also supports creating multiple relationships between providers and other entities. This includes the relationship of an individual provider to a group as well as relating providers to MCOs. Whether a provider is linked to an MCO, is FFS or is participating in another healthcare program such as medical home is displayed within the system based on X12 transactions through the State's EDI platform in conjunction with the legacy MMIS. We discuss this more thoroughly in *Section 3.10.11.1.3–Trading Partner Enrollment*.

CONFIDENTIAL

CONFIDENTIAL

Owner Information

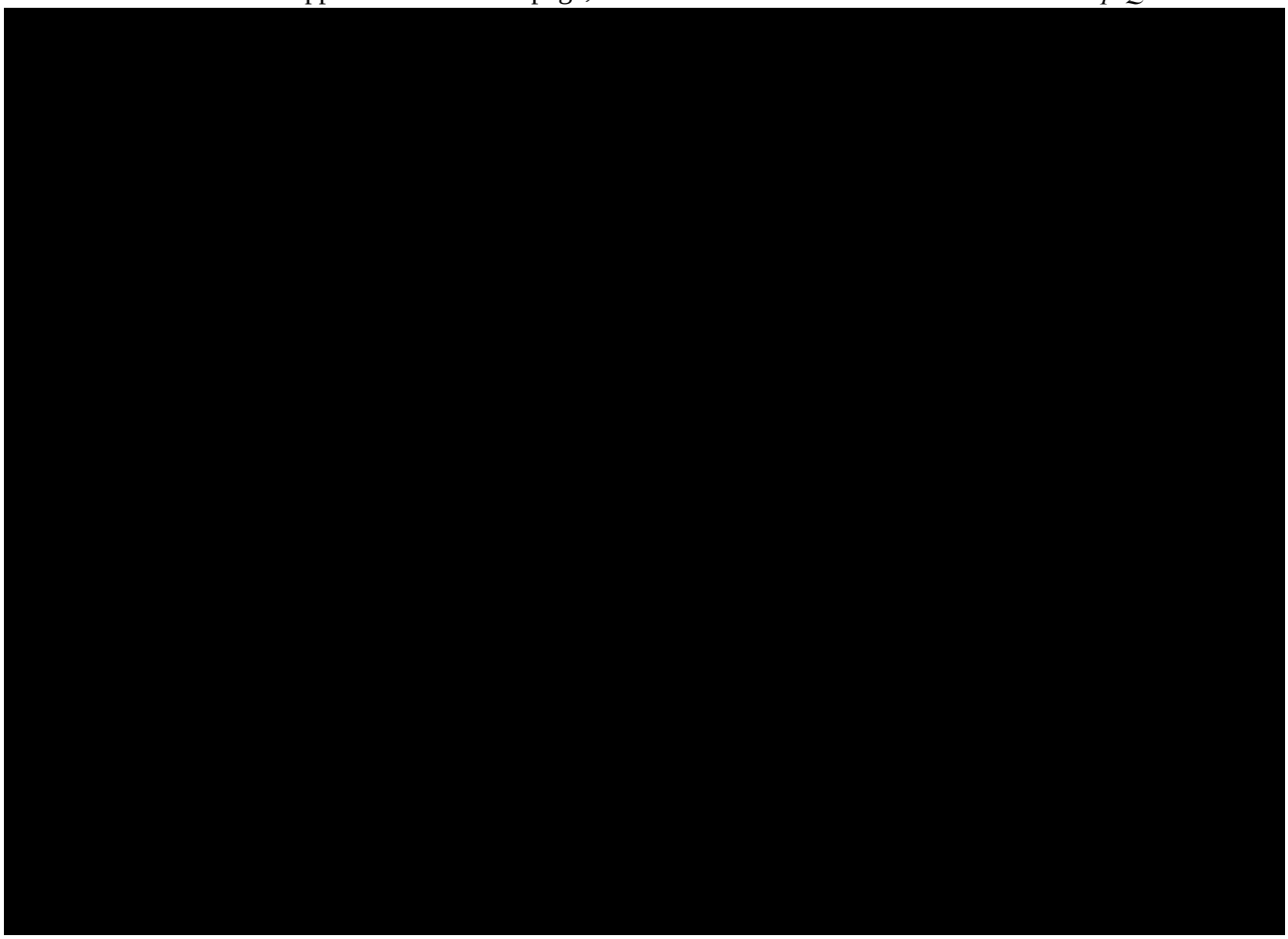
Our solution captures all required information for each enrollment application, based on what is required by the State for that Provider type but also what is required by ACA for screening purposes. In each of our implementations, we have a screen in the enrollment flow related specifically to collecting Ownership and Disclosure information for the Provider. The form that is used to capture this information varies from State to State, but typically the system is required to capture the certain types of ownership information for the Provider, as shown in *Exhibit 3.10.11.1-28: Disclosure of Ownership and Control Interest Statement*.

The owner information page captures ownership data, including individual, managing employee, and organizational ownership information. The owner page captures information such as tax id, birth date, percentage of ownership and address information for all owners and managing employees.

CONFIDENTIAL

CONFIDENTIAL

The federally required follow-up questions such as relationship of owners to one another or with subcontractors also appear on the owner page, as shown in *Exhibit 3.10.11.1-29: Ownership Questions*.



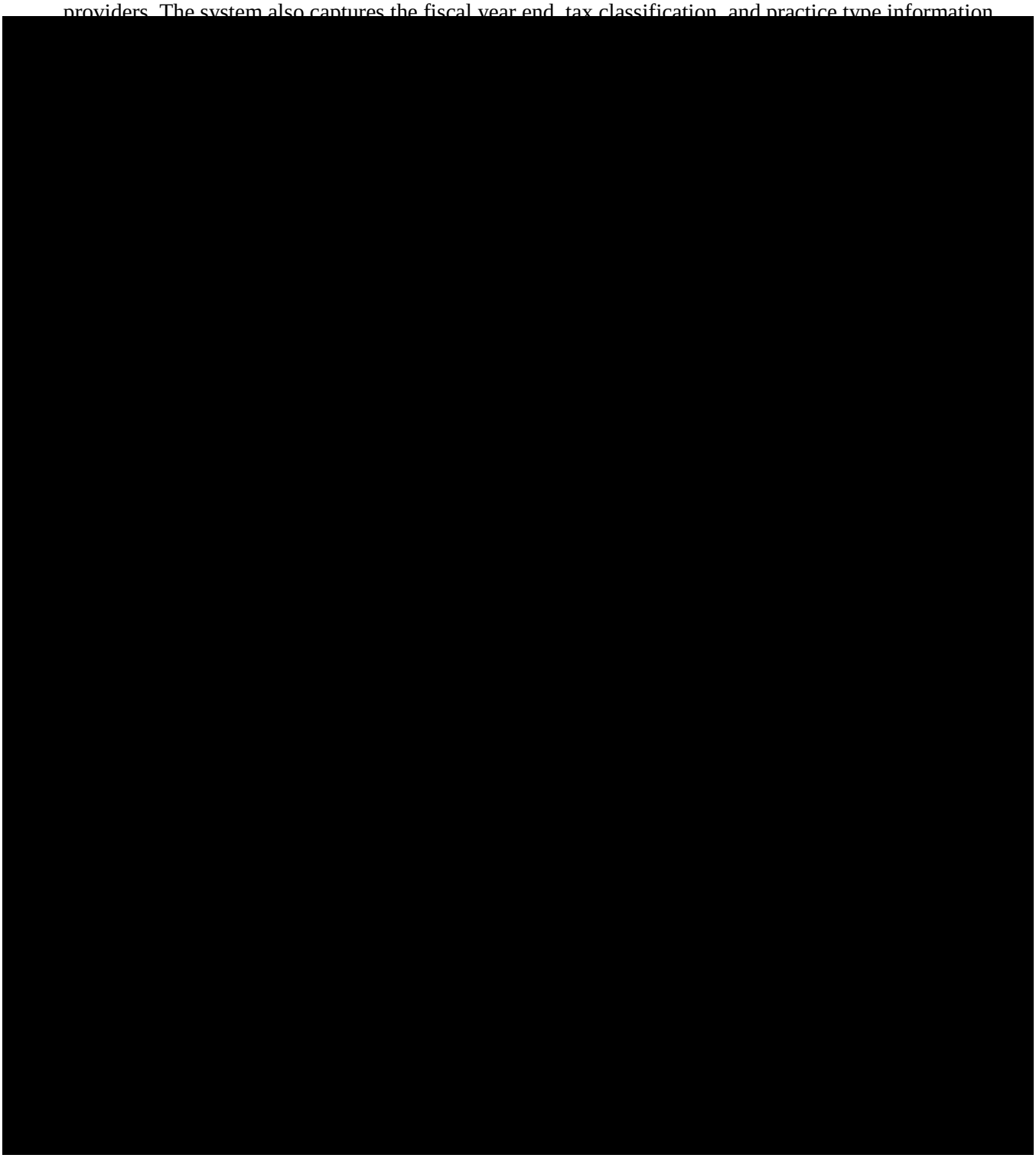
The ownership information that is captured is used in screening and for high risk providers, five percent owners will also have to submit to the fingerprint-based criminal background checks.

CONFIDENTIAL

CONFIDENTIAL

W-9 and DBA Information

Providers who receive payment from Medicaid must submit a W-9 form. Our solution requires providers applying with applicable application types to submit W-9 information. As shown in *Exhibit 3.10.11.1-30: W-9 Form, the W-9 Form page is pre-populated with the legal business name and SSN for individual* providers. The system also captures the fiscal year end, tax classification, and practice type information



CONFIDENTIAL

Payment Information

Most providers are paid using electronic funds transfer and States have implemented the requirement differently. In our Nebraska implementation, the ACH Authorization page was created to capture banking information for purposes of issuing EFT payments. In the District of Columbia implementation, the screen does not display as the District process of collecting this is done off-line. The approach and data collected on this screen, shown in *Exhibit 3.10.11.1-32: ACH Information*, is configurable according to the needs of the State.

MAXIMUS configures the application workflow to require certain institutional Providers to submit an application fee prior to initiating the review and screening process. Configuration is based on CMS and DPHHS regulations for the collection of application fees, which are required for prospective, re-enrolling, and reactivating institutional Providers. Institutional Providers are required to pay an application fee unless they are already enrolled in Medicare or have already paid the application fee to Medicare or another state program.

CONFIDENTIAL

CONFIDENTIAL

The amount of the application fee is a system parameter that we update in the system on an annual basis per the CMS published rate. Providers have the ability to submit an electronic payment online via a link in the web portal as shown in *Exhibit 3.10.11.1-33: Application Fee*, or by paper check through the mail.

CONFIDENTIAL

CONFIDENTIAL

Malpractice Insurance

Providers are required to maintain professional liability insurance with minimum coverage amounts in the aggregate and per occurrence. Information regarding malpractice insurance is captured on the Professional Liability Insurance page as shown in *Exhibit 3.10.11.1-34: Professional Liability Insurance*.

CONFIDENTIAL

CONFIDENTIAL

Providers are required to report details of malpractice claims submitted within the past ten years. Previous malpractice claims are captured on the Malpractice Claims History page, shown in *Exhibit 3.10.11.1-35*. Additional details of the claim are dynamic and required based on answers to previous questions. For example, if a suit was filed in court, the provider must supply the date and court case information.

CONFIDENTIAL

CONFIDENTIAL

Medicare Information

The MAXIMUS Provider Services solution comes with a Medicare screen for capturing any information related to the Provider's enrollment in that program. We will modify this screen to collect and maintain any additional data needed to support Pay for Performance (P4P) information received from Medicare through the TIBCO Managed File Transfer Service or other comparable CMS data matching service.

In addition to capturing Medicare enrollment date and Medicare number, as shown in *Exhibit 3.10.11.1-36: Medicare Number*, our existing Medicare screen captures subpart NPIs used by Medicare. This data can be added to an interface program to facilitate COB claims processing.

CONFIDENTIAL

CONFIDENTIAL

3.10.11.1.2 Data History

MAXIMUS appreciates the importance of maintaining data integrity by tracking changes with the ability to identify who made the change and when. Most data collection screens have a history icon to view the history of changes that may have been made to the data fields displayed on that section of the screen. *Exhibit 3.10.11.1-37: View Audit Trail* provides an example of a Provider viewing changes made to Primary Contact name for the Provider.

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.

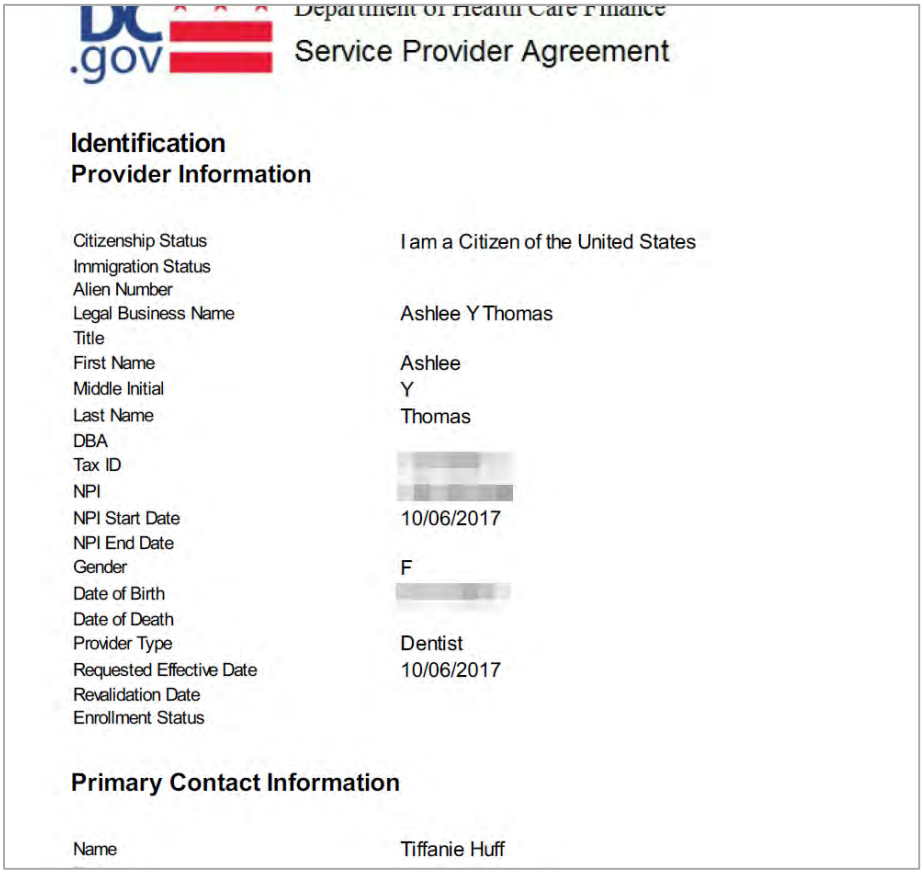
CONFIDENTIAL

CONFIDENTIAL

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 3.10.11.1-38: 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

The provider can view a PDF version of all data entries made into their application, as shown in *Exhibit 3.10.11.1-39: Provider Application PDF*. The system prompts them to review their data prior to application submission.



Department of Health Care Finance

Service Provider Agreement

Identification
Provider Information

Citizenship Status	I am a Citizen of the United States
Immigration Status	
Alien Number	
Legal Business Name	Ashlee Y Thomas
Title	
First Name	Ashlee
Middle Initial	Y
Last Name	Thomas
DBA	
Tax ID	
NPI	
NPI Start Date	10/06/2017
NPI End Date	
Gender	F
Date of Birth	
Date of Death	
Provider Type	Dentist
Requested Effective Date	10/06/2017
Revalidation Date	
Enrollment Status	

Primary Contact Information

Name	Tiffanie Huff

Exhibit 3.10.11.1-39: Provider Application PDF. *The responses provided during the application process are consolidated for review in a single PDF document.*

3.10.11.1.3 Trading Partner Enrollment

The MAXIMUS Solution is built on a normalized database that enables provider relationships to specific entities (e.g. groups, health plans, MCOs, PCMH, trading partners, etc.) to be tracked. For each of our three current module provider service installations, trading partner enrollment is managed and controlled through each state's EDI platform in conjunction with the legacy MMIS. We typically would envision this function being included as part of the Option A Provider Services so that providers or submitters can access X12 functions for our web portal. In our Tennessee Provider implementation, providers have the ability to view X12 transactions via the self-service web portal enabled through a SOA ESB integration with the state's EDIFECS platform for data owned by the requesting provider. As part of our CAQH-CORE implementation in Tennessee, we are currently working on an enhancement to enable all X12 transactions to be accessible from the web portal and to track Clearinghouse enrollments so they are able to access data for multiple providers. In the design, we are implementing a handshake approach so that a provider authorizes a clearinghouse to download the X12 transactions on its behalf.

CONFIDENTIAL

MAXIMUS will work with the Department to understand the capabilities in the current EDI platform and determine how best to track provider relationships with submitters for purpose of sending/receiving X12 transactions. We anticipate a need to integrate with the Montana EDIFECS platform to perform trading partner enrollment. MAXIMUS will extend the enrollment capabilities of our Provider Services solution to allow for the enrollment and tracking of EDI Trading Partners, including the ability for the entity to indicate their preferred list of HIPAA X12 transactions to submit and receive.

3.10.11.1.4 Provider Review

The enrollment approval workflows contain steps in which different users have a role in reviewing the same applications. An area for workers to make notes is essential to communication among reviewers. The MAXIMUS Provider Services solution contains a notes feature for internal users to create notes on the provider file. As shown in *Exhibit 3.10.11.1-40: Notes*, notes are viewable by all internal roles.

CONFIDENTIAL

CONFIDENTIAL

An Enrollment Specialist's home page is their work queue, which includes Providers that have already been assigned. *Exhibit 3.10.11.1-41: Provider Enrollment Specialists Queue* shows how tasks remain in a particular work queue until they are processed and are ready for the next step. Enrollment Specialists can either select from the list of Providers already assigned to them, or can retrieve the next Provider in the queue.

CONFIDENTIAL

CONFIDENTIAL

Once the Enrollment Specialist selects the Provider, they are able to begin the enrollment review process. An example Provider in Provider review is shown in *Exhibit 3.10.11.1-42: Enrollment Specialist Provider Review.*

Enrollment Specialists can either approve or reject the data. When rejecting the data, the Enrollment Specialist is able to return the application to the Provider to request the corrected information. Once all data is approved for the Provider, the Enrollment Specialist is able to approve the application, which will then move the application into the Provider Screening step of the workflow.

Provider Communications

Our 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. Providers receive email communications at designated events based on the workflow. In addition, all emails are viewable by the provider in the communication section of the home page. Our solution provides self-service capabilities for Providers to view and respond to requests received by internal users, most typically requests that are sent by Enrollment Specialists. The system also maintains a viewable list of all email notifications sent to the Provider (the Provider's 'inbox').

CONFIDENTIAL

CONFIDENTIAL

The provider is able to view this communication (and all communications) by visiting the homepage. *Exhibit 3.10.11.1-44: Provider Inbox* shows the portion of the Provider homepage where the Provider can view all communications sent to them by the system. For more information on our solution's email functionality, see *Section 3-10-12–Self Service Portal*.

MAXIMUS is implementing an external Correspondence Management platform supported by the Quadient Inspire ™ Platform. This platform will enables users to create timely, contextual, personalized and accurate communications for all channels, including email and SMS text, from one intuitive interface. We will capture the user's communication preference during the enrollment process. Like all data, the provider has the ability to update their preferences when they are in maintenance status.

3.10.11.1.5 Provider Screening

The MAXIMUS Provider Services solution is a CMS-compliant technology solution that performs all of the Provider screening and enrollment functions required by federal regulations (42 CFR 455 Subpart E). Our solution includes the ability to screen Providers against the following data sources:

- Office of Inspector General List of Excluded Individuals and Entities (OIG LEIE)
- Medicare Exclusion Database (MED)
- Medicaid Excluded Providers List (MCSIS)
- System for Award Management (SAM), formerly the Excluded Parties List System (EPLS)
- Social Security Death Master File (SSDMF)
- National Plan and Provider Enumeration System (NPPES)
- Provider Enrollment, Chain and Ownership System (PECOS)
- Department of Health for licensure, sanction and revocation data
- Licensure board data from other States
- DEA database to determine if the Provider has an active DEA segment

Our automated monthly database checks reveal the potential matches with the various exclusion databases required for screening and enrollment. A positive match during the monthly database check process sets the application up 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. The Provider Screening page shows the results of all database checks in the event of a hit as a result of the automated monthly database screening.

CONFIDENTIAL

CONFIDENTIAL

Exhibit 3.10.11.1-45: Provider Screening Results Page is a screen shot from our system showing matches and available data from a SAM/EPLS match and an OIG match on the List of Excluded Individuals and Entities (LEIE) database. An Enrollment Specialist can view to determine potential matches and recommend approval or termination of the Provider from the program.

The screening results for all Providers are available for review by all authorized users. DPHHS staff are able to view screening results for all Providers. Because many of the data sources do not have key data such as SSN, we configure the system to require a manual review in the cases where key data searches are not available. We will work with DPHHS to determine how best to configure the system in Montana.

CONFIDENTIAL

CONFIDENTIAL

Assign Risk Level

The MAXIMUS Provider Services solution is built to support the CMS requirements for additional screening activities based on risk level as established by 41 CFR § 455 and sub regulatory guidance in the Medicaid Provider Enrollment Compendium (MPEC). *Exhibit 3.10.11.1-46: Provider Risk Level* shows this risk level entry.

For more detail on assigning risk level, see *Section 3.10.10.13–Ownership Disclosure & Individuals Associated with an Application*.

CONFIDENTIAL

CONFIDENTIAL

Site Visit

High and moderate risk providers who have not already had a site visit conducted by Medicare or another state must have a new site visit when the primary service location address changes. A change to the address for these provider types triggers the site visit workflow. The site visit specialist records the results of the site visit, ass shown *Exhibit 3.10.11.1-48: Site Visit Screen*.

For more details on the site visit process, see *Section 3.10.10.16–Tracking Site Visits*.

CONFIDENTIAL

CONFIDENTIAL

Background Check

The MAXIMUS Provider Services solution also is compliant with CMS regulations by individual owners requiring fingerprints as part of the application process. When a high-risk provider reports a new owner with a five percent or greater ownership interest, the system triggers the background check process for the new owner.

If the Provider or owner has already passed a background check with Medicare or another state, the Enrollment Specialist records the information in the system, as shown in *Exhibit 3.10.11.1-49: Fingerprint and Background Check Information*, including the date of the background check and a screen print as evidence of the background check. If a new owner must be background checked, the system issues a notice to the provider indicating a 30-day deadline for the owner to supply fingerprints. A 10-day reminder notice is also generated if the owner has not supplied fingerprints by day 20. The system tracks this date and if fingerprints have not been obtained by the due date, the system automatically moves to the termination process. The Enrollment Specialist updates the system with the background check date, results, and who performed the background check (e.g., Medicare if applicable). Then the system moves to either approve or terminate the provider based on the results of the background check.

For more detail on tracking an owner's background check, see *Section 3.10.10.13–Ownership Disclosure & Individuals Associated with an Application*.

CONFIDENTIAL

CONFIDENTIAL

3.10.11.1.6 Provider Revalidation

The MAXIMUS solution captures revalidation requirements for providers based on risk category and provider type. The revalidation date is automatically populated on the Provider Information page, as shown in *Exhibit 3.10.11.1-50: Revalidation Date*. The system checks this date to identify providers due for revalidation. The revalidation workflow triggers notices to the provider at 90, 60, and 30-day intervals to prompt the provider to complete the online revalidation process. Revalidation applications are processed according to the same screening requirements as new applications.

CONFIDENTIAL

CONFIDENTIAL

When the system detects the revalidation date is less than 90 days in the future, the Begin Re-enrollment workflow is initiated automatically and the Begin Re-Enrollment link appears, as shown in *Exhibit 3.10.11.1-51: Begin Re-Enrollment*. The workflow contains a set of automated procedures that will remind the provider and ultimately terminate the provider if the revalidation processes are not completed in the appropriate timeframe. When the provider enters the system, the revalidation process is initiated by clicking the Begin Re-enrollment link.

The revalidation workflow takes the provider through the required data, capturing updates, and performing edits so all data is correct. In all three of our past implementation, the revalidation process is also used to capture additional data that was not included in the legacy MMIS and could not be converted. This process is also used to "clean up" old data that has been in the legacy system for years but may have not been updated as required.

CONFIDENTIAL

CONFIDENTIAL

3.10.11.1.7 Provider Updates

The MAXIMUS Providers Services solution contains an Update Workflow, shown in *Exhibit 3.10.11.1-52: Provider Update*, which allows existing Providers to use the web portal to make direct updates to specific types of data within their enrollment profile. We configure our solution based on state specific processing rules for the type of data that can be updated without involvement by the operations staff or approval from state personnel.

CONFIDENTIAL

CONFIDENTIAL

When a provider is in maintenance status and not due for revalidation, the provider can make updates to most data elements on the provider file. To make an update, the provider logs in and clicks the Update Registration link, as shown in *Exhibit 3.10.11.1-53: Update*.

An internal user with the Operator role can make updates to a provider file using the Update function on the Provider Search screen, as shown in *Exhibit 3.10.11.1-54: Operator-Based Update*. This action places the provider in the Update workflow and follows the same process as if the provider had made the update. Internal users can also retroactively change data, such as effective dates, to be in the past.

CONFIDENTIAL

CONFIDENTIAL

3.10.11.1.8 Changing Provider Status

An internal user with an Administrator role has the ability to change a provider's effective date, terminate or dis-enroll a provider, and reactivate a terminated provider.

Terminate Provider

The MAXIMUS Provider Services solution contains a termination feature that can done individually or in mass through a development script to identify providers based on criteria determined by the department. The system can either place all providers in a termination workflow for manual review, or automatically update the status with a termination reason and date that will then trigger the transaction to the MMIS.

The administrator role has the ability terminate a provider using the Admin function while the provider is in conversion or maintenance status, as shown in *Exhibit 3.10.11.1-55: Provider Termination*. The administrator must enter a termination reason and effective date of termination for transmission to the MMIS. The list of termination reasons and codes are configurable according to the requirements of the State.

Disenroll Provider

Our solution is designed in compliance with MITA standards, including supporting the separate business processes for Disenroll Provider and Terminate Provider. In our solution, the term 'dis-enroll' applies to Providers opting voluntarily to no longer provide services in the State's Medicaid program. In our other State implementations, Providers are able to request dis-enrollment via the web portal but an internal review process is required before the dis-enroll action is taken on the Provider. The system also provides functionality to auto-terminate Providers in the case where re-enrollments are not completed on time or when license are not renewed on time. In all cases where eligibility is ending for a Provider (regardless of the reason) system generated notices can be sent to select email groups to notify State users (and potentially other stakeholders) that the Provider's enrollment has ended.

CONFIDENTIAL

CONFIDENTIAL

Authorized users with the Administrator role have the authority to dis-enroll providers in the conversion or maintenance status by using the Provider Disenrollment feature. The screen shown in *Exhibit 3.10.11.1-56: Provider Disenrollment* can be configured to capture additional information and to send to the MMIS.

The disenrollment function is completed at the provider type/Medicaid ID level. The provider may stay enrolled under other Medicaid IDs they may have for other services. Waiver providers approved for specific services may be unapproved from providing some services while staying approved for others.

Suspend Provider

The MAXIMUS Provider Services solution is packaged with enrollment monitoring workflows that can be configured to the Montana implementation to auto-suspend or cancel open enrollments based on defined rules. Other monitoring workflows within the solution include the Enrollment Cancellation Process, the Revalidation Monitoring workflow, License Monitoring Process, and Reactivate/Re-Open Provider Enrollments process.

Enrollment Cancellation Process

The Enrollment Cancellation workflow auto cancels new enrollments if the Provider does not submit the electronic application within a period specified by the State. The current configuration allows the Provider 10 days from the date the application was started to submit the application. This timeframe is configurable within the system. The monitoring process begins when the Provider initially clears the NPI and Duplicate check steps within the application entry process. The Provider receives a message at this point indicating that they have 10 days to submit their enrollment or their enrollment will be cancelled. For the Montana implementation, we will configure the notice to display no later than ten (10) business days prior to the State-identified auto-closure date(s). In addition, we will make sure that Providers receive a subsequent automated notification of auto-closure regarding open enrollment applications. The subsequent notification will be configured to be sent no later than two (2) business days prior to the State-identified auto-closure date.

CONFIDENTIAL

CONFIDENTIAL

License Monitoring Process

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 navigate to the web portal to provide a new expiration date for their renewed license. If the Provider does not take the action to renew the license and the license expires, the system auto-terminates the Provider for failure to renew the license. Optionally, our system can be configured to refer these Providers to the State for further review prior to taking the action to terminate the Provider.

If the State's License Board is capable of providing a web service or interface to the MAXIMUS solution for purposes of validating license, our preference would be to handle the license monitoring via the interface. In this model, our solution requests current license information (number and expiration date) from the Licensing Board and automatically updates the system with renewed license information.

Reactivate Provider

Authorized users have an online admin function that allows a user to reactivate or re-open a Provider's enrollment that may have been previously terminated or suspended. In our experience, reactivations are not typically done in bulk but are more of a one-off update based on request of the State. However, our solution does have a Reactivation workflow process that can be configured to reopen or reactive applications that had previously been suspended or closed. This process is configurable based on DPHHS defined rules.

The Administrator role is able to reactivate terminated providers, as shown in *Exhibit 3.10.11.1-57: Reactivate Provider*. The user must enter the new effective date, new revalidation date, and comments explaining the reason for the reactivation.

CONFIDENTIAL

CONFIDENTIAL

3.10.11.1.9 Data Retention

MAXIMUS will retain all data (including PII) as directed by DPHHS, understanding the data retention requirements might be longer for some data. 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 percent 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.

All uploaded documents are viewable in the provider file indefinitely or according to record retention requirements by clicking the download link shown in *Exhibit 3.10.11.1-58: Document Display*.

3.10.11.1.10 Mass Updates

MAXIMUS understands that program changes or other factors may necessitate a mass update to provider data or even a mass disenrollment. Our solution is capable of performing mass updates based on criteria defined by DPHHS by writing scripts that are tested thoroughly in test environments for the desired outcome. The script can include email or paper communication to affected providers with text drafted in collaboration with DPHHS. In our previous implementations, we have found that mass updates take the form of very different processes that need to be full vetted and tested before they are executed in production.

Payment Support Functions

To support functions that are managed by other system modules, the MAXIMUS solution must include the ability to link provider data owned by our solution with data that is used across the Medicaid Enterprise. We are able to handle these situations in a variety of different ways. For data that is contained in the MMIS, we already provide sophisticated cross-reference functions that enable us to maintain provider data and send accurate provider updates to the MMIS. These cross-references are built as part of the data conversion effort and enable MAXIMUS to direct data updates to the specific provider entities in the MMIS.

This cross-referencing functionality will allow our solution to automatically link the unique provider records in our Solution to other provider IDs used throughout the State enterprise (e.g., SABHRS or State Eligibility Systems IDs). We can store these additional provider IDs in the same manner we handle Medicare numbers or we can extend the functionality to allow more of relationship process where we create relationships between the provider and these entities to allow many to many relationships. Our online portal allows providers to enter these additional identification numbers and edits can be enforced to

CONFIDENTIAL

require these numbers if necessary. We can also load these numbers during the data conversion process. Our solution will display all provider IDs that are associated with the unique provider in our solution.

As part of our implementation of the trading partner functionality, we intend to create a relationship structure between submitters and providers. This concept will enable a many to many relationship where a provider can have more than one submitter and a submitter can submit for more than one provider. This relationship will also include the transaction types so that a provider can use different submitters to submit different transactions if necessary. We will enable functionality so that a provider can designate one biller to receive 835 files. These complex configurations will require extensive discussion during requirements review where we will create matrix of the transaction types and the relationships that are allowed for each.

3.10.11.1.11 Maintenance Requirements

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

ID	Maintenance Requirement	MAXIMUS Summarized Response
PMNT01	The Contractor's solution shall have the capability to terminate inactive providers based on criteria determined by the department for either automatic termination or initiate a workflow for manual termination.	Our solution features a monitoring program in which provider registrations are targeted for closure based on configurable rules. For registrations meeting certain criteria (such as an expired license), the program initiates automated termination. Other criteria can initiate manual terminations, such as a potential hit on an exclusions database. We will configure termination workflows according to DPHHS parameters. For more information on Provider termination, *see Section 3.10.11.1.8–Changing Provider Status* and *Section 3.10.11.1.10–Mass Updates*.
PMNT02	The Contractor's solution shall collect and retain electronically all provider documentation (e.g., original application and copies of correspondence) for actively participating providers. For terminated providers, records shall be retained electronically according to record retention requirements (i.e., 7 years).	In our current configuration, the solution supports the scanning and indexing of paper enrollment forms and stores them in a Hyland OnBase document repository. All Provider correspondence, whether paper-based or electronic, is captured and retained in our document repository as electronic copies for the period specific by the State. For more information on document retention, see *Section 3.10.11.1.9–Data Retention*.
PMNT03	The Contractor's solution shall require, capture and maintain the 10-digit National Provider Identifier (NPI) for all healthcare providers required to have an NPI and interface with NPPES to verify the NPI is valid.	The MAXIMUS Solution is natively compliant with NPI and has an interface with NPPES to validate the NPI. Group Providers must enroll using a Type 2 NPI (Organization) and Individual Providers must enroll using 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. See *Section 3.10.11.1.1–Data Entry and Maintenance, Provider Key Identifiers*, for more information on collection of the NPI and the NPPES interface.
PMNT04	The Contractor's solution shall record and display begin and end dates for specific provider enrollment and demographic data (e.g., license, eligibility period, physical address) and provide access to historical provider record information.	The MAXIMUS Provider Services solution maintains effective dates (begin and end dates) for all enrollment data based on provider type. Providers must enter and upload license data and operators validate license data. The solution maintains current and historical address information for providers that is viewable online. All data is stored in the database and history is accessible. For more information on displaying and maintaining demographic data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Demographic Information*.
PMNT05	The Contractor shall use a standardized format for provider names that differentiate between first name, middle name/initial, last name, and business or corporate names and allows flexible searches based on the provider name.	The MAXIMUS Provider Services solution uses consistent provider naming conventions to differentiate between first names, last names, and business or corporate names. Search capabilities are flexible and allow for partial and full name searches. See *Section 3.10.11.1.1–Data Entry and Maintenance* for more information on capturing provider names and the solution search function.

ID	Maintenance Requirement	MAXIMUS Summarized Response
PMNT06	The Contractor's solution shall allow provider records to be associated and linked by tax identification number (TIN) and parent organizations.	Our solution provides for multiple relationships between providers and other entities. This includes the relationship of an Individual provider to a group as well as relating providers to MCOs. Ownership data, including individual, organizational ownership is captured and maintained for each provider. In addition to supplying a TIN, providers must also supply the NPI of the group to be associated. For more information on affiliations, see *Section 3.10.11.1.1–Data Entry and Maintenance, Linking Individuals to Billing Providers*.
PMNT08	The Contractor's solution shall allow for collection and maintenance of site visit, finger printing and background check information (e.g., the type of site visit (e.g., field representative, pre enrollment, program staff), date the site visit/ finger print/background check completed, reason and outcome if applicable).	Enhanced screening is part of the solution's standard workflow according to the provider's risk level. High and moderate risk providers are required to pass a site visit with high risk providers also required to pass a fingerprint-based background check. Our solution tracks all steps in these activities, as well as outcomes, to help inform enrollment decisions. For more information on collecting site visit and background check information, see *Section 3.10.11.1.5–Provider Screening, Site Visit and Background Check*.
PMNT09	The Contractor's solution shall collect and maintain licensure information to include at a minimum, licensing state, license number, licensure begin and end dates.	Our solution captures expiration dates for all credentialing data, including licenses. It maintains effective dates (begin and end dates) for all enrollment data based on provider type. Provider license information, including licensing state and license number, is required and screened at enrollment and revalidation. For more information on collecting and maintaining licensure information, see *Section 3.10.11.1.1–Data Entry and Maintenance, Demographic Information*.
PMNT10	The Contractor's solution shall collect and maintain the Pay for Performance (P4P) information from Medicare.	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. Our system will be modified to support the collection and maintenance of Pay for Performance information from Medicare. For more information on Medicare data collection and TIBCO, see *Section 3.10.11.1.1–Data Entry and Maintenance, Medicare Information* and *Section 3.10.1.6–Interfaces*.
PMNT11	The Contractor's solution shall collect and maintain date specific (as applicable) provider endorsement and accreditation information.	We understand that States may require capturing and maintaining specific accreditations based on provider type. Our highly configurable solution currently captures CPR certification for individual providers. The solution also captures for DME/POS providers Our solution can be configured for capturing additional state-specific data elements, including endorsement or accreditation number, effective dates, source, type, and level if applicable. We prefer to conduct verification by automated interface where it is an option for agencies with this ability. For more information on capturing and maintaining accreditation data, see *Section 3.10.11.1.1–Data Entry and Maintenance* and *Section 3.10.11.1.2–Data History*.
PMNT12	The Contractor's solution shall collect and maintain malpractice insurance information including expiration date.	To submit an application, a provider must submit liability insurance information, including effective and expiration dates, carrier name and address, policy number, agent name and coverage amounts both by occurrence and in the aggregate. For more information on malpractice insurance and malpractice claim data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Malpractice Insurance*.
PMNT13	The Contractor's solution shall provide dynamic navigation that allows users to have one click access to additional detail for summary information (e.g., from the providers screen, select a specific location to view location details such as address, contact(s), office hours).	The MAXIMUS Provider Services solution provides a 'PRIOR' and 'NEXT' button on each webpage to allow users to easily navigate from one screen to the next. Each screen also contains edit icons that allow the users, with one click, to add, view, or update additional information.
PMNT14	The Contractor's solution shall collect and store standardized W-9 information that reflects the owner of the EIN and the Doing Business As (DBA) name.	The solution requires providers paid by Medicaid to submit w-9 information. This includes indicating the fiscal year end, tax classification, and practice type information. DBA information is captured on the Provider Information screen. For more information on capturing W-9 and DBA data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Provider Key Identifiers*.

ID	Maintenance Requirement	MAXIMUS Summarized Response
PMNT15	The Contractor's solution shall provide the capability to reactivate terminated providers without requiring a complete re-enrollment.	Users with the Administrator role have the ability to reactivate terminated providers. To reactive, the Administrator role must enter the new Effective date, the New Re-enrollment Due Date and is required to enter free-form comments to explain the reason for the reactivation. For more information on Provider Reactivation, see *Section 3.10.11.1.8–Changing Provider Status*.
PMNT16	The Contractor's solution shall track and support provider review schedules to ensure providers continue to meet program eligibility requirements and initiate notification(s) to the provider, agency staff, and modules of State healthcare programs agreements and contracts.	Our solution maintains a revalidation schedule for each Provider based on State and CMS defined rules and automatically generates reminder notices to Providers when revalidation due dates approach according to State defined business rules. Current configuration calls for notices to be sent 90 days, 60 days, and 30 days in advance of the program revalidation date. The revalidation workflow is identical to the new application workflow in that the operator is required to perform all review and screening activities to ensure providers continue to meet program eligibility requirements. For more information on Provider revalidation, see *Section 3.10.11.1.6–Provider Revalidation*.
PMNT17	The Contractor's solution shall accept, validate and store new and updated provider information entered by internal users.	By initiating an update workflow, internal users with the operator role have the ability to enter new and updated provider information. The solution accepts these updates as if they were made by the provider and routes the updates appropriately through the review process. For more information on maintaining Provider data through the Provider update process, see *Section 3.10.11.1.7–Provider Updates*.
PMNT18	The Contractor's solution will collect, store, maintain and display current and historical addresses by type (e.g., physical address, correspondence address and billing address) and include begin and end dates.	Our solution maintains current and historical address information for providers. This includes a primary business address, billing/pay address, correspondence address, remittance address, and other address as part of the standard implementation. For more information on capturing address information and displaying historical data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Address and Contact Information* and *Section 3.10.11.1.2–Data History*.
PMNT19	The Contractor's solution will collect, store, maintain and display current and historical Drug Enforcement Administration (DEA) number(s) including begin and end dates.	The DEA Registration page is where providers are required to supply their DEA number as well as issued and expiration dates. They are also required to upload a copy of the DEA license for verification purposes. For more information on capturing DEA data and displaying historical data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Demographic Information* and *Section 3.10.11.1.2–Data History*.
PMNT20	The Contractor's solution will collect, store, maintain and display provider business relationships (e.g., ownerships and managing entities) for use in provider screening and ongoing monitoring activities.	Our solution provides for multiple relationships between providers and other entities. This includes the relationship of an Individual provider to a group as well as relating providers to MCOs. Ownership data, including individual, organizational ownership is captured and maintained for each provider. The owner page captures information such as tax id, birth date, percentage of ownership and address information for all owners and managing employees. The federally required follow-up questions such as relationship of owners to one another or with subcontractors also appear on the owner page. Providers are able to update this information and it is viewable to all roles within the system. The solution uses the ownership information to conduct the automated screening both at initial enrollment and as part of the monthly database monitoring process. For more information on capturing owner and managing employee data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Owner Information*.
PMNT21	The Contractor's solution shall have the ability to perform mass updates to provider information using flexible selection criteria.	The MAXIMUS Provider Services solution provides a function to perform mass updates (e.g. deactivation) of providers based on State defined rules. This would be accomplished based on an ad-hoc request and a script would be written, tested, and applied according to standard procedure. For more information on mass updates, see *Section 3.10.11.1.10–Mass Updates*.
PMNT22	The Contractor's solution shall provide indicators to identify providers that are Fee-for-Service (FFS), Managed Care Organization (MCO) network only, or participating in any other healthcare programs (e.g., medical homes).	Our solution provides for multiple relationships between providers and other entities. This includes the relationship of an Individual provider to a group as well as relating providers to MCOs. The relationship feature is also how our solution indicates FFS or participation in other healthcare programs. For more information on establishing provider relationships, see *Section 3.10.11.1.1–Data Entry and Maintenance, Linking Individuals*.

ID	Maintenance Requirement	MAXIMUS Summarized Response
PMNT23	The Contractor's solution shall provide the capability to capture and crosswalk subpart NPIs used by Medicare (but not Medicaid) to facilitate COB claims processing.	Our Medicare page captures a provider's enrollment status with Medicare, including subpart NPIs. For more information on capturing Medicare data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Medicare Information*.
PMNT24	The Contractor's solution shall auto-populate fields with valid data where required.	Our solution is pre-populated with conversion data after an extensive mapping effort. Pages are pre-populated with relevant data that was entered in prior pages. For example, the W9 page is pre-populated with the Legal Business Name and SSN for individual providers. Users have the option of copying over the primary service address into other address pages to prevent duplicative data entry. For more information on the address page copy feature, see *Section 3.10.11.1.1–Data Entry and Maintenance, Address and Contact Information*.
PMNT25	The Contractor's solution shall allow internal users to add and view free-form and structure notes on or associated with individual provider files.	Internal users are able to add and view free-form notes at the individual provider application level. For more information on internal notes, see *Section 3.10.11.1.4–Provider Review*.
PMNT26	The Contractor's solution shall allow authorized internal users to link and unlink individual practitioners from and to billing providers with the ability to link an individual provider to multiple billing providers. Each relationship shall include an effective date when initiated and an end date associated with the termination of the affiliation.	Billing providers and internal users are able to link and unlink new members, end date existing members, and delete members. Individual providers can be linked to multiple billing providers. The system requires effective dates and end dates when users make the respective updates. For more information on linking individuals to billing providers, see *Section 3.10.11.1.1–Data Entry and Maintenance, Linking Individuals*.
PMNT27	The Contractor's solution shall collect, store and maintain multiple provider contacts, including the contact name, title, contact type, telephone number, email address and location.	During enrollment or revalidation, providers must supply a primary provider contact on the Primary Contact Information page. This page collects the name, title, address, phone number, phone extension, fax number, and email address for the primary contact. In addition, providers can designate other contacts based on function. For example, providers supply contact information on all the address pages for that particular function, such as correspondence, billing, or remittance. For more information on the address pages, see *Section 3.10.11.1.1–Data Entry and Maintenance, Address and Contact Information*.
PMNT28	The Contractor's solution shall have the capability to indicate providers who are suspended or under review or investigation and a method for indicating the reason for the suspension or in review status.	Using the provider search function, a user can obtain a listing of providers who were identified as potential matches with any of the screening databases during the monthly screening process. The screening page for those providers reveals the returned data from the potential database match. Free form notes indicate the reason for any providers who were suspended or terminated. For more information on Provider suspension or review, see *Section 3.10.11.1.5–Provider Screening* and *Section 3.10.11.1.8–Changing Provider Status*.
PMNT29	The Contractor's solution shall allow authorized users to enter, view and update provider data (e.g., demographic data, taxonomy, banking information).	As a role-based system, the MAXIMUS Provider Services solution restricts which users may enter, view, and update provider data. The operator role may enter and update provider data and most other roles are able to view the data. Some restrictions are built in for other agencies and what data they can view. For example, behavioral health staff cannot view non-behavioral health provider data. For more information on internal users viewing and updating Provider data, see *Section 3.10.11.1.7–Provider Updates*.
PMNT30	The Contractor's solution shall allow authorized users to retroactively update provider data.	Users with the Administrator role can update provider data, including changing effective dates to dates in the past.
PMNT31	The Contractor's solution shall store and display geographic codes for provider locations.	All address locations contain zip codes and either county indicators or quadrant and ward for addresses from the District of Columbia. The public-facing provider search function allows search based on geographic location, including city, state, and zip code. For more information on the data captured on address pages, see *Section 3.10.11.1.1–Data Entry and Maintenance, Address and Contact Information*.

ID	Maintenance Requirement	MAXIMUS Summarized Response
PMNT32	The Contractor's solution shall have configurable event based workflow to instantiate information requests, correspondence or electronic notifications throughout the provider lifecycle.	The MAXIMUS Provider Services solution employs a workflow engine that routes applications based on business-defined rules. The flexible workflow engine automatically generates correspondence (email) based on the status of the enrollment and is configured to generate correspondence based on State defined business rules. Operators use the Return to Provider workflow to initiate information requests by email to the provider. For more information on our solutions' configurable workflow, see *Section 3.10.11.1–System Workflow and Data Collection*.
PMNT34	The Contractor's solution shall have the ability to suspend the provider record for providers that fail to respond to requests (e.g., revalidation, recertification, and updated licensure) in compliance with all federal and State policies and regulations.	In the current configuration, Providers receive a notification at 60 days and again at 30 days, reminding them to navigate to the web portal to provide a new expiration date for 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 system is configured currently to send Revalidation notices at 90, 60, and 30-day intervals. If the Provider fails to take the required action within each defined timeframe, the system creates a task in the work queue for a Provider Enrollment Specialist to review the Provider file and take appropriate action. If the next appropriate action is to forward the Provider file to the DPHHS for termination, the referral will include copies of all notices and documentation of all Provider contact throughout the 90-day period. Optionally, the system can be configured to auto-terminate the Provider if they have not taken any action to revalidate within their required timeframe. For more information on Provider revalidation, see *Section 3.10.11.1.6–Provider Revalidation*.
PMNT35	The Contractor's solution shall allow for mass updates to provider status based on criteria defined by the department (e.g., group practice changes) and initiate notification to the providers and appropriate programs.	The MAXIMUS Provider Services solution provides a function to perform mass updates (e.g. deactivation) of providers based on State defined rules. This would be accomplished based on an ad-hoc request and a script would be written, tested, and applied according to standard procedure. This same script is also capable of sending notifications by email or paper to the affected providers. For more information on Mass Updates, see *Section 3.10.11.1.10–Mass Updates*.
PMNT36	The Contractor's solution shall have the ability to end date provider participation in specific programs while maintaining participation in other programs and initiate notification(s) to the provider, agency staff, and modules.	Our solution permits Administrators to end date provider participation either individually or through mass updates. Email notifications are designed and configured according to the State's requirements.
PMNT37	The Contractor's solution shall record and display multiple instances of specific provider enrollment and demographic data (e.g., license, eligibility period, physical address, CLIA levels) and provide access to historical provider record information.	Most data allow for multiple instances with history that is viewable by the user. For more information on displaying historical data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Demographic Information*.
PMNT38	The Contractor's solution shall validate email addresses associated with the provider account through a confirmation and/or activation email process that requires the user to respond to activate the email account for agency communication.	Users supply contact information at account creation. To activate the account, the system sends an email to the address provided. The email contains a link for the user to activate the account. For screenshots on this process, see *Section 3.10.11.1.1–Data Entry and Maintenance, Account Creation*.
PMNT39	The Contractor's solution shall collect and maintain provider data necessary to support other module functions (e.g. claims processing, service authorizations, and reporting functions).	The MAXIMUS Provider Services solution is currently active in other states and supports an interface to the MMIS. The interface contains the data required to establish the provider account in the MMIS, as well as any downstream functions. We can easily add data elements to our solution to accommodate any data that is not currently found in our solution to support other module functions. For more information on our solutions' data collection process, see *Section 3.10.11.1–System Workflow and Data Collection*.

ID	Maintenance Requirement	MAXIMUS Summarized Response
PMNT40	The Contractor's solution shall provide the ability to interface with external systems to automate verification and validation of provider information and credentials for enrollment, screening and monthly monitoring (e.g., CMS data matching, licensure, Social Security Administration's Death Master File, the National Plan and Provider Enumeration System (NPPES), the List of Excluded Individuals/Entities (LEIE), the Excluded Parties List System (EPLS)), and provide online alerts or notifications via workflow when adverse results or mismatches occur.	The MAXIMUS Provider Services solution provides automated interfaces with exclusion sites, including OIG LEIE, EPLS/SAM, and MED, as well as SSDMF. The system interfaces with the National Plan and Provider Enumerator System (NPPES) to verify the National Provider Identifier of provider applicants. This functionality validates provider information during enrollment, re-enrollment, and runs monthly. As part of the system Monthly Database checks process, our solution checks the Provider against the exclusion databases and the SSDMF to verify that the provider has not been added in the last month. In the event of a potential match, our solution places the registration in a configurable workflow for the operator to review the circumstances and determine if the provider should be referred to the State for termination. For more on monthly Provider Screening, see *Section 3.10.11.1.5–Provider Screening*.
PMNT41	The Contractor's solution shall require and capture termination reasons for all provider terminations.	For terminated providers, the provider information page displays the termination date and reason for the termination. This information is required to initiate the termination and send the termination transaction to the MMIS. For information on terminating providers, see *Section 3.10.11.1.8–Changing Provider Status, Terminate Provider*.
PMNT42	The Contractor's solution shall collect, process and maintain the data elements necessary to enroll trading partners with the department to support HIPAA X12 transactions.	Our system captures additional information as required for entities enrolling as Trading Partners, including the ability to select the types of X12 transactions they want to submit and receive. For more information, see *Section 3.10.11.1.3–Trading Partner Enrollment*.
PMNT43	The Contractor's solution shall provide the ability to capture and store electronic payment information e.g., (credit card, bank account).	Providers supply banking information on the ACH Authorization page. This page captures financial institution information, including routing numbers and account numbers for purposes of setting up EFT with Medicaid. Institutional providers required to pay an application fee may do so on the Application Fee page. Providers have the option to pay online or by paper check. For more information on capturing EFT data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Payment Information*.
PMNT44	The Contractor's solution shall provide the ability to display payment information (e.g., provider administrative fees).	Institutional providers required to pay an application fee may do so on the Application Fee page. Providers have the option to pay by online or by paper check. This page also supports provider's declaration that they are exempt from the fee either because they already paid to Medicare or another state, or due to hardship. This page can be configured to capture other types of administrative fees that a specific state might require. Our solution allows providers to view any of the payment types that are configured to be tracked within the system. For more information on capturing fee payment data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Demographic Information*.
PMNT45	The Contractor's solution shall provide the ability to automatically and manually unlink provider records determined to be unrelated.	Provider records can be unlinked individually or by mass update when an affiliation is no longer valid (a rendering provider no longer works at a specific clinic). When a provider's enrollment is terminated, the system also ends any affiliations with groups. For more information on linking and unlinking affiliates, see *Section 3.10.11.1.1–Date Entry and Maintenance, Linking Individuals*.
PMNT46	The Contractor's solution shall have the ability to assign classifications (e.g., provider type and specialty) to all providers including atypical providers.	During the enrollment process, all providers, including atypical providers, declare their provider type and specialty. Selections are controlled based on setting in tables so that an individual cannot select Hospital, for example. On the Specialty screen, a provider can declare more than one specialty and designate a primary specialty. Providers also supply the state from which the certification was issued, specialty Board Name and begin and end dates of the specialty. See *Section 3.10.11.1–System Maintenance and Workflow* for more information on configuration for application type, provider category and provider role.
PMNT47	The Contractor's solution shall provide the ability to collect and maintain bed data (e.g. nursing home, hospital).	Certain facility provider types are required to supply bed data on the Number of Beds page. The provider types required to supply bed data is configurable to State requirements. For more information on capturing bed data and historical data, see *Section 3.10.11.1.4–Demographic Information* and *Section 3.10.11.1.2–Data History*.

ID	Maintenance Requirement	MAXIMUS Summarized Response
PMNT48	The Contractor's solution shall provide the ability to collect conditional enrollment and maintenance data that is configurable by provider role (e.g., ORP, Rendering, Attending and Billing/Pay to Providers) and provider classification (e.g., case manager, physician, home health agency) and displays indicators on the provider record to distinguish the provider role(s) and classifications.	Our solution collects provider data and requires document uploads for enrolling providers. The specific data and document requirements vary by provider type and is configurable. For example, bed data is required for institutional providers, but not individual providers. Provider roles, such as ORP or billing providers are determined by the application type (standard, waiver, streamlined, etc.). The requirements for the application are configured so that, for example, an ORP provider is not required to provide W9 information since Medicaid does not pay them. See *Section 3.10.11.1.2–Data History* for more information on configuration for application type, provider category and provider role.
PMNT49	The Contractor's solution shall automate the identification of providers due to revalidate their enrollment information and initiate notification(s) to the provider, agency staff, and modules.	The MAXIMUS Provider Services solution maintains an end date (revalidation due date) for each provider in the system. In the current configuration, the initial revalidation notice is sent to the provider 90 days in advance of their current revalidation due date in the system. The system tracks all notices sent to providers and can generate follow up notices at predetermined intervals. If the Provider fails to take the required action within each defined timeframe, the system creates a task in the work queue for a Provider Enrollment Specialist to review the Provider file and take appropriate action. If the next appropriate action is to forward the Provider file to the DPHHS for termination, the referral will include copies of all notices and documentation of all Provider contact throughout the 90-day period. Optionally, the system can be configured to auto-terminate the Provider if they have not taken any action to revalidate within their required timeframe. If the Provider successfully completes revalidation, the system generates a written confirmation notice via email to the Provider. For more information on provider communication, see *Section 3.10.11.1.4–Provider Review, Provider Communications*.
PMNT50	The Contractor's solution shall support the ability to compare provider enrollment and revalidation information with PECOS if the provider is enrolled with Medicare. Depending on provider risk category, the solution shall verify completion of the fingerprint background check (if required), payment of application fee (if required) and verify Medicare ownership information matches the provider record in the provider module. If a mismatch is found, create an alert to the designated work group.	Our system provides automated checks against PECOS in the case where the system needs to validate participation in Medicare, if a site visit has been completed, whether a fee has been paid or if a sanction or background check has negative results. 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, including verifying completion of the fingerprint-based background check, application fee payment, Medicare owner information and site visit completion. If a mismatch is found, the file will be flagged as such and placed in an operator's queue for review. For more information on Medicare data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Medicare Information*.
PMNT52	The Contractor's solution shall collect, validate and maintain Clinical Laboratory Improvement Amendments (CLIA) certification information including the level of certification, the specific procedures each laboratory is authorized to perform, effective and end dates, and location of the certification for use in claims adjudication.	Provider types that are required to have CLIA certification must complete the CLIA Information page during enrollment. This page captures the specific services they are authorized to perform, as well as the CLIA number, certification type, and effective and expiration dates. The provider-entered data is matched against weekly refreshes on CLIA data. For more information on displaying historical data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Demographic Information* and *Section 3.10.11.1.2–Data History*.
PMNT53	The Contractor's solution shall have the ability to indicate providers using electronic funds transfer (EFT) and submitting claims electronically.	The current configuration requires all providers to receive payments electronically and to complete the ACH Authorization page. This page can be configured to be optional for all providers, with a rule that if it is completed, then the provider is agreeing to receive payment electronically. For more information on capturing EFT data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Payment Information*.

ID	Maintenance Requirement	MAXIMUS Summarized Response
PMNT54	The Contractor's solution shall support communications (e.g., email, SMS, correspondence) to and from providers, track and monitor responses to department communications.	Current functionality supports communications to the provider by email, paper mail, or interactive chat function. MAXIMUS is implementing an external Correspondence Management platform supported by the Quadient Inspire ™ Platform. This platform will enable users to create timely, contextual, personalized and accurate communications for all channels, including email and SMS text. Communications to the provider are captured on the online account and are viewable by the provider or any authorized user with access to the account. Communications from the provider are documented in internal notes or can be uploaded.
PMNT55	The Contractor shall ensure information exchanges are documented in trading partner agreements as specified in 45 CFR 162.915.	We intend to execute trading partner agreements with the applicable entities. Our system is configured to ensure compliance with the agreements per federal regulations.
PMNT56	The Contractor's solution shall have the ability to assign an individual provider an unlimited number of valid provider classifications (e.g., physician-family practice, physician-oncologist, hospital-acute care, registered nurse-pediatrics).	The MAXIMUS Provider Services solution supports a provider who has multiple provider types, specialties, and taxonomy classifications. For more information on the process of selecting an application type, provider type, specialty, and taxonomy codes, see *Section 3.10.11.1.1–Data Entry and Maintenance, Provider Key Indicators*.
PMNT57	The system shall allow a single provider to have more than one electronic submitter associated with their provider file, and designate one biller to receive 835 files	As part of our implementation of the trading partner functionality, we intend to create a relationship structure between submitters and providers. This concept will enable a many to many relationship where a provider can have more than one submitter and a submitter can submit for more than one provider. This relationship will also include the transaction types so that a provider can use different submitters to submit different transactions if necessary. We will enable functionality so that a provider can designate one biller to receive 835 files. These complex configurations will require extensive discussion during requirements review where we will create matrix of the transaction types and the relationships that are allowed for each.
PMNT58	The Contractor's solution shall have the ability to automatically and manually link the unique provider number to other provider IDs used throughout the State enterprise (e.g. SABHRS or State Eligibility Systems IDs). The solution shall display all provider IDs.	The MAXIMUS solution enables any number of provider IDs to be linked to a unique provider record. We will include this function in the same manner we track Medicare ID numbers in our solution. We will define each of the required provider identification numbers with a type and format and define whether the data is required or optional. We can then allow providers or internal workers to enter and maintain this information with supporting edits. This information can also be loaded automatically as part of the data conversion process. As we analyze eternal data requirements, we will map these fields into the external user ID by type and automatically load them during the data conversion process.
PMNT60	The Contractor's solution shall be configurable to allow users to indicate the method of how required documentation will be submitted (e.g., mail and facsimile).	The MAXIMUS Provider Services solution supports automated uploading of documents directly from the provider's computer. However, our solution also supports paper submissions, which can be mailed or faxed so that operations staff scan, index and upload the documents to the provider account. Our solution can be configured for users to indicate the method of how documentation will be submitted.
PMNT61	The Contractor's solution shall have configurable workflow to present for validation, updates submitted online/electronically by specific criteria (e.g., program type, data type, risk level).	The configurable workflow engine and user interface in our solution allow us to implement the enrollment processes to meet the requirements and policy set forth by DPHHS. Our current workflows accommodate different tasks based on program type, data type, and risk level. For example, waiver providers have a different workflow to allow for outside agency review. Moderate and high-risk providers have a separate workflow for site visit and criminal background check data capture. For more information on site visit and background check capture, see *Section 3.10.11.1.5–Provider Screening*.
PMNT62	The Contractors solution shall support manual and automatic classification of a provider risk level status (limited to moderate to high) which shall trigger additional steps and screening as applicable.	Our solution is designed to assign the appropriate risk level by provider type and is configurable to the State's policy to designate the correct risk level for each provider type. In addition, if an individual's risk level changes, a user with an administrator role can change the risk level at any time to trigger the additional screening required for the new risk level. For more information on risk level assignment, see *Section 3.10.11.1.5–Provider Screening, Assign Risk Level*.

ID	Maintenance Requirement	MAXIMUS Summarized Response
PMNT63	The Contractor's solution shall provide the capability for users to review enrollment and revalidation information prior to final submission of the enrollment or revalidated information.	The application submission process presents a message to the user when the last page is completed and the provider is ready to submit. This user-friendly message invites the provider to review the application prior to submission by clicking on the Generate PDF button. This action presents a PDF containing all data entries and gives the provider one document to review so the provider is not required to page through the entire application. For a screenshot of the PDF, see *Section 3.10.11.1.2–Data History*.
PMNT64	The Contractors solution shall support manual and automatic classification of a provider risk level status (limited to moderate to high) which shall trigger additional steps and screening as applicable.	Our solution is designed to assign the appropriate risk level by provider type and is configurable to the State's policy to designate the correct risk level for each provider type. In addition, if an individual's risk level changes, a user with an administrator role can change the risk level at any time to trigger the additional screening required for the new risk level. For more information on risk level assignment, see *Section 3.10.11.1.5–Provider Screening, Assign Risk Level*.
PMNT65	The Contractor's solution shall capture and maintain at a minimum, the data set defined in Part 11 of the State Medicaid Manual and provider related TMSIS required fields.	The MAXIMUS Provider Services solution is currently active in other states and supports an interface to the MMIS. The interface contains the data required to fort he State to complete its MMIS TMSIS reporting. We can easily add data elements to our solution to accommodate any data that is not currently found in our solution. For more information on capturing and maintaining data, see *Section 3.10.11.1.1–Data Entry and Maintenance* and *Section 3.10.11.1.2–Data History*
PMNT66	The Contractor shall collect and maintain certifications by specific industry standard or state policy (e.g., NCQA Certification and NCQA Certification Level).	Our solution captures many provider certifications, including those for specialties, CLIA, CPR, state controlled substance registration. We can add screens or other certifications to support additional industry standards or state policy certification requirements. For more information on capturing and maintaining accreditation data, see *Section 3.10.11.1.1–Data Entry and Maintenance, Demographic Information* and *Section 3.10.11.1.2–Data History*.

3.10.12 Self-Service Portal

3.10.12 Self-Service Portal

This section addresses self-service portal requirements. The Provider Services module must support self-service provider enrollment and maintenance activities in addition to other self-service functions necessary to support day to day business functions including but not limited to; a provider inbox, interactive chat functionality, and a provider locator for both public and authenticated users to find actively enrolled providers based on specified criteria. The Offeror must describe their approach to meet each of the Self-Service Portal requirements defined in Attachment F, Requirements Matrix.

MAXIMUS will implement our secure Provider Services solution to provide general screening and enrollment information using modern functionality through a web-based user interface, web portal, and enhanced electronic messaging tools. We deploy the Provider web portal to facilitate effective online communication with Providers in support of the Provider screening and enrollment process. The system's web portal gives Providers an intuitive and easy-to-use site where they can fill out and submit applications and upload required verification documents electronically. The portal supports the Providers with access to their communications inbox and helps them through the registration process by giving them the ability to receive guidance through our interactive chat functionality.

Since our initial implementation of the web portal in Tennessee, we have continued to augment and improve the user interface based on feedback from Tennessee Provider services staff as well as the Provider community themselves. Beginning with our initial implementation, Providers immediately began to gravitate to the web portal to submit their electronic applications and revalidations. The Provider community were pleased with the faster process for 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 and straightforward for providers to use.

Underneath the intuitive and easy to use web portal, our solution also yields a technical system and platform for managing workflows that support assigning, routing, and monitoring tasks and gives 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. In the remainder of this section, we provide 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.

3.10.12.1 Provider Search (Public)

MAXIMUS Provider Services solution Search functionality, combined with the drill down capabilities of the system dashboards provide an easy-to-use, comprehensive view of the State's complete Provider community.

The MAXIMUS Provider Services 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 DPHHS. The search functions offer a variety of search parameters all of which are configurable to meet any unique requirements of the Department. Our intuitive search function provides search results for the entire Provider profile including Provider demographics, location(s), affiliations, networks, contracts, credentialing, communications, a practice profile, and a quality summary.

Our solution is designed to be the system of record for all Provider data in each State where we implement. The system offers an intuitive, wizard guided data entry process for Providers via the web portal, whether they are newly enrolling or are revalidating their existing Provider profile. Additionally, our solution's Open Interface Framework allows us to import external Provider data from any source, including State MCOs and Credentialing agencies. For example, in our Tennessee implementation, the majority of the individual Provider's data comes from the CAQH credentialing repository via an interface with CAQH. 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. End users and information consumers need not be experts in Provider management to find and use the Provider data. Our Online Provider Directory is updated in real-time and presents a variety of view options for information consumers. Through use of the business rules engine and the flexible queries that support our search functions, the search capabilities of our system are easily configurable to meet the needs of the Department and the State's broader health care community. All search screens and search results screen adhere to ADA compliance specifications and usability requirements.

Public Search – GIS

Exhibit 3.10.12-1: Public Provider Search – GIS provides one example of the public search functionality available in our solution. This search function is available to all users (the user does not need to have an account to perform this search). This search function is primary geared toward eligible recipients to search for active Providers in a certain geographic region but is also useful for displaying the concentration (or lack there-of) of Providers in a certain geographic region.

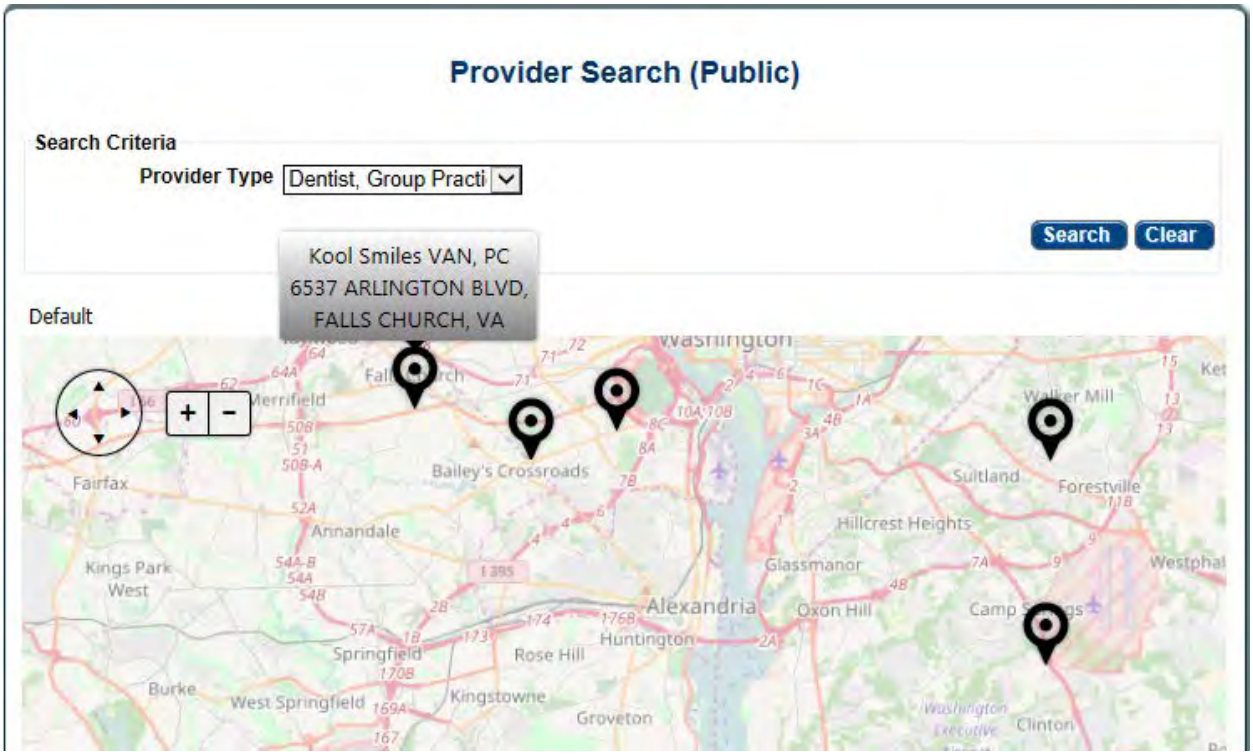


Exhibit 3.10.12-1: Public Provider Search – GIS. *Our solution offers any user the ability to search and view Providers based in a geographic region of the State, based on Provider type.*

The system is capable of supporting the GIS searches through use of our integration 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.

Public Search – Active Providers Advanced Search

In addition to the GIS search, our system also provides an advanced search for the public to search for Providers based on Provider Type, Specialty, Name, City, State, and Zip code. *Exhibit 3.10.12-2: Active Providers Advanced Search* shows the types of search parameters that can be used to find certain Providers in the State's Medicaid program.

CONFIDENTIAL

The name search capabilities on this search screen allow users to filter the search results by indicating if the Provider's name equals (exact match), begins with, ends with, or contains a certain set of characters. Users can view further details about the Provider by clicking on the Provider's name. The search function allows the user to edit the search criteria from the Provider look-up results page.

As shown in the screen shot above, users can sort the retrieval results based on any category of data displayed on the search results grid. Information displayed on the search results and on the Provider detail screen use standard terminology and standard Provider related data fields. On all search results screens in our solution, users are able to export all search results in PDF or excel.

The system also uses Google Maps to provide the user the ability to obtain directions to the Provider's location, as shown in *Exhibit 3.10.12-3: Provider Directions using Google Maps.*

CONFIDENTIAL

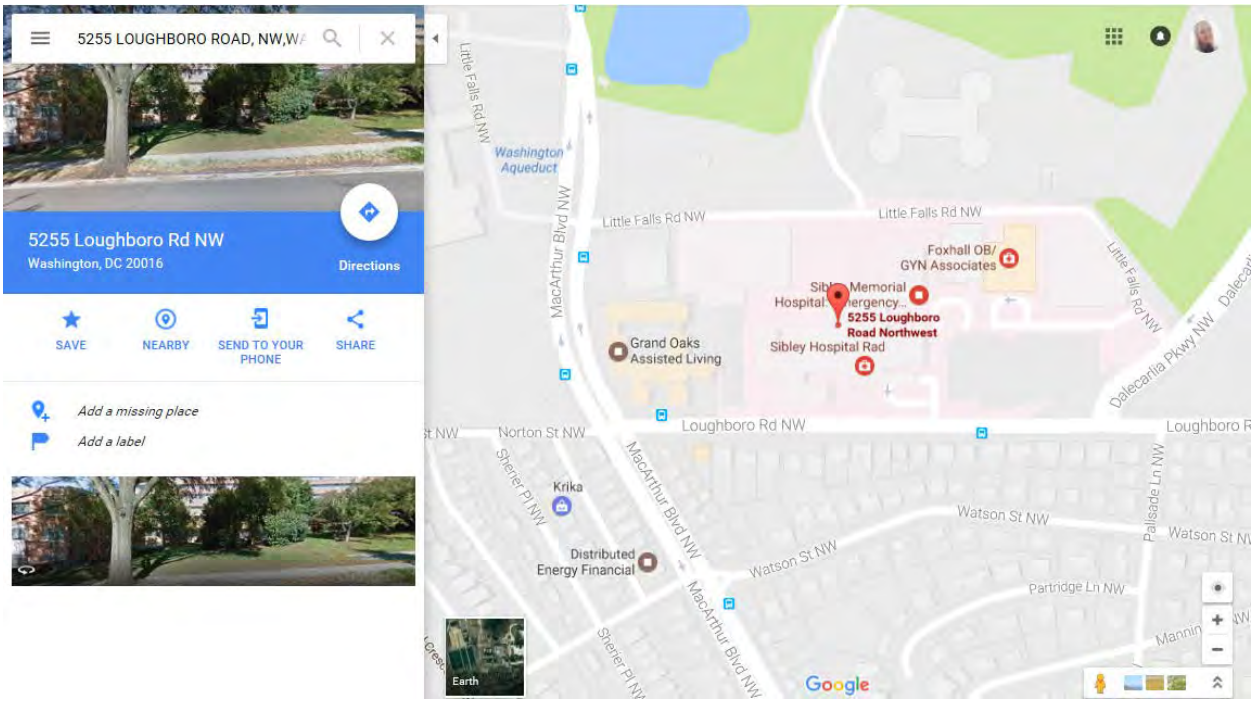


Exhibit 3.10.12-3: Provider Directions using Google Maps. *Our solution uses Provider Enrollment Master File to track all active Providers and allows public users to search and find directions for Providers at specific locations.*

For the Montana Provider Services module implementation, MAXIMUS will augment both our public and internal search capabilities to allow search criteria on the various types of programs that the Provider may be active and add any other additional fields that may be required.

3.10.12.2 Provider Search (Internal Users)

Our solution provides the functionality to allow a Provider to submit multiple application types and tracks the outcome of each submitted application. The system is packaged with a robust search function, a system dashboard that allows drilldown capabilities, and numerous on demand reports. *Exhibit 3.10.12-4: Provider Search* illustrates the types of search options an authorized user has on-demand for finding a Provider in the system. These search and reporting capabilities allow users to search applications and trace the system and user actions that have been taken for each Provider submitted application.

CONFIDENTIAL

As shown in the above Exhibit, users are able to select from a multitude of search parameters. Once the search results are displayed, the user has the ability to export the results into an Excel or PDF file. Users can click on the 'Review' button to review the provider's entire enrollment profile and history. We will configure this search screen to expand the types of search parameters as required by the State.

3.10.12.3 User Account Setup – Provider Self-Service

To submit and update enrollment applications online via the Provider Services web portal, providers (or credentialing agents enrolling on behalf of the Provider) must first establish an account on the portal. *Exhibit 3.10.12-5: Initial Provider Web Registration* shows the initial screen a provider/credentialing agent will use to set up an account.

CONFIDENTIAL

CONFIDENTIAL

In our current Provider Services configuration, the key identifier given to establish the account is the Tax ID of the Provider. This could be the SSN or an Individual Provider or the EIN of an organization/entity. If there are no Providers existing in the system that currently use that Tax ID, the user is able to proceed forward in the account setup process without having to enter any additional demographic information for the Provider. If at least one Provider does exist (this could be either a converted Provider from the MMIS or a newly added Provider), then the user is required to add additional information that uniquely identifies a Provider using that Tax ID at a specific practice location. We configure the system this way to make sure that the registering user has sufficient information about that Provider to be authorized to take actions to update or revalidate the Provider.

Once the user gets past this screen, the remaining account set-up process is a simple two-step procedure to gather the user account information for the user. The system then sends an email confirmation to the user where they can click a link and active their account in the system. The initially established user account for the Tax ID becomes the Admin user for the Provider account. When the newly authorized user logins to the system using their account credentials, they are then taken to the Provider homepage. *Exhibit 3.10.12-6: Provider Homepage* shows the information the user will see after successful login.

CONFIDENTIAL

CONFIDENTIAL

As shown in the screenshot in *Exhibit 3.10.12-6* the Provider user is able to view existing Providers in the system that use the Tax ID associated with the account. In some cases, this could result in multiple providers being displayed in the My Providers grid. The user also has available to them other self-service options including the ability to update their account profile, select an existing Provider for update, or begin a new enrollment for a new Provider. The Admin user for the Provider account also has the ability to add or remove provider account users and change user roles for all self-service functions.
Exhibit 3.10.12-7: Maintain User Accounts shows how the Admin user can add new users to the account and define the security access for each added user.

CONFIDENTIAL

An example of the flexibility that this function provides is shown in the screenshot above. The HeartlandAdmin* user is the user admin for the Provider account. This user can create new user accounts and modify existing accounts. In the example shown, the user role ‘g3475snf’ has been created and granted access to only view Documents and Reports. The Documents and Reports in this definition are the ability for that user to only view EDI transactions and eRAs for the Provider. This user will not have the ability to view or update any of the other data in the Provider’s enrollment profile. We implemented this functionality in our Tennessee Provider Services project and will bring this functionality to our solution for Montana.

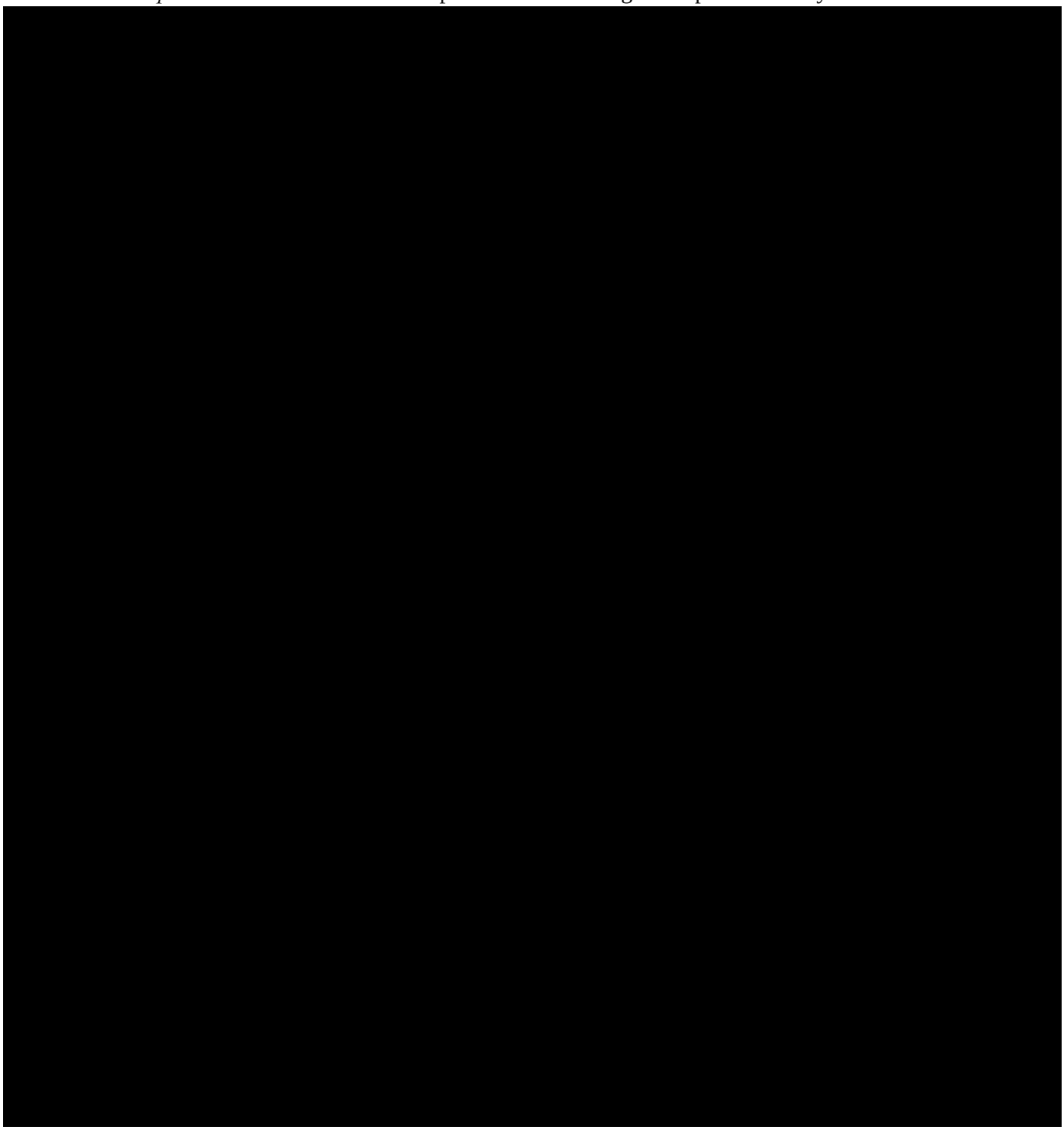
3.10.12.4 Self-Service Update for an Existing Provider

Our solution provides self-service functionality to allow existing providers (both active and inactive) to perform updates through the web portal. Each submitted update by the provider is tracked via a new workflow that is established for the update or revalidation. The system validates and stores the new

CONFIDENTIAL

information for the Provider in the system, and forwards the update on to the Enrollment Specialist for internal review and approval, when required.

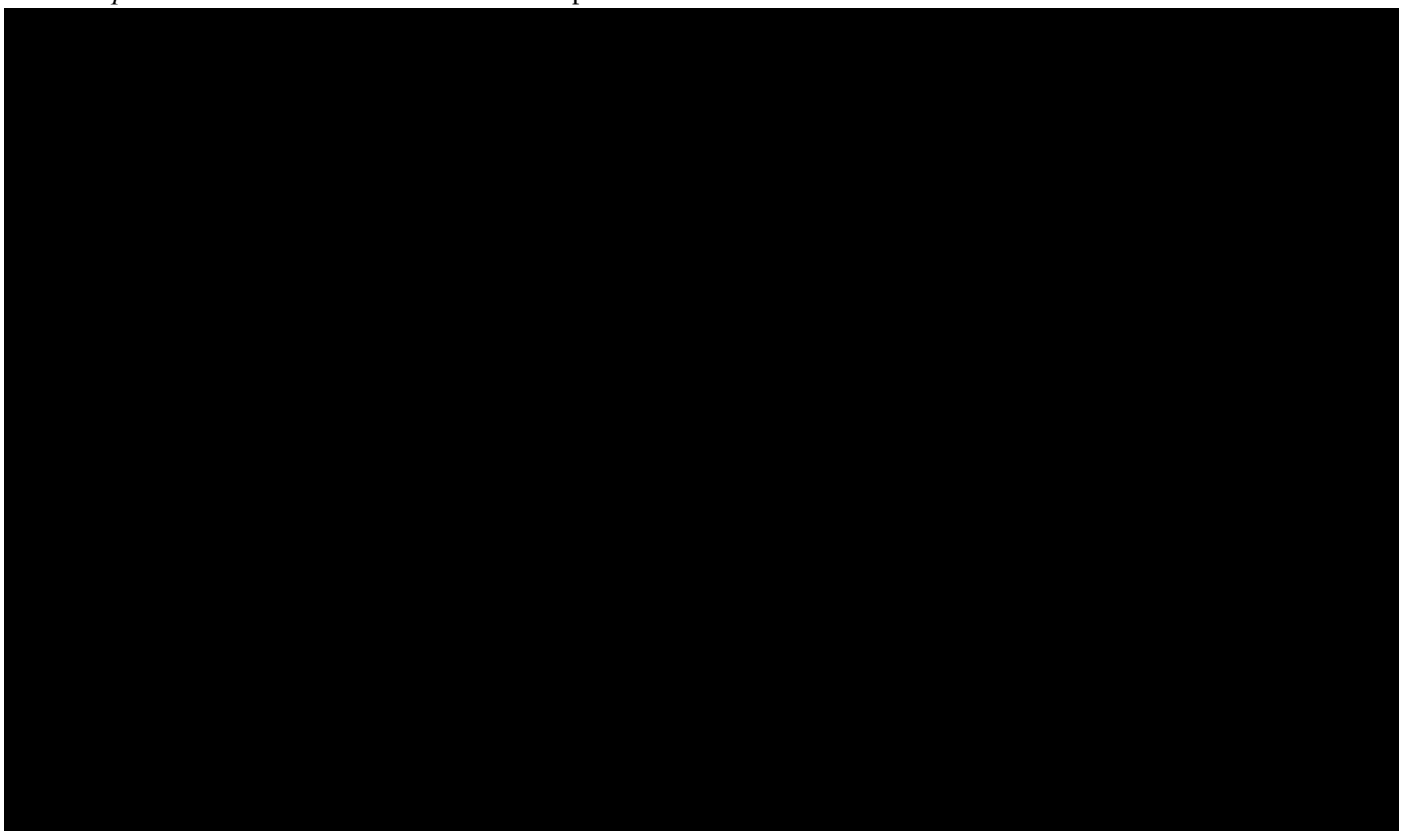
In the previous section, we provided details on the steps a Provider takes to establish a user account and navigate to the Provider Homepage. We will continue with that example in this section to provide examples of how Providers can submit self-service updates via the web portal. *Exhibit 3.10.12-8: Initiate Provider Update* illustrates the action the provider takes to begin an update in the system.



CONFIDENTIAL

CONFIDENTIAL

From this screen, the Provider is able select from the list of data categories that are relevant for their Provider Type. The list of most often submitted updates are displayed at the top of the screen. This is configurable and we can add or remove screens from this list as required by the State. For this example let's assume the Provider chooses to select the Affiliations screen for update. Once the Provider selects the Affiliations for update, the system takes the Provider to the Individual Affiliations screen where they can add or update Individual practitioners within their practice. *Exhibit 3.10.12-10: Individual Affiliations Update* shows the screen for affiliation updates.

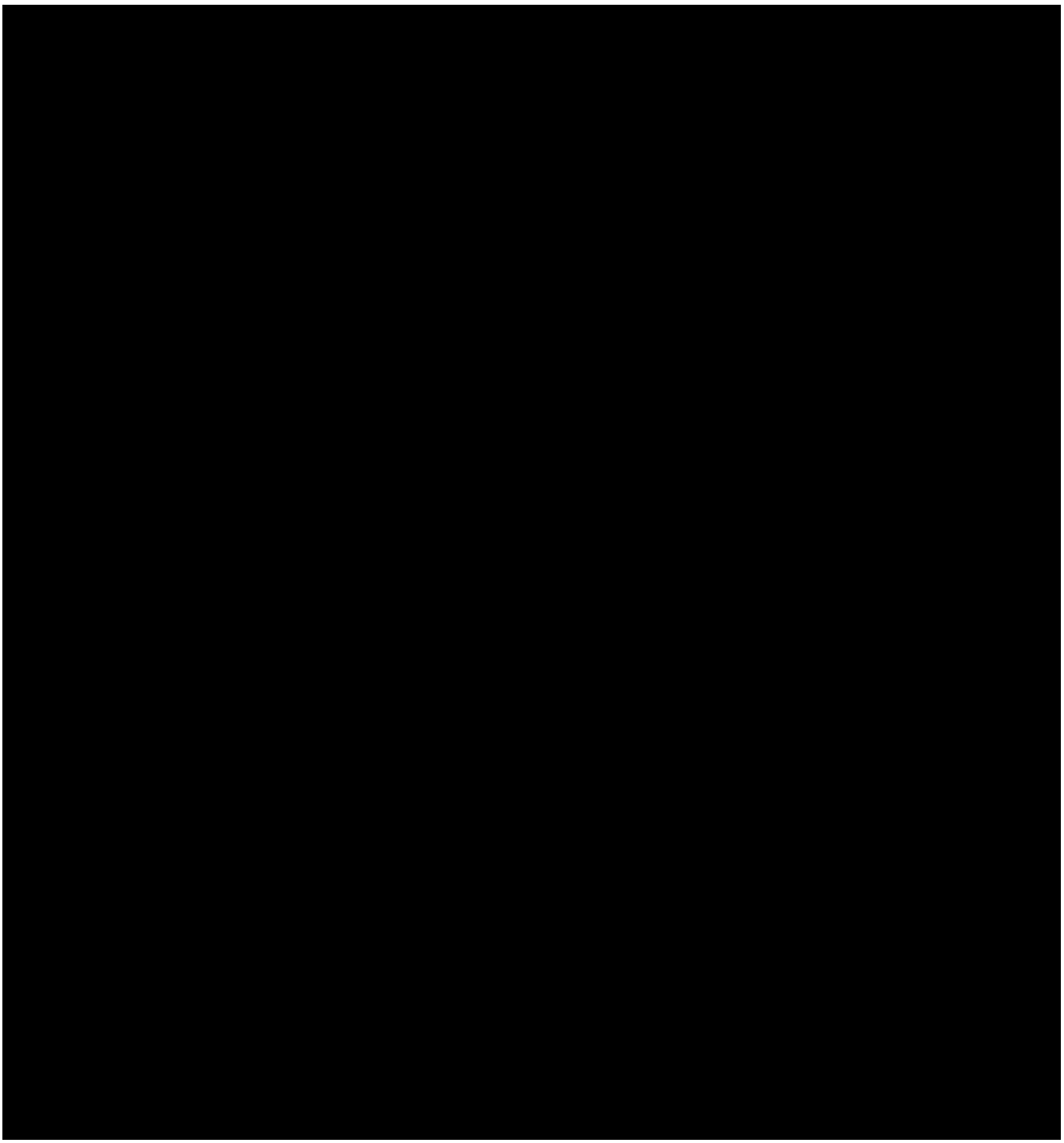


Once on the screen, the Provider can make updates or return to the Update Summary screen. The provider is able to submit the updates from this screen or from the Update Summary screen. The number displayed at the bottom left of the screen is the system assigned tracking number for this workflow for the Provider, referred to as the Provider's Registration ID. This ID is viewable by the Provider and relates to the workflow that the provider is currently in. Once the Provider has taken the action to submit the update, the system accepts the data as current within the system.

3.10.12.5 User Account Setup – Internal Functions & Users

Internal users are assigned an account with defined user role. Our flexible role-based security model accommodates different types of configuration for teams and partner access to the system. Our solution is packaged with a set of pre-defined roles. These pre-defined roles are the core internal users of the system and generally their privileges do not vary from state-to-state. *Exhibit 3.10.12-11: User Roles* lists the basic user roles packaged with our Provider Services solution.

CONFIDENTIAL



Security roles are based on business function and necessary access to information. Individual Providers can only access their own information, while operation staff have broader access to information based on their position requirements. The administrator role has broader access across multiple functional areas, including security administration. MAXIMUS will verify the roles that are needed for State authorized staff, Providers, and Trading Partners during the onset of the MPATH project. We recognize the need to create a new role for Trading Partners, which will largely be patterned after the Provider user role.

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

3.10.12.6 Viewing Messages

Our solution provides self-service capabilities for Providers to view and respond to requests received by internal users, most typically requests that are sent by Enrollment Specialists. The system also maintains a viewable list of all email notifications sent the Provider (the Provider's 'inbox'). By using our system's Chat functionality (discussed further in *Section 3.10.12.4–Online Chat*) Providers also have the capability to initiate a dialogue with internal users (Enrollment Specialists and CSRs) to assist them in completing their enrollment, revalidation, or update.

In *Section 3.10.10.5–Enrollment Review* we provided an overview of the system's Return to Provider functionality, mostly from the perspective of the Enrollment Specialist identifying the need to request additional or corrected information from the Provider to submit a complete enrollment. In this section, we discuss the Return to Provider function more from the Provider's perspective which will demonstrate how our solution effectively allows Providers to respond to messages or notifications sent by internal users. *Exhibit 3.10.12-12: Return to Provider* provides an example of an email that was automatically sent to the Provider based on an enrollment review conducted by an internal user.

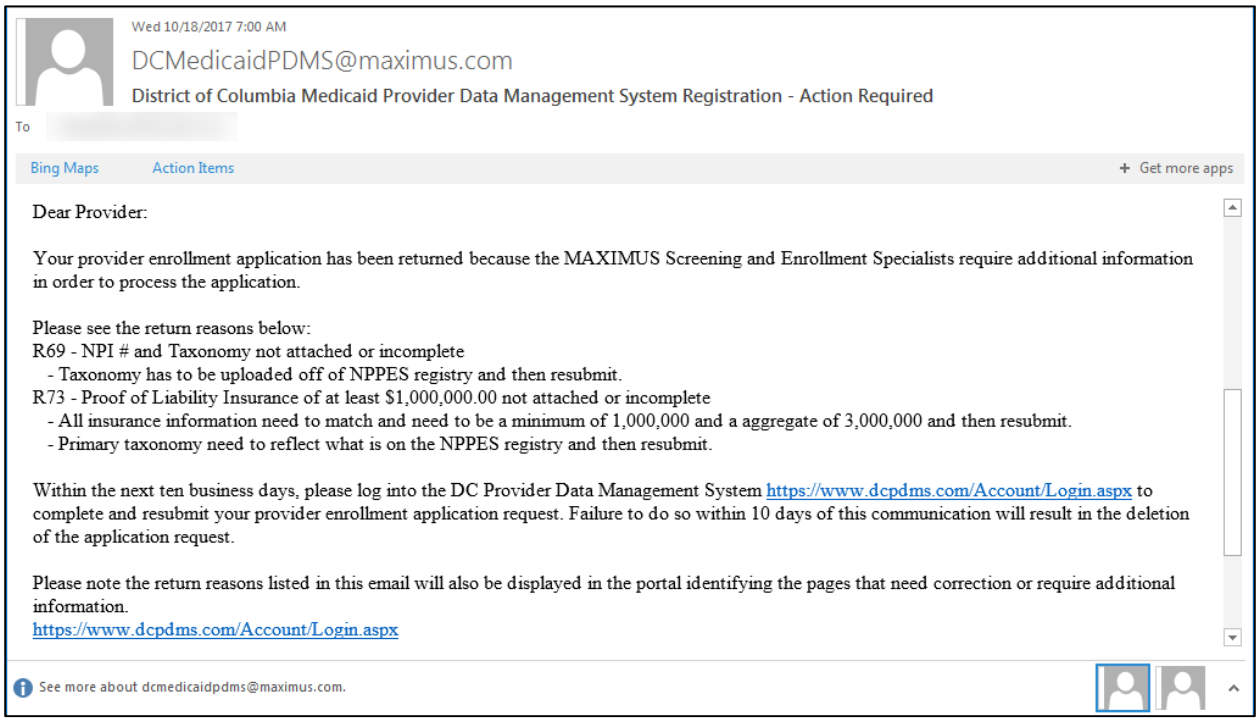


Exhibit 3.10.12-12: Return to Provider. *During the application review process, Provider Enrollment Specialists are able to review each section of the electronic application and take the action to "Return to Provider" if an issue exists with the application.*

CONFIDENTIAL

The email notification sent to the Provider contains the details of the types of actions they need to take on their enrollment to respond to the Enrollment Specialist's request. The provider is able to view this communication (and all communications) by visiting their homepage. *Exhibit 3.10.12-13: Provider Inbox* shows the portion of the Provider homepage where the Provider can view all communications sent to them by the system.

In addition to the directions given to the Provider in the Return to Provider email notification, our solution also provides a sophisticated function that navigates the Provider directly to the screen(s) where they need to take the action to correct their enrollment. *Exhibit 3.10.12-14: Update Enrollment* provides an example of where the provider would be taken if they were to click on the 'Continue Registration' link on their homepage in the case where their enrollment application had been returned by the Enrollment Specialist.

CONFIDENTIAL

CONFIDENTIAL

As seen on the screenshot in above Exhibit, the Provider is also able to view the reasons and actions that need to be taken on the screen to correct the enrollment. These are the same text that the Provider sees in the email communication, displayed on the screen for convenience to further assist the Provider in making the required updates to their enrollment. The provider is then able to make the necessary enrollment updates and resubmit their enrollment to the Enrollment Specialist.

In addition to the extensive online capabilities of the web portal, enrolled Providers and authenticated users also have convenient access to online web chat assistance. We successfully implemented web chat as a service access channel in our District of Columbia Provider Services implementation. The web chat functionality for our District of Columbia implementation is demonstrated in the screenshot in *Exhibit 3.10.12-14: Update Enrollment*. If the State chooses to procure our proposed Option B Services, trained MAXIMUS CSRs will be on the receiving end of Provider initiated chat sessions, otherwise this function will be supported by staff from the State's incumbent vendor. For our Montana Provider Services implementation we intend to use the MedChat product. MedChat is designed for a streamlined user experience, and exclusively for healthcare. Integrating our Provider Services application with third-party COTS products has proven to be a relatively simple task given the flexibility of our system architecture and open framework. MedChat provides the functionality to record/store all sessions and the sessions are available to internal staff for reference. To provide a frame of reference for the State, currently in our District of Columbia implementation we average between 45 and 55 chat sessions per week. The chat sessions are tracked and the weekly tally is provided in the Weekly Status report.

CONFIDENTIAL

In summary, our solution contains a communications framework that allows us to create and configure the content of any system generated e-mail or message based on business rules, workflow items and events that occur within the system. Our solution 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 messages 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. All notifications automatically sent to Providers through the system are retained and the Provider is able to view all communications from their homepage.

3.10.12.7 Linking Individuals to Billing Providers

The MAXIMUS Provider Services solution provides robust functionality that allows for the establishment and tracking of Individual Providers that are affiliated with Billing Providers. Both the Individual and Billing Providers are able to update their enrollment profile to create affiliations to each other. In our experience, different States have different rules for how an Individual ultimately becomes confirmed as a rendering provider within a Group (Billing Provider). The eventual configuration for the State is largely driven by what the MMIS requires regarding the data requirements for establishing the affiliation. Because of the varying requirements in each State, and based on our experience, we have spent a great deal of time and effort in establishing a flexible framework to accommodate the different affiliation business rules for each State.

In the current configuration of our Provider Services solution in the District of Columbia, Individual Providers see a screen during their enrollment workflow where they are able to enter the information for each of the Billing Providers they intend to become affiliated with. On this same screen, the Individual is also able to view all of their confirmed affiliations with existing Billing Providers. *Exhibit 3.10.12-15: Group and Facility Affiliations* shows a snippet of the screen an Individual Provider sees during their enrollment process.

CONFIDENTIAL

In the Pending Group Affiliations section of the screen, the Individual Provider is able to add one or many Billing Providers with whom they intend to affiliate. The Individual can also view their current, confirmed affiliations with other Billing Providers in the Confirmed Group Affiliations section of the screen. While the Individual Providers can provide this information in their enrollment, in the current District of Columbia configuration the rule is that the Billing Provider must still confirm the Individual within their practice before the Individual becomes a confirmed member.

Billing Providers view a slightly different version of this screen during their enrollment process. *Exhibit 3.10.12-16: Individual Providers Associated with Your Group* illustrates a snippet of the screen that Billing Providers see during their enrollment and update process.

CONFIDENTIAL

CONFIDENTIAL

Using this screen, Billing Providers are able to take several actions for adding and maintaining their Individual members. Billing Providers are able to add new members, end date existing members, and delete members (only if the Individual has not yet been sent to the MMIS). The system assigns an affiliation status to the Individual Provider based on the current enrollment status of the Individual. The system automatically changes these statuses as circumstances change for both the Group and the Individual during their respective enrollment/update processes.

Billing Providers in all of our State implementations are amazed by the efficiency of the process as compared to the paper enrollment process. Billing Providers can confirm Individual members in an expedited manner as all of the paperwork is eliminated in the electronic enrollment process. The system workflow automatically triggers actions to advance the confirmation of the Individual through to completion and sends the confirmed affiliation to the MMIS.

CONFIDENTIAL

CONFIDENTIAL

Other business rules currently enforced in our current configuration relate to the NPIs that must be entered for both the Individual and the Group. Group Providers must enroll using a Type 2 NPI (Organization) and Individual Providers must enroll using 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.

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

3.10.12.8 Website Resources and Online Help Features

The Provider Services self-service web portal provides easily accessible links to users for training materials and other relevant web resources, including State sites as required. The Provider Education & Training Resources page organizes static web content by communications, training materials and links to other websites. The website provides a Contact Us link where we provide contact information for the call center and any other required contacts as communicated by the State. *Exhibit 3.10.12-17: Website Resource Links* shows the current District of Columbia configuration for this type of information on the portal.

3.10.12.9 Self-Service Portal Requirements

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

CONFIDENTIAL

ID	Self-Service Portal Requirement	MAXIMUS Summarized Response
PSER01	The Contractor's solution shall provide a self-service tool that will allow authenticated users to search by provider name (including phonetic search), NPI/API, network(s), location(s) (including city, state and zip code), provider classification(s), provider role, all languages spoken/language accommodations (e.g., English, Spanish, American Sign Language (ASL)), accessibility, gender, and whether or not a provider is accepting new patients. At a minimum the results display shall include; provider name, locations, phone numbers, provider classification(s), provider role, network(s), all languages spoken/language accommodations (e.g., English, Spanish, American Sign Language (ASL)), office hours, accessibility, whether or not a provider is accepting new patients, and any restrictions on the freedom of choice among providers in the public provider locator (e.g., ages served, gender).	Our system is packaged with a robust search function, a system dashboard that allows drilldown capabilities, and numerous on demand reports. Authorized users of the system, which will include State Staff, Fiscal Agent staff, and MAXIMUS administrators, will have access to the internal search function. These search and reporting capabilities allow users to search applications and trace the system and user actions that have been taken for each Provider submitted application. MAXIMUS will extend the capabilities of the internal search function to allow for the additional search parameters specified in this requirement. Refer to *Section 3.10.12.2–Provider Search (Internal Users)* for further details on this functionality.
PSER08	The Contractor's solution shall provide an online self-service tool for providers to access a provider inbox for messages and notices. The solution shall provide the ability to send, receive, and respond to messages.	Our solution provides self-service capabilities for Providers to view and respond to requests received by internal users, most typically requests that are sent from Enrollment Specialists. The system also maintains a viewable list of all email notifications sent the Provider (the Provider's 'inbox'). Refer to *Section 3.10.12.6–Viewing Messages* for further details on this functionality.
PSER09	The Contractor's solution shall provide an online self-service tool for providers to add or remove provider account users and change user roles for all self-service functions.	To submit and update enrollment applications online via the Provider Services web portal, providers (or credentialing agents enrolling on behalf of the Provider) use a self-service web portal function to establish an account on the portal. In our current Provider Services configuration, the key identifier given to establish the account is the Tax ID of the Provider. This could be the SSN or an Individual Provider or the EIN of an organization/entity. Refer to *Section 3.10.12.3–User Account Setup – Provider Self Service* for further details on our approach for this requirement
PSER10	The Contractor's solution shall allow individual practitioners to submit a request to link or unlink an affiliation with a billing provider. Each relationship shall include an effective date when initiated and an end date when the affiliation is terminated.	In our Provider Services solution implementation in the District of Columbia, Individual Providers see a screen during their enrollment workflow where they are able to enter the information for each of the Billing Providers they intend to become affiliated with. On this same screen, the Individual is also able to view all of their confirmed affiliations with existing Billing Providers. We will bring this same functionality to the Department and configure the solution to meet any unique Department needs. Refer to the *Section 3.10.12.7–Linking Individuals to Billing Providers* for more detail on this process.
PSER11	The Contractor's solution shall accept, validate and store new and updated provider information entered through the Provider Self Service tool.	The system validates and stores the new information for the Provider in the system, and forwards the update on to the Enrollment Specialist for internal review and approval, when required. Refer to *Section 3.10.12.4–Self Service Update for an Existing Provider* for further details on this system function.

ID	Self-Service Portal Requirement	MAXIMUS Summarized Response
PSER12	The Contractor's solution shall allow authorized billing providers to link and unlink individual practitioners from and to billing providers with the ability to link an individual provider to multiple billing providers. Each relationship shall include an effective date when initiated and an end date associated with the termination of the affiliation.	The MAXIMUS Provider Services solution provides robust functionality that allows for the establishment and tracking of Individual Providers that are affiliated with Billing Providers. Both the individual and Billing Providers are able to update their enrollment profile to create affiliations to each other. We have found that different States have different rules for how an Individual ultimately becomes confirmed as a rendering provider within a Group (Billing Provider). The eventual configuration for the State is largely driven by what the MMIS requires regarding the data requirements for establishing the affiliation. Because of the varying requirements in each State, and based on our experience, we have spent a great deal of time and effort in establishing a flexible framework to accommodate the different methods for each State. For further details on our proposed approach to meet this requirement, refer to *Section 3.10.12.7–Linking Individuals to Billing Providers*.
PSER15	The Contractor's solution shall provide online interactive chat functionality as a reliable transaction channel that allows enrolled and authenticated users to chat directly with a customer care representative. The chat session shall be recorded, stored, and accessible to internal staff for reference.	In addition to the extensive online capabilities of the web portal, our solution provides enrolled Providers and authenticated users with convenient access to online web chat assistance. Using Medchat, Providers have the capability to initiate a dialogue with internal users (Enrollment Specialists and CSRs) to assist them in completing their enrollment, revalidation, or update. Refer to *Section 3.10.12.6–Viewing Messages* for further details on how we will implement the chat functionality for the State.
PSER16	The Contractor's solution shall include a configurable self service tool that allows active and inactive providers to update and validate their provider record through direct data entry via the web, based on selected criteria.	Our solution provides self-service functionality to allow existing providers (both active and inactive) to perform updates through the web portal. Refer to *Section 3.10.12.4–Self Service Update for an Existing Provider* for further details on this system function.
PSER17	The Contractor's solution shall a provide public provider search feature that will allow users to search by provider name (including phonetic search), network, location(s) (including city, state and zip code), provider classification(s), all languages spoken/language accommodations (e.g., English, Spanish, American Sign Language (ASL)), accessibility, gender, and whether or not a provider is accepting new patients. At a minimum the results display shall include; provider name, network(s) location(s), phone numbers, provider classifications, all languages spoken/language accommodations (e.g., English, Spanish, American Sign Language (ASL)), office hours, accessibility, whether or not a provider is accepting new patients, and any restrictions on the freedom of choice among providers in the public provider locator (e.g., ages served, gender).	The MAXIMUS Provider Services solution is packaged with robust search functionality and provides a public facing search function that is accessible by any user accessing the web portal. Users do not need to establish an account in the system to perform the public web search. MAXIMUS will extend the capabilities of the publicly available search function to allow for the additional search parameters specified in this requirement. We can also extend the search results to display as much Provider information as is available in the system, or as specified by DPHHS. Refer to *Section 3.10.12.– Provider Search (Public)* for further details on how our solution meets this requirement.
PSER22	The Contractor's solution shall provide online key contact information at a minimum by program type and business process.	Our solution provides key contact information via a link on the web portal. The contact information can be based on program type and/or business process. Refer to *Section 3.10.12.8–Web Resources and Online Help Features* for additional details.
PSER23	The Contractor's solution shall provide an online self-service Frequently Asked Questions (FAQ) tool that is easily navigable and searchable. The FAQ shall be updated quarterly or as directed by the State.	This requirement is identified in Appendix F as an Option A Services requirement. Please refer to *Section 3.10.13.9–Self-Service Portal – Option A Services* for further details on our approach for meeting this requirement.
PSER24	The Contractor's solution shall allow users to view, download and/or print current and historical provider information (e.g., manuals, instructions, bulletins, program descriptions, eligibility criteria and forms).	This requirement is identified in Appendix F as an Option A Services requirement. Please refer to *Section 3.10.13.9–Self-Service Portal – Option A Services* for further details on our approach for meeting this requirement.

ID	Self-Service Portal Requirement	MAXIMUS Summarized Response
PSER25	The Contractor's solution shall provide links to relevant web resources (e.g., State and Federal websites, and other entities determined by the State to be appropriate for the self-service portal).	The Provider Services self-service web portal provides easily accessible links to users for training materials and other relevant web resources, including State sites as required. Refer to *Section 3.10.12.8–Website Resources and Online Help Features* for examples of how we implement this functionality.
PSER26	The Contractor's solution shall allow enrolled providers, enrolled trading partners, State users, and other users designated by the State, access to the secure areas of the self-service portal following successful authentication through single sign-on.	Users are assigned an account with defined user role. Our flexible role-based security model accommodates different types of configuration for teams and partner access to the system. Our solution is packaged with a set of pre-defined roles. These pre-defined roles are the core internal users of the system and generally their privileges do not vary from State-to-State. Refer to *Section 3.10.12.3–User Account Setup – Internal Functions* for further details on this process.
PSER27	The Contractor's solution shall provide access for users to view current and historical fee schedules.	This requirement is identified in Appendix F as an Option A Services requirement. Please refer to *Section 3.10.13.9–Self-Service Portal – Option A Services* for further details on our approach for meeting this requirement.
PSER28	The Contractors solution shall create and present a tracking or confirmation number when provider information is updated via the self-service portal.	The system assigns a Registration Number which is the system assigned tracking number for the workflow for the Provider. This ID is viewable by the Provider and relates to the workflow that the provider is currently in. Refer to *Section 3.10.12.4–Self-Service Update for an Existing Provider* for further details.

3.10.13 Option A Provider Services

> 3.10.13 Option A Provider Services
>
> In addition to the primary scope of the Provider Services module, states may procure additional provider self-service portal components and services for activities not categorized in Section 3.10.1 through 3.10.12. These services are integral to the provider's ability to complete necessary activities in order to participate in one or more of State healthcare programs. Option A Provider Services requirements provide flexibility to State's or Agencies who may desire to procure the components or services outlined in Option A as a part of this procurement versus a separate procurement. The Offeror is not required to include Option A in their proposal. If the Offeror chooses to include these services in their proposal the Offeror must describe in their response, their approach to meet the Option A requirements detailed Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution is designed and built around provider requirements with an easy-to-use, intuitive interface and web enabled access for all functions. The MAXIMUS Provider Services solution is built on a technology platform that is SOA-based Open interface framework and supports ESB communications and technology to support modern functions, including mobile technology. By connecting with other systems and data partners within the Medicaid Enterprise, we are able to support a provider web portal that includes self-service options for all aspects of the provider interaction with the Medicaid Program. As part of our Tennessee Provider module, we have successfully integrated many of the functions and transactions required for the additional provider self-service portal requirements included in Option A and we plan to leverage our experience and system functions for Montana.

MAXIMUS is including Option A services in our proposal. We understand that many states may procure these additional provider self-service portal components and services to support a single integrated provider platform across the Medicaid Enterprise. We believe the best approach for these functions is to include the as an integrated component of our base implementation. This approach maximizes the staff and project infrastructure already mobilized for the base system and reduces overall risk because we are able to do testing on all functions of the provider self-service portal one time. It also reduces the impact to

CONFIDENTIAL

providers of having to learn multiple system releases and transitions all functions to the new system immediately.

We show this as an additional development track that follows the configuration of the provider self-service portal. At the conclusion of the Option A track, all provider self-service functions for both the base and Option A will be finished to enable consolidate system and integration testing. *Exhibit 3.10.13-1: Option A Implementation Schedule* shows our integrated plan for including Option A functions and services into the base system implementation plan.

MAXIMUS understands that the Option A functions might need to wait until a SOA-based system integration is in place or even an update of the existing EDI platform to support CORE compliance. We are flexible in implementing these functions based on the availability of other systems within a state to support these services. If a state wanted to wait until the M&O period to initiate the Option A functions, MAXIMUS would support this approach by externalizing the components of the development track and integrate them into an M&O release. We would work with the state and its system partners to develop the appropriate schedule to implement the functions. MAXIMUS is able to provide this flexibility because our expertise in implementing the CORE requirements and our strong M&O support plan.

Understanding CAQH Core

In 2005, CAQH established the Committee on Operating Rules for Information Exchange (CORE) to form an industry-wide stakeholder collaboration committed to the development and adoption of national operating rules for administrative transactions. The CAQH CORE requirements were introduced to

CONFIDENTIAL

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 requirement for accessibility, performance and structure and expand on the base X12 transaction and code set rules.

To implement the X12 HIPAA EDI components of Option A components in an online manner, vendors must verify that their solutions are able to meet the CAQH-CORE requirements. ACA defines operating rules as "the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications." Operating rules build on existing standards to make electronic transactions more predictable and consistent, regardless of the technology. Rights and responsibilities of all parties, security, transmission standards and formats, response time standards, liabilities, exception processing, error resolution and more must be clearly defined to facilitate successful interoperability. Beyond reducing cost and administrative hassles, operating rules foster trust among all participants.

MAXIMUS has a solid understanding of the CORE Operating Rules as offered by CAQH and mandated by the Affordable Care Act (ACA). Many of our team members are veterans of the initial HIPAA 4010 implementation and have extensive experience with the transactions and code sets. MAXIMUS has been working on implementing new online EDI functions within our online portal in a manner where we comply with the CAQH CORE requirement. In our Tennessee implementation our compliance efforts for CORE require close coordination and use of the EDIFECS platform and a SOA-based real-time data integration effort to bring necessary data to the portal in accordance with CORE performance requirements allowing our team to become proficient on the guidelines and rules. We have already integrated some of the high profile CORE related requirements into our Provider Services solution and have initiated a new project to bring all EDI transactions into our online portal.

Being able to readily implement CORE requirements into our solution demonstrates the flexibility and versatility of the modern, service oriented architecture of our system. We understand that all vendors will have to meet the CORE requirements and it's important to not only be able to state you can add these requirements but to understand the federal standards that also have to be met. We will work closely with states that choose this option to determine how we can implement the functions to meet the CORE requirements. Although CORE requirements are not currently included in the MECT, we envision the need to be able to support how we meet these ACA requirements.

Our self-service solution successfully serves the provider community in our three implementations by enabling online access to all services. The implementation of Provider Services solution for the State of Tennessee includes claim status, eligibility enquiry, electronic Remittance Advice. Additionally we are in the midst of development for a configurable sub module for the Claims entry and related 837 EDI X12 interface. We are expecting to complete that implementation by the first quarter of 2018 and make it available as our CORE offerings. The remainder of this section contains the details regarding how MAXIMUS solution meets the Option A Provider Services requirements for states that choose Option A.

3.10.13.1 Self-Service Member Eligibility Inquiry

3.10.13.1 Self-Service Member Eligibility Inquiry

This section outlines the requirements for Self-Service Member Eligibility Inquiry. The Offeror's proposed Option A solutions and services shall include real time verification of eligibility through the Self-Service Portal and provide eligibility information including benefit plan enrollment, care management enrollment, waiver program information, program limits, service limits, and TPL information on the self-service portal to providers and other users authorized by the State. The Offeror must describe their approach to meet each of the self-service eligibility requirements defined in Attachment F, Requirements Matrix.

To implement the Member Eligibility Inquiry (270) transaction for the State of Tennessee, MAXIMUS implemented a series of web services calls suing the SOA architecture supporting our Provider Services module, the EDIFECS platform and components of the legacy MMIS. MAXIMUS will customize the feature for the needs in Montana to perform real-time member eligibility inquiries either through an interface with the legacy MMIS or after the System Integration module is implemented. MAXIMUS will work with DPHHS and the EDI vendor to gather the requirements for Self-Service Member Eligibility Inquiry to implement the transaction as part of the provider self-service portal.

During the DDI phase, MAXIMUS will work with DPHHS and the System Integrator to develop a set of web services enabled via API to the State hosted Data Warehouse. We anticipate allowing both parties to consume the web services allowing a two-way interface to support both 270/271 transactions. When the MPATH Integration hub is available, MAXIMUS will work with the System Integrator to consume the web services for Eligibility Inquiry via ESB. In Tennessee, MAXIMUS consumed EDIFECS services exposed via a service bus and provided a user interface that allows providers to enter member's identification to initiate an eligibility inquiry and receive an eligibility response. Our solution allows providers to obtain member eligibility by searching using different required and optional parameters.

As a search is initiated, our solution sends a web services request to EDIFECS. It receives the eligibility response (271) that provides the user with member's eligibility dates, eligibility for one or more benefit plans, eligibility category, MCO details and other details as needed for the provider to determine a member's eligibility for services. The solution has the feature to print member eligibility information by the provider. *Exhibit 3.10.13.1-1: MAXIMUS Provider Services solution User interface for Member Eligibility Inquiry* shows an example of the eligibility inquiry user interface used by providers.

CONFIDENTIAL

Our solution is designed to send SOAP requests to EDI system and display the response back to the provider in easy and intuitive user interface. The usage statistics are stored to allow the state to determine the usefulness of the solution and how much usage is occurring. The usage statistics are made available from the MAXIMUS Provider Services reporting platform and are sent in a weekly email report to the appropriate stakeholders.

Self-Service Member Eligibility Requirements

The following table includes Attachment F Self Self-Service Member Eligibility Requirements and our summarized response to each requirement.

CONFIDENTIAL

ID	Self-Service Member Eligibility Requirement	MAXIMUS Summarized Response
PSER04	The Contractor's solution shall provide an online self-service tool for authorized users to perform real-time member eligibility inquiries. Eligibility inquiry responses will include at a minimum, eligibility dates, eligibility for one or more benefit plans, care management enrollment information, waiver program information, program limits, TPL information, and other member information necessary for the provider to determine if the member is eligible for services.	MAXIMUS is building real time member eligibility inquiry for the State of Tennessee. We intend to use this functionality as a starting point because the required data fields are defined, web service interfaces available and ESB integration is used. We will configure the functionality to enable a web services API with the data warehouse and ultimately through the ESB. Eligibility inquiry responses will include at a minimum, eligibility dates and any other data as directed by DPHHS.
PSER38	The Contractor's solution shall allow an external user to print member eligibility responses or download in PDF format.	MAXIMUS Provider Services solution has functionality to print member eligibility responses or download in PDF format.

3.10.13.2 Self-Service Claim Status Inquiry

> 3.10.13.2 Self-Service Claim Status Inquiry
> This section outlines the requirements for Self-Service Claim Status Inquiry. The Offeror's proposed Option A solutions and services shall include real time claims status inquiry to allow providers to check the status of their claims. The Offeror must describe their approach to meet each of the self-service claim status inquiry requirements defined in Attachment F, Requirements Matrix.

MAXIMUS is also extending the provider web portal in Tennessee to include claims status inquiry (276). We are enabling this interface in the same manner as the eligibility inquiry transactions, using a SOA-based web service integration enabled through the ESB. MAXIMUS will work with DPHHS during the DDI phase to consume the web services via API to the State hosted Data Warehouse. When the MPATH Integration hub is available, MAXIMUS will work with ESB Vendor to consume the web services for Claim Status Inquiry via ESB. In Tennessee, MAXIMUS consumed EDIFECS services exposed via service bus and provided a user interface that allows providers to enter claim, provider or service information to initiate the inquiry request.

Exhibit 3.10.13.2-1: MAXIMUS Provider Services Solution User Interface for Real Time Claim Inquiry shows the claims status inquiry user interface. Different search criteria are available for providers. MAXIMUS will work with DPHHS to determine what parameters can be used to identify claims and configure the web services to enable the required information to be sent with a response transaction that providers claims status information. As a search is initiated, our solution sends a SOAP request to EDIFECS. It receives the claim status response (277) that provides the user with claim status details. Our solution has options to print member claim information along with the parameters.

CONFIDENTIAL

Our solution is designed to send SOAP requests to the EDI vendor and show the response back to the provider in easy and intuitive user interface. We store the usage statistics for the feature to allow for the state to determine the feature's usefulness and amount of usage. The usage statistics are made available from the MAXIMUS Provider Services reporting platform.

Self-Service Claim Status Inquiry Requirements

The following table includes Attachment F Self-Service Claim Status Inquiry Requirements and our summarized response to each requirement.

CONFIDENTIAL

ID	Self-Service Claim Status Inquiry Requirement	MAXIMUS Summarized Response
PSER06	The Contractor's solution shall provide an online self-service tool for providers to view claim status.	MAXIMUS is building real time claim status inquiry for the State of Tennessee. We intend to use this functionality as a starting point because the required data fields are defined, web service interfaces available and ESB integration is used. We will configure the functionality to enable a web services API with the data warehouse and ultimately through the ESB. Claim status inquiry responses will include at a minimum, claim information and any other data as directed by DPHHS.
PSER43	The Contractor's solution shall allow authenticated users to download or print a claim status report in Excel and PDF.	MAXIMUS Provider Services solution has functionality to print claim status responses or download in PDF format.

3.10.13.3 Service Warrant and Remittance Advice Inquiry

3.10.13.3 Self-Service Warrant and Remittance Advice Inquiry

This section outlines the requirements for self-service warrant and remittance advice access. The Offeror's proposed Option A solutions and services shall provide access to remittance advice and warrant information through self-service portal for the provider and other users authorized by the State. The Offeror must describe their approach to meet each of the requirements for self-service warrant and remittance advice access defined in Attachment F, Requirements Matrix.

The first EDI transaction that was enabled through the MAXIMUS solution in Tennessee was the ability for providers to obtain electronic remittance advice. Enabling this transaction has been a big success for the State and providers as it has reduced the amount of customer service necessary to support paper remittance advice and questions about the status of claims. The MAXIMUS solution enabled Service Warrant and Remittance Advice Inquiry transaction for the State of Tennessee using a web service proof of concept through the ESB. MAXIMUS, EDIFECS and the legacy MMIS vendor worked together to develop the web services prototype and the subscriptions that would be used within the ESB. Once these components were developed, testing began. Once proven, these initial components are the basis for implementing the remaining transactions. MAXIMUS believes this is a good concept that could work well as the System Integrator is implementing the System Integration module.

MAXIMUS will work with DPHHS, the data warehouse vendor and the EDI vendor to gather the requirements to enable Service Warrant and Remittance Advice Inquiry. Together we will work out the mechanism for allowing remittance advice to be accessed through the self-service portal to verify that the provider in question should have access to the data. We have found this to be an especially important step implement because of the protected data that is included in the transaction.

MAXIMUS will work with DPHHS during the DDI phase to consume the web services via API to the State hosted Data Warehouse. When the MPATH Integration hub is available, MAXIMUS will work with the ESB Vendor to consume the web services for Remittance Advice Inquiry via ESB. In Tennessee, MAXIMUS consumed EDIFECS services exposed via service bus and provided a user that allows the providers get remittance advices and download them. Our solution is designed to get remittance advices using different parameters which edit against an authentication service. *Exhibit 3.10.13.3-1: MAXIMUS Provider Services Solution User Interface for Remittance Advice* depicts the user interface where providers access their remittance advice. Depending on the criteria, multiple can be shown.

CONFIDENTIAL

Our solution is designed to send SOAP requests to the EDI vendor and show the response back to the provider in easy and intuitive user interface. We will store the usage statistics for the feature to allow the state to determine the feature usefulness. The usage statistics is made available from MAXIMUS Provider Services reporting platform.

Self-Service Warrant and Remit Advice Inquiry Requirements

The following table includes Attachment F Self-Service Warrant and Remit Advice Inquiry Requirements and our summarized response to each requirement.

ID	Self-Service Warrant and Remit Advice Inquiry Requirement	MAXIMUS Summarized Response
PSER02	The Contractor's solution shall include an online self-service tool allowing authenticated users to view current and all previous warrants.	MAXIMUS Provider Services solution allows authenticated users to view current and previous warrants. We will customize the feature as per needs of DPHHS.
PSER07	The Contractor's solution shall provide an online self-service tool that allows authenticated users to access and view current and previous remittance advice that can be sorted by various parameters (EFT, date, NPI, etc.).	MAXIMUS has implemented this functionality in Tennessee. We intend to use this functionality as a starting point because the required data fields are defined, web service interfaces available and ESB integration is used. We will configure the functionality to enable a web services API with the data warehouse and ultimately through the ESB. We will allow authenticated users to access and view current and previous remittance advice that can be sorted by various parameters (EFT, date, NPI, etc.).
PSER40	The Contractor's solution shall allow authenticated users to download warrants and remittance advice in multiple formats (e.g., Excel or PDF) as directed by the State.	MAXIMUS Provider Services solution has functionality to print member eligibility responses or download in PDF format.

CONFIDENTIAL

3.10.13.4 Self-Service Claims Based Medical History

3.10.13.4 Self-Service Claims Based Medical History

This section outlines the requirements for Claims Based Medical History. The Offeror's proposed Option A solutions and services shall include member medical history access on the Self-Service Portal to allow providers with the authorized roles to access a member's medical histories interactively. The Offeror must describe their approach to meet each of the claims based medical history requirements defined in Attachment F, Requirements Matrix.

MAXIMUS will enable the ability of providers to access Claims Based Medical History for a particular member. We anticipate this functionality using the Claim Status Inquiry transaction requests as the basis for receiving the details of the member's entire medical history available. We anticipate customizing the user interface to enable providers to limit the amount of history based on certain parameters including dates of service and potentially procedures codes. We will need to work closely with DPHHS to understand what parameters can be used to obtain the data from the data warehouse. Depending on the API exposed by the data warehouse or EDI vendor, MAXIMUS collects all the other necessary information that would allow us to show the claims that are processed/in-process for a member.

Self-Service Claims Based Medical History Requirements

The following table includes Attachment F Self-Service Claims Based Medical History Requirements and our summarized response to each requirement.

ID	Self-Service Claims Based Medical History Requirement	MAXIMUS Summarized Response
PSER21	The Contractor's solution shall allow authorized users to search and view Claims Based Medical History.	MAXIMUS will build claims based medical history into Provider Services solution using the claims status functionality as the basis. We will work with DPHHS to understand what parameters can be used to obtain the medical history and define the filters to limit what claims data is sent.

3.10.13.5 View, Upload and Download HIPAA Compliant Healthcare Transactions

3.10.13.5 View, Upload and Download HIPAA Compliant Healthcare Transactions

This section outlines the requirements to View, Upload and Download HIPAA Compliant Healthcare Transactions. The Offeror's proposed Option A solutions and services shall allow authorized users to view, upload and download HIPAA compliant healthcare transactions (e.g., 270/271 batch eligibility status inquiry and response, 837 batch claims submission, and 276/277 Claim Status request and response) on the Self-Service Portal. The Offeror must describe their approach to meet each of the requirements to view, upload and download HIPAA compliant healthcare transaction requirements defined in Attachment F, Requirements Matrix.

MAXIMUS understands the needs of some providers to utilize batch processes to initiate and receive large volumes of transactions. While we anticipate being able to utilize the SOA-based web service integrations we developed for the online functions, we also know the complexity of the batch transactions will require close coordination with the EDI vendor and the data warehouse vendor. In our current implementations, the batch functions are directly supported by the EDI platform with coordination with the legacy MMIS vendor. We anticipate detailed designs being required so we can receive and transmit the required data and receive the necessary response in a transaction we can make available for download.

MAXIMUS will work with DPHHS and the EDI vendor to gather the requirements for batch processing of 270/271 eligibility status inquiry, 276/277 claim status inquiry and 837 batch claim submissions. For

CONFIDENTIAL

each of the three HIPAA transactions, 270/271, 837 and 276/277 transactions, we propose to build a user interface to allow providers to input a Batch EDI file. MAXIMUS will provide volume serial number (VSL) for each file that is uploaded by the user. This EDI file will then be transferred to the EDI vendor using web service transactions that they can consume. Several response transactions will be required. One to verify the transactions was received with or without error and then the response transactions that need to be provided on the self-service portal. On a successful validation, the EDI vendor responds with a positive response and a serial number for the batch. The MAXIMUS Provider Services solution will provide the batch number to the end user. Rejected transactions will be processed in the same manner with the appropriate response transaction and reasons. Exhibit 3.10.13.5-1: MAXIMUS Provider Services Solution User Interface for Batch Eligibility Inquiry shows an example of the user interface we are proposing to develop to support transfer and receipt of batch transactions.

Our solution will provide another link to verify the status of the batch transactions. The provider can look at all the different batches and the VSLs for each batch. MAXIMUS will query the EDI vendor services to get the status of each batch using the VSL for the batch. As the batch is complete, the provider can download the response for each batch.

CONFIDENTIAL

Our solution is designed to not store any eligibility and claim information, leaving those functions to the system of record. Instead, we will design our processes to send SOAP requests to the EDI vendor and consume the response so it can be displayed back to the provider in easy and intuitive user interface in a pass through manner. We store the information about the batch requests performed by the user. We get the response for each batch request from the EDI vendor as the provider downloads the response. Our solution records usage statistics for all the features. The usage statistics can be made available from the MAXIMUS Provider Services reporting platform.

HIPAA Requirements

The following table includes Attachment F Self-Service View, Upload and Download HIPAA Compliant Healthcare Transactions Requirements and our summarized response to each requirement.

ID	HIPAA Requirement	MAXIMUS Summarized Response
PSER39	The Contractor's solution shall allow authorized user to view, upload and download HIPAA compliant healthcare transactions (e.g., 270/271batch eligibility status inquiry and response, 837 batch claims submission, and 276/277 Claim Status request and response) on the Self-Service Portal.	MAXIMUS Provider Services module will be enhanced to include this functionality. We will base the batch transactions on the online functions we develop with the extra steps of verification and volume reporting.

3.10.13.6 Self-Service Online Provider Appeal Request

> 3.10.13.6 Self-Service Online Provider Appeal Request
>
> This section outlines the requirements for Online Provider Appeal Requests. The Offeror's proposed Option A solutions and services shall provide the functionality for providers to request appeals. Automated workflow integration will route appeals to the appropriate work unit or user. The Offeror must describe their approach to meet each of the online provider appeal request requirements defined in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution has a comprehensive appeal workflow for providers who have been denied or terminated. The appeal workflow is driven by Business Process Engine with capabilities described in *Section 3.10.1.9–Workflow*. In our previous implementations, all the providers who are terminated or denied due to screening failure, background check failure, site visit failure etc., are automatically put into appeal workflows. MAXIMUS will work with DPHHS to define the appeal workflow that conforms to the requirements of the State. MAXIMUS will configure the workflow to route appeals to appeal specialists as appropriate. Our solution displays appeal statuses on the provider home page. It will allow for terminated/denied providers to initiate new appeals, view appeal statuses etc.

MAXIMUS will configure the appeals functionality for other business interactions like claims for DPHHS. MAXIMUS business analysts will work with DPHHS to identify the necessary information to start an appeal process based on the type of appeal. We will also design for any documents that the provider needs to upload as part of initiating an appeal. With the information in the appeal, we will instantiate an appeal workflow that is driven by our Business Process Engine. Based on the type of appeal, we will route the appeal request to appropriate users. An operator/appeal specialist can get to a new appeal by clicking "Get Next in Queue" similar to that of selecting a provider enrollment. The workflow will be configured so that the appeal specialist can request additional information from the provider. The appeal specialist will have options to route the appeal to the appropriate person. For example, if the appeal is for a claim, the appeal specialist can route the appeal to a claim processing user.

And if the appeal is for an enrollment, the appeal specialist can route the appeal to an enrollment specialist, who could be a DPHHS user.

Depending on the DPHHS requirements, we can build the workflow to notify the claim processing user or enrollment specialist that a new appeal is ready for review. Depending on the type of appeal, MAXIMUS can configure the solution to request different kinds of information from the claim processing user or enrollment specialist. Depending on the action taken by claim processing user or enrollment specialist, the decision on the appeal will be conveyed to the provider. Our solution will send an email containing the appeal decision and the status of the appeal request in the self-service will be updated accordingly.

MAXIMUS will build the necessary interfaces to be invoked based on the appeal result. In case of a successful appeal by the provider for a claim, MAXIMUS will send the claim information to the MMIS or other vendor solution to be paid. In case of an enrollment or termination, MAXIMUS will send an update to the MMIS based on the result of the appeal request.

We will build the workflow to notify the provider on the appeal result. MAXIMUS will also build a user interface to show the list of appeals and their statuses.

Self-Service Online Provider Appeal Request Requirements

The following table includes Attachment F Self-Service Online Provider Appeal Request Requirements and our summarized response to each requirement.

ID	Self-Service Online Provider Appeal Request Requirement	MAXIMUS Summarized Response
PSER03	The Contractor's solution shall support on-line self-service tool for all providers to request an appeal.	MAXIMUS will extend current functions to enable providers to request an appeal for all business interactions.
PSER41	The Contractor's solution shall allow users to view the status of their appeal request.	The MAXIMUS solution allows providers to see the current status of their appeal.

3.10.13.7 Self-Service PCCM Member Inquiry

> 3.10.13.7 Self-Service PCCM Member Inquiry
>
> This section outlines the requirements for Self-Service PCCM Member Display. The Offeror's proposed Option A solutions and services shall include display and download functionality to allow providers enrolled in care management programs to view their caseload and download their member registries. The Offeror must describe their approach to meet each of the self-service PCCM member inquiry requirements defined in Attachment F, Requirements Matrix.

MAXIMUS understands the need for care management providers to be able to access their caseloads and download member registries. We appreciate the goal of making the Provider Services solution a one-stop solution for all provider needs. The solution must be functional and designed with the end-user experience in mind. Working with DPHHS for requirements, we will design and build a user interface for providers enrolled in care management programs to view their caseload and download their member registries in a fast, easy, and effective way. We will design these functions to work in the same manner as the online inquiry transactions where a provider utilizes a user interface to set parameters to filter the results of the inquiry. This function will require a new web services integration to send the request information to the data warehouse or through the ESB to obtain the results. We will work closely with DPHHS to determine how and when this function can be implemented. We will focus on security and access because of the

protected nature of the data. We intend to allow authorized users to download and print member registries in Excel and PDF formats.

MAXIMUS has provided several interfaces in our previous implementations for different purposes. MAXIMUS will work with DPHHS and the MMIS vendor to define the requirements for building a standardized interface via service bus for populating the PCCM member registry.

Self-Service Registry Requirements

The following table includes Attachment F Self Self-Service Registry Requirements and our summarized response to each requirement.

ID	Self-Service Registry Requirement	MAXIMUS Summarized Response
PSER14	The Contractor's solution shall allow authorized users to view registries for PCCM and other care management programs.	MAXIMUS will provide a user interface for providers enrolled in care management programs to view their caseload and download their member registries.
PSER44	The Contractor's solution shall allow authenticated users to download or print member registries in Excel and PDF.	The user interface will have authorized users to download and print member registries in Excel and PDF formats.

3.10.13.8 Self-Service Online Claims Entry

> 3.10.13.8 Self-Service Online Claims Entry
> This section outlines the requirements for Online Claims Entry. The Offeror's proposed Option A solutions and services shall include a real-time direct data entry claims solution for all claim types, corrections, void and replacement claims via the self-service portal and reject claims that fail front-end edits. The Offeror must describe their approach to meet each of the online claims entry requirements defined in Attachment F, Requirements Matrix.

For states will fee for service caseloads, the ability to enter claims is a necessity as it cuts down on internal data entry and vastly reduces the amount of paper that is required. MAXIMUS is in the process of building processes to enable 837 transaction entry for the State of Tennessee in Provider Services solution. The implementation for an 837 interface is scheduled to be completed by the second quarter of 2018. Given that claims data is defined by HIPAA, we believe we can use these newly designed processes directly in Montana. MAXIMUS will gather requirements from DPHHS to validate required authentication and workflow and leverage the user interface and other components we are developing for our implementation in Montana.

MAXIMUS has built-in libraries that take data from the user and build EDI transactions. We will validate the user interface data, confirm the transaction is set for the correct EDI version that is supported by the EDI vendor, and validate the EDI file as required. The interface will also be capable of receiving acknowledgements. Validation details will be presented to the provider in a user-friendly manner.

Handling Claim Inputs and Types

MAXIMUS has expertise and understanding of EDI 837 claim transactions. We will collect all the data necessary for creating EDI 837 Transactions. The 837 transaction is designed to transmit one or more claims for each billing provider. The transaction data will include structures (segments) for billing provider, subscriber, patient, claim level, and claim service line level.

MAXIMUS will collect the conditional data as required for Professional (837P), Institutional (837I) and Dental (837D) claims. The user will choose the type of claim they want to create as they initiate the claim process. Rendering Provider, Provider Group, Individual Provider, and billing agent are collected if the

claim type is Professional. Attending Provider, Service Facility, billing agent information is collected if the claim type is Institutional. If the claim type is Dental, we will also collect accident information along with applicable provider information. MAXIMUS will also add all the necessary sections for Encounter claims, Adjustments, Roster billing, claim corrections, and the ability to void and replace claims.

After an initial search for the provider, our user-friendly screens will be pre-populated with the required provider data from the Operational Data Store to create the billing provider segment. This information includes provider NPI, taxonomy code, employee identification number and zip plus the four digit postal code. The service location information is pre-populated in the service location section of the claim form. Our solution will contain edits to confirm the billing provider is active and, if not, will be provided steps to re-activate the enrollment.

The EDI 837 transaction provides a large amount of data at both claim level and service line level. Our solution will contain edits to confirm all data at the claim level and service line level have the correct member eligibility, valid revenue codes, procedure codes, and diagnosis codes. The user has the option to upload attachments associated with the claim or indicate they are sending paper or fax documentation. Available help text displays the claim number so it can be referenced on the paper or fax documentation.

After claim data is entered, the solution validates the data, converts the claim information into X12 837 format, and sends it to the EDI vendor via the ESB. Tracking information sent by EDI vendor will be presented to the end user.

We know that providers often submit subsequent claims with similar data entries as previous claims. Our solution will provide a claim template feature that allows users to save the data as a template. This template feature greatly reduces the time spent doing later data entry, reduces the risk of errors, and expedites the time to payment.

Self-Service Online Claims Entry Requirements

The following table includes Attachment F Self-Service Online Claims Entry Requirements and our summarized response to each requirement.

ID	Self-Service Online Claims Entry Requirement	MAXIMUS Summarized Response
PSER13	The Contractor's solution shall include a self-service tool for providers to directly and efficiently enter claims.	MAXIMUS is on the process of implementing this functionality in Tennessee. We will leverage this functionality to extend the functionality of the provider self-service portal to include a self-service tool for providers to directly and efficiently enter claims.
PSER29	The Contractor's online self-service claims entry tool shall accommodate and accept all claim types including Professional, Institutional, Dental, Encounter claims, Adjustments, Roster billing, claim corrections, and the ability to void and replace claims.	Our solution will accommodate and accept all claim and transactions specified in the 837 guides.
PSER30	The Contractor's online self-service claims entry tool shall include a validation feature that performs real-time front end editing prior to claim submission, not allowing submission of claims that fail the front end edits. Edits will include, but are not limited to, active provider enrollment, member eligibility, valid revenue codes, procedure codes, and diagnosis codes. Front end edit(s) shall be displayed to the user for review and correction. The validation feature will not display pricing information.	The claim entry user interface will include all the validations required for submitting a successful claim. We will provide user-friendly error messages to the end user for making corrections. We will utilize the implementation guides in Montana to define the edits that are required.

ID	Self-Service Online Claims Entry Requirement	MAXIMUS Summarized Response
PSER31	The Contractor's online self-service claims entry tool shall allow an authenticated user to upload an attachment to associate with a specific claim or multiple claims.	Our solution allows users to upload an attachment associated with specific or multiple claims. The system provides fields for the user to indicate they are sending attachments by mail or fax, along with instructions such as including claim number on the paper, mailing address, and fax number. We will work with DPHHS to determine how claims attachments will be processed and sent to the EDI vendor.
PSER32	The Contractor's online self-service claims entry tool shall instruct users to include a claim confirmation number on any paper attachment when users indicate that an attachment is being mailed or faxed in order to allow for efficient association between a claim and an attachment.	Our solution allows users to upload an attachment associated with specific or multiple claims. The system provides fields for the user to indicate they are sending attachments by mail or fax, along with instructions such as including claim number on the paper, mailing address, and fax number. We will automatically assign a relationship between the attachment and the claim to validate we have a proper relationship.
PSER33	The Contractor's online self-service claims entry tool shall allow users to indicate paper attachments will be mailed and/or faxed.	Our solution allows users to upload an attachment associated with specific or multiple claims. The system provides fields for the user to indicate they are sending attachments by mail or fax, along with instructions such as including claim number on the paper, mailing address, and fax number.
PSER34	The Contractor's online self-service claims entry tool shall provide a tracking or control number to the user upon successful completion of the transaction.	After the claim is submitted, our solution will present tracking information to the end user as sent by EDI vendor.
PSER35	The Contractor's online self-service claims entry tool shall provide a configurable auto populate feature for appropriate fields for each claim type (e.g., provider information, submission date and member associated information).	Our self-service claims entry tool will provide a configurable auto populate feature for all appropriate fields for each claim type. We will work with DPHHS to determine which fields can be populated and what values should be used.
PSER36	The Contractor's online self-service claims entry tool shall include a claim template feature that allows users to create a templates to be stored and used in the online claims entry tool.	Our self-service claims entry tool will include a feature to save claim templates that will make it easier and faster for the users to initiate new claims.
PSER37	The Contractor's solution shall provide search capabilities for users entering data in the online claims entry tool. The search tool will include provider information and provider associated service authorization information.	Our self-service claims entry tool will provide search capabilities for entering data in the online claims entry tool. We will bring in valid providers and can perform edits to confirm the correct provider type is being added.
PSER42	The Contractor's online self-service claims entry tool shall convert all entered claims into an X12 837 format.	After successful validation, our self-service claims entry tool will convert all the claims into X12 837 format and will send the claim to EDI vendor via Service bus.

Self-Service Portal – Option A Services

In this subsection, we address the three requirements from Appendix F that were listed under the Self-Service portal category but were identified as Option A Provider Services. The Provider Services self-service web portal provides easily accessible links to users for training materials and other relevant web resources, including State sites as required. The Provider Education & Training Resources page organizes static web content by communications, training materials and links to other websites. The website provides a Contact Us link where we provide contact information for the call center and any other required contacts as communicated by the State. We can also enable content links on any page. All reference materials are generally stored in PDF format and can be viewed, downloaded or printed as necessary. *Exhibit 3.10.13.8-1: Website Resource Links* shows the current District of Columbia configuration for this type of information on the portal.

CONFIDENTIAL

Self-Service Portal – Option A Requirements

ID	Self-Service Online Claims Entry Requirement	MAXIMUS Summarized Response
PSER23	The Contractor's solution shall provide an online self-service Frequently Asked Questions (FAQ) tool that is easily navigable and searchable. The FAQ shall be updated quarterly or as directed by the State.	This is a current feature of the system. We have FAQs posted and accessible from any screen.
PSER24	The Contractor's solution shall allow users to view, download and/or print current and historical provider information (e.g., manuals, instructions, bulletins, program descriptions, eligibility criteria and forms).	The majority of system information is stored in PDF format and can be printed as required. Our solution also contains functions that enable online data to be viewed, downloaded, or printed. We will identify what historical provider information must be included in these functions.
PSER27	The Contractor's solution shall provide access for users to view current and historical fee schedules.	The MAXIMUS solution will enable all Option A functions via web service APIs that provide data integration with other systems containing the necessary data. We are able to extend these web services to obtain historical fee schedule information and provide them to providers on a user interface accessible for a variety of screens. MAXIMUS will work with the Department to understand the system that contains this information, how it is updated, and what data should actually be shown to providers.

3.10.14 Option B Provider Services

> 3.10.14 Option B Provider Services
>
> In addition to the primary scope of the Provider Services module, states may procure components and services not categorized in Section 3.10.1 through 3.10.13. Option B Provider Services requirements provide flexibility to States or Agencies who may desire to procure the components or services outlined in Option B as a part of this procurement versus a separate procurement. The Offeror is not required to include Option B in their proposal. If the Contractor chooses to include these services in their proposal the Contractor must describe in their response, their approach to meet the Option B requirements detailed in Attachment F, Requirements Matrix.

With an existing and proven Provider Services solution that meets Centers for Medicare & Medicaid Services (CMS) requirements and our experience operating similar provider screening and enrollment projects in five other jurisdictions, MAXIMUS has unparalleled qualifications to deliver and operate Provider services. Through our strong national presence and Provider operations in multiple jurisdictions, we 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 to exceed expectations.

Building on more than fifteen years of experience serving Medicaid Providers and our successful operation of ten provider operations across seven states and the District of Columbia, MAXIMUS is fully prepared to assist the efforts of participating states implementing and maintaining enhanced Medicaid Provider screening and enrollment requirements mandated by the ACA. As demonstrated in *Exhibit 3.10.14-1: MAXIMUS Provider Services Solution*, the foundation of our approach is our proprietary, custom-designed, fully compliant solution. This system, along with our leadership team, have been central in implementing relevant Provider screening and enrollment programs in Tennessee, Nebraska, and the District of Columbia.

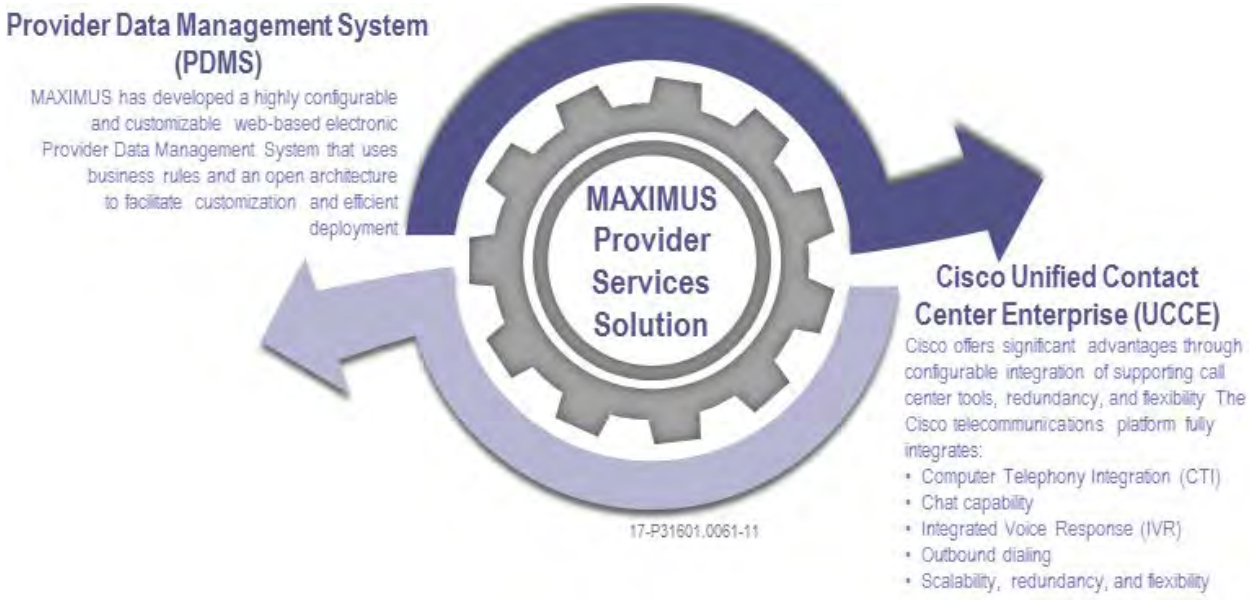


Exhibit 3.10.14-1: MAXIMUS Provider Services Solution. *Our solution combines our highly configurable and customizable web-based system with Cisco Unified Contact Center Enterprise to provide a solution that exceeds performance expectations.*

MAXIMUS experience enables us to deliver the best combination of highly configurable technology and operational expertise to provide participating states with a successful and effective Provider screening and enrollment solution.

3.10.14.1 Conduct Provider and Maintain Site Visits

> 3.10.14.1 Conduct Provider and Maintain Site Visits
>
> This section outlines the requirements necessary for conducting and maintaining provider site visit information. During the provider enrollment screening process for moderate and high-risk providers, there is a mandated requirement for the Agency to conduct an on-site evaluation of the provider. The Offeror's Proposed Option B solutions and services shall include providing staff to act on behalf of the Agency in order to conduct the on-site evaluation of the provider. The Contractor will upload the results of the site visit evaluation into the provider's profile within the Provider Services module. Site visits can include but are not limited to: verification that the information submitted to the Agency is accurate and in compliance with federal and state enrollment requirements, accurate business hours, checking personnel at the business location, etcetera. The Offeror must describe their approach to meet each of the Site Visit requirements defined in Attachment F, Requirements Matrix.

MAXIMUS is fully prepared to assist the participating states' efforts in implementing and maintaining Medicaid Provider screening and enrollment requirements. As part of the Provider screening workflow, MAXIMUS Operations conduct unannounced site visits, pre-enrollment and post-enrollment, to all

moderate, high risk, new, and re-enrolling providers submitting applications. Our Site Visit Specialist will be equipped with a Microsoft Surface Pro Tablet to allow completions of site visit checklists, take photographs, and upload completed material to the provider record, via a secure and paperless environment.

Pre-Enrollment Unannounced Site Visit

Once a provider completes an application, the provider is screened and applicable databases are checked. MAXIMUS Provider Services solution then places the application in the site visit workflow, initiating an unannounced pre-enrollment site visit by our Site Visit Specialists. Our solution assigns the applications to the Site Visit Specialist who retrieves the application and conducts the site visit.

Providers remain in site visit status until the Site Visit Specialist updates the system with the results of the site review.

As shown in *Exhibit 3.10.14.1-1: MAXIMUS Pre- and Post-Unannounced Site Visit Workflow*, the Site Visit Specialist performs the following tasks as part of the pre-enrollment unannounced site visit, using the MAXIMUS-issued mobile tablet:

1. Document the specialist's name, organization, and reason of the visit
2. Observe the facility to ensure the site is in operational compliance within the State guidelines
3. Interview the staff identified in the application to make sure all questions listed in the Site Visit Checklist are answered
4. Gather all quantitative and qualitative data to support an enrollment decision
5. Document in detail each interview and any observations
6. Using the MAXIMUS-issued mobile tablet, take pictures, per the checklist, including the following:
   - Front of the facility, including the signage and hours of operation
   - Handicap accessibility
   - Any required facility licenses
   - Inventory of any supplies such as medication, or any Durable Medical Equipment (DME) distributed to the recipients
7. Review the Site Visit Checklist for accuracy and ensure it is complete before leaving the facility
8. Upload all documentation and photo files into the system
9. Complete the site visit section of the application workflow
10. Recommend the application for a denial or enrollment decision

Exhibit 3.10.14.1-1: MAXIMUS Pre- and Post- Unannounced Site Visit Workflow. *Site Visit Specialists perform a thorough review of the Provider's site to ensure they meet all State requirements.*

Exhibit 3.10.14.1-2: Provider On-Site Inspection Checklist depicts a portion of the site visit checklist implemented as part of our Provider screening and enrollment services.

THE MONTANA DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES

DME / POS Provider Site Visit checklist

New Applicant ○ In-State: ○
Re-enrollment ○ Out-of-State ○

Applying Provider: _____

Date of Site Visit: _____ Time: _____

Reviewer: _____ Witness: _____

DC Medicaid Provider Number: _____ NPI: _____

Provider Address: _____

Contact Person: _____ Phone: _____

Email: _____ Fax: _____

DIRECTIONS TO COMPLETE THE INSPECTION:
Check the appropriate box indicating whether or not the provider's location mirrors what was provided in the application package.

Provider On-Site Inspection Checklist

Requirement	Item Verification	Evaluation	
		Yes	No
1	Business name appears on clear signage	○	○
	Is there a visible sign that states the name of the provider and shows that the business operates at least 32 hours per week?		
	Company Name _____	○	○
	Address _____	○	○

Exhibit 3.10.14.1-2: Provider On-Site Inspection Checklist. *Site visit specialists complete all portions of the checklist and upload the completed checklist to the system in real time.*

Post-Enrollment Unannounced Site Visit

Once Providers pass initial screening and pre-enrollment site visit requirements, the Site Visit Specialist logs the initial date of enrollment and tracks the due date for the unannounced post-enrollment site visit in the web portal. Our solution creates a task in the Site Visit Specialist work queue for a post-enrollment site visit after three months and within one year from the Provider's initial date of enrollment. The timing of the post-enrollment site visit is configured using State-defined rules.

Post-enrollment site visits follow the same processes and procedures as the pre-enrollment site visit. If the Site Visit Specialist is unable to complete the visit on the scheduled date, the specialist must make a second attempt to complete the site visit within ten days of the first attempt.

Conduct Provider Site Visit Requirements

The following table includes Attachment F Conduct Provider Site Visit Requirements and our summarized response to each requirement.

ID	Conduct Provider Site Visit Requirement	MAXIMUS Summarized Response
PSV01	The Contractor shall conduct pre- and post-enrollment onsite screening of moderate and high-risk providers according to Agency onsite screening protocols and federal onsite screening regulations, including at a minimum: -Conducting the initial assessment to verify the facility location, hours and personnel; -Verifying operational status; and -Confirming final determination of provider enrollment status.	MAXIMUS is fully prepared to assist participating states in implementing and maintaining enhanced Medicaid Provider screening and enrollment requirements. As part of the Provider screening workflow, MAXIMUS Operations conduct Pre and Post unannounced site visits to all moderate, high risk, new, and re-enrolling providers that submit an application to be part of the Medicaid Provider program to ensure providers are practicing in an appropriate and ethical manner. Our Site Visit Specialist will be equipped with a Microsoft Surface Pro Tablet to complete the checklist and upload the completed form in the provider record without using paper.

3.10.14.2 Include Reference Documents

> 3.10.14.2 Include Reference Documents
>
> This section outlines the requirements necessary to include reference documents in the provider portal. The Offeror's Proposed Option B solutions and services shall include providing access to current and historical provider manuals and other reference documentation, as necessary, within the portal. The Contractor will not be responsible for creating or maintaining manuals. The Offeror must describe their approach to meet each of the Current and Historical Reference Document requirements defined in Attachment F, Requirements Matrix.

Include Reference Documentation Requirements

MAXIMUS understands the importance of providing thorough and complete reference information for internal and external users of our solution. Therefore, our solution includes a reference page for users to access current and historical provider claims manuals, as well as training materials that show all new changes or enhancements and detail information on how to complete a provider application or navigate the MAXIMUS Provider Services System.

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

ID	Include Reference Documentation Requirement	MAXIMUS Summarized Response
RFDC01	The Contractor's solution shall provide external and internal users access to current and historical provider manuals (e.g., CMS1500, Dental Claims Manual, Institutional Claims manual, Pharmacy Claims Manual and other Agency manuals or provider bulletins related to Medicaid policy and claims processing. NOTE: Contractor shall not be responsible to create the content of the manuals.	Our web-accessible system includes easy to use pages where users can access or download current and historical provider manuals.

3.10.14.3 Customer Relationship Management

> 3.10.14.3 Customer Relationship Management
>
> This section outlines the requirements for a Customer Relationship Management Tool. The Offeror's Proposed Option B solutions and services will include providing and utilizing a Customer Relationship Management (CRM) tool in order to

manage correspondence with providers. The CRM tool will be able to capture interactions with providers through free-form text, pre-defined data elements, and be capable of searching logged correspondence on command. The CRM tool will support attachments; linking of documents and information within the tool; and routing of correspondence and captured information through the workflow to specific individuals. The Offeror must describe their approach to meet each of the Customer Relationship Management tool requirements defined in Attachment F, Requirements Matrix.

As part of our commitment to the delivering exceptional service to the states participating in this procurement, MAXIMUS will extend its established and highly configurable Provider Services solution to provide full Customer Relationship Management (CRM) functionality. Using our solution, we provide comprehensive collection and tracking in support of day-to-day operations. *Exhibit 3.10.14.3-1: MAXIMUS Provider Services Solution* provides an overview of our solution feature sets.

Exhibit 3.10.14.3-1: MAXIMUS Provider Services Solution. *Our solution includes features designed to offer a full range of support to the Montana Department of Public Health and Human Services (DPHHS) Provider screening and enrollment program.*

Cisco Unified Contact Center Enterprise (UCCE)

MAXIMUS will integrate our Provider Services solution with the Cisco Unified Contact Center Enterprise (UCCE) or "Cisco" enterprise telephony contact center solution. Cisco offers significant advantages through configurable integration of supporting call center tools, redundancy, and flexibility. As demonstrated in *Exhibit 3.10.14.3-2: Cisco Unified Contact Center Enterprise*, the Cisco telecommunications platform fully integrates:

- Computer Telephony Integration (CTI)

- Chat capability
- Integrated Voice Response (IVR)
- Outbound dialing
- Scalability, redundancy, and flexibility

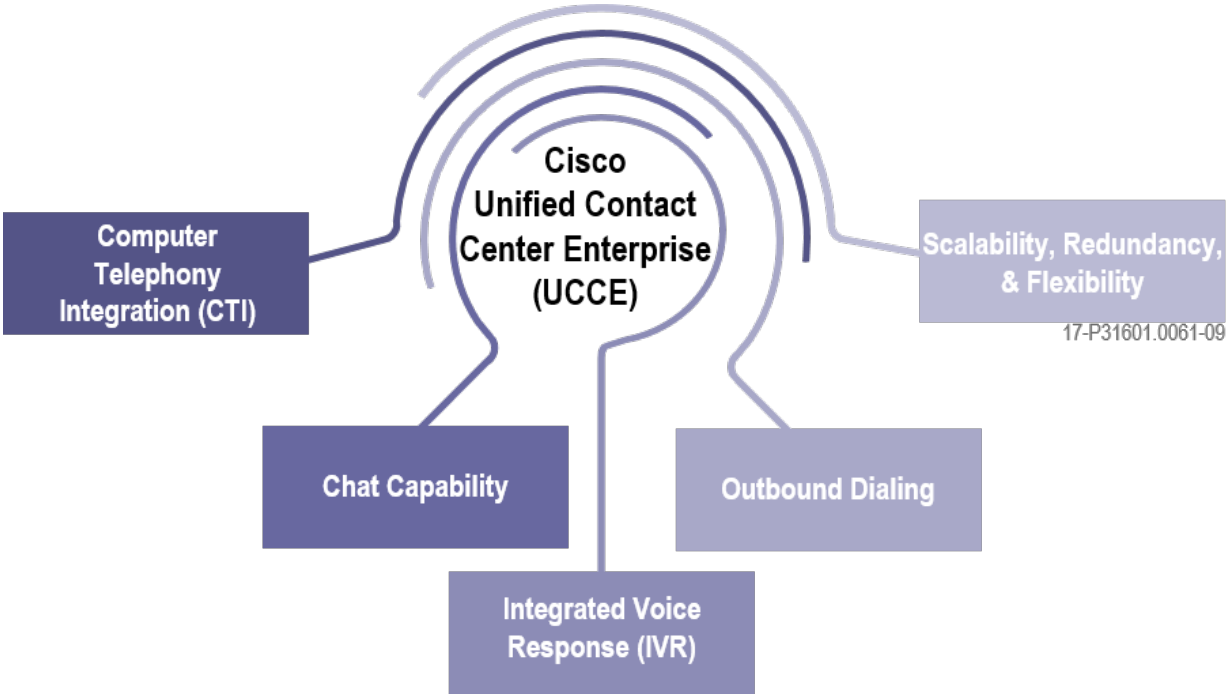


Exhibit 3.10.14.3-2: Cisco Unified Contact Center Enterprise. *Cisco offers significant advantages through configurable integration of supporting call center tools, redundancy, and flexibility.*

A key feature of this integrated solution is provided through Computer Telephony Integration (CTI). Once the caller has been authenticated via Integrated Voice Response (IVR) system prompts and responses, CSRs are automatically presented via their computer screen, through computer-telephony integration (CTI), with the caller's information. This CTI functionality is also known as "screen-pop" capability.

CTI allows CSRs to access the caller's information, case notes, and call history almost immediately, allowing them to validate the caller's identity efficiently and giving them a full understanding of the caller's case, allowing them to meet the caller's needs quickly.

MAXIMUS will establish and maintain a toll-free call center number that includes a 24-hour voice messaging system that informs callers of the call center's hours of operation and allows them an option to leave voice messages.

SPOTLIGHT ON:

Our telephony platform

Cisco has been recognized as a leader in Unified Communication by Gartner – and has been positioned as a leader in the Gartner Magic Quadrant for Unified Communications.

Through Cisco, we have chosen a telephony platform that delivers:

- Intelligent contact routing, call treatment, and contact management
- A modernized infrastructure able to support additional functionality through configurable telephony and reporting applications
- Redundant data centers to support operational business continuity for call centers

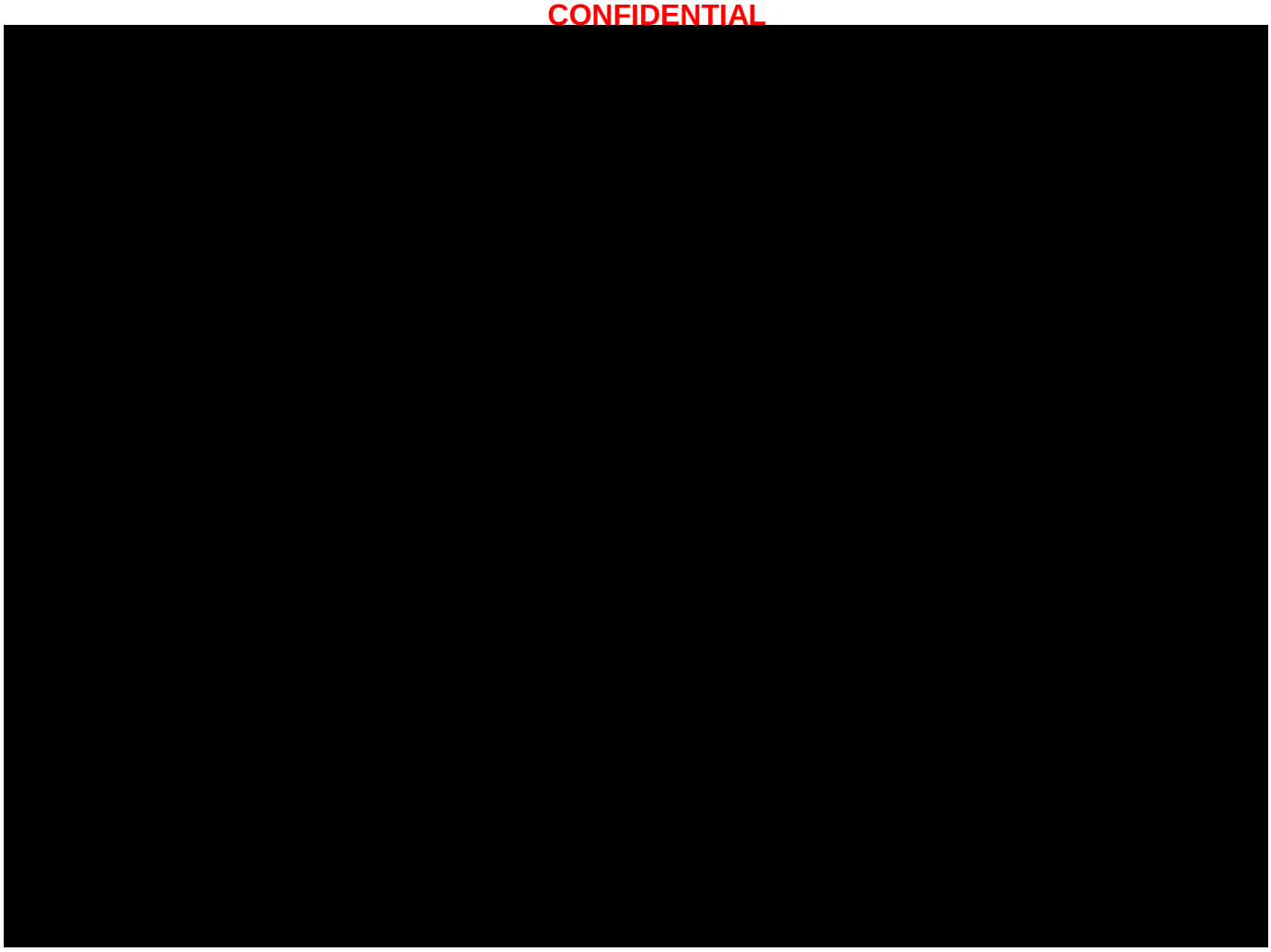
Work Queues and Auto-Alert Capabilities

Our solution contains workflows that set up work queues and auto-alerts to assign different types of work to the correct roles, thereby providing details about the status of an application or other work item, and increasing automation and efficiency. Workflows also trigger alerts to external entities and other agency users regarding changes to a Provider's enrollment status.

Data Collection

To continuously improve access, functionality, and accuracy, MAXIMUS will work with State staff during the start-up phase our operational implementation to design detailed policies, procedures, and business rules for data collection. We will also design the building of fields for documenting detailed call information as well as a field for storing the caller's preferred method of communication. As shown in *Exhibit 3.10.14.3-3: Provider Record Screen*, the MAXIMUS Provider Services solution includes free-form, customized text fields for adding additional details and comments that allow our representatives to ensure all call details are recorded accurately.

CONFIDENTIAL



The MAXIMUS Provider Services solution records and links every call, email, web chat conversation, as well as received and generated pieces of written correspondence. As a result, we capture a detailed and comprehensive record of the caller's full contact history. Our solution is fully integrated with the Hyland OnBase scanning and imaging solution to create a digital image of written correspondence associated with the provider record.

Hyland OnBase Scanning and Imaging Solution

Hyland OnBase provides enterprise content management of records, forms, and correspondence by converting all documents to searchable PDF files and storing them in an integrated document repository. These documents are tagged with the Provider ID, which automatically links them with the appropriate Provider record, enabling users to search by the complete index criteria of the documents or the information contained within the document.

Customer Relationship Management Requirements

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

ID	Customer Relationship Management Requirement	MAXIMUS Summarized Response
CRM01	The Contractor's solution shall provide the capability to automatically alert external entities (e.g., managed care companies and financial management companies for self-directed care) and other Agency users about their providers' enrollment status and enrollment status changes.	Our solution contains workflows that set up work queues and auto-alerts to assign different types of work to different roles, increasing automation and efficiency. Also built into our solution workflow is the ability to automatically alert external entities and other Agency users about changes to a Provider's enrollment status
CRM02	The Contractor shall provide a voice messaging system for after hours callers indicating the hours of operation and provide options for leaving messages.	Through our Cisco telephony solution, MAXIMUS will establish and maintain a toll-free call center number that includes a 24-hour voice messaging system that informs callers of the call center's hours of operation and allows them an option to leave voice messages.
CRM03	The Contractor shall establish and maintain a toll-free telephone number for the call center.	Through our Cisco telephony solution, MAXIMUS will establish and maintain a toll-free call center number that includes a 24-hour voice messaging system that informs callers of the call center's hours of operation and allows them an option to leave voice messages.
CRM04	The Contractor shall use Computer Telephone Integration (CTI) to provide personalized routing and work-object handling based upon identifiers received from the caller regarding language, inquiry area, and ability to produce reports on both electronic and voice transactions.	Our Cisco telephony solution uses Computer Telephony Integration (CTI). Once the caller has been authenticated, CSRs are automatically presented with the caller's information and complete call record on their computer screen through CTI, also known as "screen-pop" capability. CTI allows CSRs to access the caller's information, case notes, and call history almost immediately, giving them a full understanding of the caller's case and allowing them to meet customer needs as quickly as possible. The Cisco telephony solution will be fully integrated with our solution to provide full reporting capabilities for both electronic and voice transactions.
CRM05	The Contractor shall provide, configure and maintain an automated call and contact tracking system (CRM tool) for all calls and correspondence received.	The MAXIMUS Provider Services solution automatically records and links every call, email received, every message sent by text or email, every web chat conversation, and every received or generated piece of written correspondence to create a full and detailed record of the caller's contact history.
CRM06	The CRM tool must log and track information for each call that includes at a minimum the following elements: a. time of call b.date of call c. identifying information on caller d. representative ID e. call type f. call category g. inquiry description h. ticket status i. response description j. call reference number	MAXIMUS will work with the State staff during implementation to design detailed policies, procedures, and business rules for data collection, including building all the identified fields and the caller's preferred method of communication.
CRM07	The Contractor's CRM tool shall have the ability to link the CRM record and the workflow tool to automatically route appropriate tickets to the State for review.	The solution workflow will be configured to flag tasks for State action and place them in a queue for the State workers.
CRM08	The Contractor's CRM tool shall have the ability to link related CRM tickets.	Our solution records and links every call, email received, every message sent by text or email, every web chat conversation, and every received or generated piece of written correspondence to create a full and detailed record of the caller's contact history.
CRM09	The Contractor's CRM tool shall have the ability to include a free form text field for each CRM ticket for comments and/or resolution.	In additional to customized fields for contact tracking, the PDMS will also include free-form text fields for adding additional details and comments that will allow our representatives to ensure all call details are recorded accurately.

ID	Customer Relationship Management Requirement	MAXIMUS Summarized Response
CRM10	The Contractor's CRM tool shall have the ability to provide for online display, inquiry, and updating of call records with access, including, but not limited to, call type, API or NPI number, inquirer's name, representatives ID or name, provider name, or a combination of these data elements.	Our solution is a web-based, Java script platform that allows users to display, search, and update call records by call type, API or NPI number, inquirer's name, representative ID or name, Provider name or number, service category, CRM number, service authorization number, and other metadata fields that are native to the application. Our CSRs have read/write access to all fields included in the Provider call record to update information in real time.
CRM11	The Contractor's CRM tool shall have the ability to provide State resources or designated resources local and remote access to the CRM system.	To increase transparency with the State, MAXIMUS will provide secure local and remote access to all our systems by providing a single access point that will be consistent across all applications. State workers will be able to have direct access through specified login credentials and remote access through a secure VPN or MPLS, whichever method is agreed upon through contract negotiations.
CRM12	The Contractor's CRM tool shall have the ability to utilize CTI to auto-populate CRM screens with caller's basic information and access to contact history.	A key feature of our integrated solution is provided through Computer Telephony Integration (CTI). Once the caller has been authenticated, CSRs are automatically presented with the caller's information and complete call record on their computer screen through CTI, also known as "screen-pop" capability.
CRM13	The Contractor's CRM tool shall have the ability to navigate from or between CRM screens to other data relevant to the call within the Provider Services module allowing multiple screens to display at one time.	Our solution has multi-screen capabilities that allows CSRs to navigate between multiples screens to view all data relevant to the caller.
CRM14	The Contractor's CRM tool shall have the ability to store the caller's preferred method of communication, including need for deaf or foreign language interpretation.	MAXIMUS will work with the State staff during implementation to design detailed policies, procedures, and business rules for data collection, including building fields for documenting detailed call information and a field for storing the caller's preferred method of communication.
CRM15	The Contractor's CRM tool shall allow users to view related correspondence records from a single correspondence record.	The MAXIMUS Provider Services solution automatically records and links every call, email received, every message sent by text or email, every web chat conversation, and every received or generated piece of written correspondence to create a full and detailed record of the caller's contact history.
CRM16	The Contractor's CRM tool shall have the ability to upload or associate attachments to correspondence records.	Hyland OnBase provides enterprise content management of records, forms, correspondence, operational reports and policy and procedures by converting all documents to searchable PDF files and storing them in a document repository that is linked to our solution. These documents are tagged with the Provider ID, which automatically links them with the appropriate Provider record, enabling users to search not only the complete index criteria of the documents, but also the information contained within the document.
CRM17	The Contractor's CRM tool shall have the ability to present the contacts authorized to perform business functions with the State's healthcare programs on behalf of the provider or entity.	MAXIMUS understands that Providers often utilize authorized contacts to conduct business on their behalf. Therefore, authorized contacts capability is native to our purpose-built Medicaid application.
CRM18	The Contractor's CRM tool shall have the ability to accommodate searches on call center records by characteristics such as call type, category, CRM number, name of provider, provider number, contact name, other entity names, service authorization number, category of service, user ID, and any combinations thereof.	Our solution is a web-based, Java script platform that allows users to display, search, and update call records by call type, API or NPI number, inquirer's name, representative ID or name, Provider name or number, service category, CRM number, service authorization number, and other metadata fields that are native to the application.

3.10.14.4 Provider Call Center

3.10.14.4 Provider Call Center

This section outlines the requirements for a Provider Call Center. The Offeror's proposed Option B services must include a provider call center for new and revalidation applications and enrollments. The Contractor will also provide enrollment support for providers during the enrollment process. Typically, this support includes responding to provider's questions about

their responses to the application questions. The base provider solution will include context sensitive help throughout the enrollment process, which is intended to reduce the number of help desk solicitations. In addition to fielding questions related to enrollment and re-enrollment, the Contractor will also be responsible for additional activities (e.g., fielding questions related to changes in provider information, financial information, provider suspension for administrative reasons, or for other reasons such as IRS "B" Notices). The Offeror must describe their approach to meet each of the Provider Call Center requirements defined in Attachment F, Requirements Matrix.

Provider Call Center Overview

MAXIMUS supports nearly 100 health and human services contact centers throughout the United States. Our shared operations environment supports over 2,000 agents across all US time zones, allowing us to meet the volume demands, capability requirements, and financial data entry requirements of this contract. Our call centers leverage our Cisco UCCE platforms and integrated technology solutions to support designated projects.

We understand the importance of not only meeting performance requirements, but also providing high-quality call center services. Our call centers provide QA/QC staff, trained and experienced supervisors to support staff based on defined rations, and the necessary training environment to ensure our CSRs are prepared to respond to the full spectrum of questions regarding the Provider enrollment and verification process, including the financial enrollment process into the State financial system.

Our centers are located in competitively priced real estate and labor markets in order to provide cost-effective value to our clients. Our sites are redundant to one another to ensure that regional outages automatically roll to other centers, assuring continuity of operations.

Support for Litigation and Investigation

We understand the support the State may need from MAXIMUS in the event of potential litigation and investigation actions in the form of supplying data, providing audit trails, or testifying in depositions or in court. MAXIMUS trains our staff regarding the sensitivity surrounding any potential litigation and expects staff to respond to requests for support in a timely and professional manner.

Our solution maintains data for an indefinite period and is easily retrievable in the form of an ad hoc query within the parameters defined by the State. We work with our State partners in defining precisely the goal of the data inquiry to ensure it is meets the intent of the request and supplies the report within the appropriate context as relevant to the litigation or investigation. Understanding the basis for the request is the first step in defining the report or audit trail parameters so that we can respond accordingly.

In addition to supplying data or reports, MAXIMUS analysts will be made available as needed to provide testimony or explanations of applicable data or functionality. In complex investigations, programming staff or operations leadership may be needed to provide details on reports and data. We work with our State partners to the extent required and requested in supplying all needed data and analysts for litigation or investigation requests.

The business processes within our solution can be easily adapted to the State's policies and procedures pertaining to a Provider's right to appeal a decision to deny or terminate enrollment. We will use a combination of people, processes, and technology to support the State in the administration of appeals related to adverse findings. Our approach is to rely on trained staff and the advanced screening capabilities of our solution to reduce the number of appeals that are likely to occur. Project support for the

State's appeals process will include preparing and presenting testimony and exhibits, as well as providing witnesses if required to support an adverse decision against a Provider's enrollment.

In the case of a denial or termination, our solution prompts staff to select the reason for the denial or termination from a drop-down window and generate a notification that includes a dynamically created message specific to the denial/termination reason selected. The notification will inform the Provider of the option to initiate the appeals process, if he or she so desires.

Our in-place business processes helps mitigate the need for appeals by allowing our staff to work with Providers to resolve discrepancies encountered during the screening and enrollment process. Providers can submit any requested additional information or clarifications prior to the State taking any adverse action, giving them a better understanding of the screening and enrollment process and reducing the need to file an appeal in the first place. Nonetheless, our solution has the functionality needed to support a full appeal process that is consistent with State and CMS guidelines.

The appeal process begins with a Provider electing to file an appeal if enrollment in the State's Medicaid program is denied or terminated. Once the appeal is filed, our solution automatically sends a confirmation email to the Provider acknowledging the receipt of the appeal, and all communications are logged in the Provider's contact/note log. The system places any appeal received into the Appeals work queue and generates an email alert to the appropriate staff member. Workflow rules in our solution can be configured to refer the appeal to other staff specialists such as licensing, Medicaid, or legal staff, as needed.

After the appropriate review, the staff member will upload copies of any decision documentation. If the Provider is determined to be eligible for enrollment into the Medicaid program, our solution generates an email notification to the Provider and places the Provider information back into the normal work queue for the enrollment process to be completed. If the Provider is determined to be ineligible for enrollment, the staff member will upload the decision documentation, and the enrollment is denied. Our solution maintains a record of all documentation associated with the appeal.

MAXIMUS will provide experienced, knowledgeable, and qualified staff to support the State in litigation depending on the nature of the need. We understand the sensitive nature of any litigation and will train staff on discretion, appropriate behavior, and the importance of maintaining confidentiality throughout the litigation and investigation process.

MAXIMUS will provide necessary support as required by the State during litigation and administrative hearing activities, including assisting the State in the due diligence required for discovery obligations that arise in litigation. If the State instructs, MAXIMUS will assist the State in litigation document retention.

We have designed our solution to store indefinitely all Provider enrollment application, revalidation, and enrollment update data. Communication with providers is captured in the provider record, including emails, reports, files, copies, and other documentation needed by the State other entities to support prosecution or defense of lawsuits. These records are stored and made accessible during litigation.

Provider Call Center Requirements

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

ID	Provider Call Center Requirement	MAXIMUS Summarized Response
PRCC01	The Contractor shall provide a provider enrollment Call Center to support and instruct providers in the application process, renewal process, provider management, and recertification process. The Call Center shall also support the financial enrollment process into the State financial system.	MAXIMUS supports contact center environments throughout the United States. Our shared operations environment supports over 2,000 agents across all US time zones, allowing us to meet the volume demands, capability requirements, and financial data entry requirements of this contract. Our call centers leverage our Cisco UCCE platforms and integrated technology solutions to support designated projects. We understand the importance of not only meeting performance requirements, but also providing high-quality call center support. Our call centers provide QA/QC staff, trained and experienced supervisors to support staff based on defined rations, and the necessary training environment to ensure our CSRs are prepared to respond to the full spectrum of questions regarding the Provider enrollment and verification process, including the financial enrollment process into the State financial system. Our centers are located in economically beneficial locations to provide value to our clients and are redundant to one another to ensure that regional outages automatically roll to the next center to provide continuity of operations.
PRCC02	The Contractor shall research and provide documentation for administrative hearings, appeals and court cases; and participate in these activities upon direction from the State.	MAXIMUS staff will support the State in providing the necessary research and data for administrative hearings, appeals, and court cases. We will participate to the extent requested by the State.

3.10.14.5 Interactive Voice Response System

3.10.14.5 Interactive Voice Response System

This section outlines the requirements for an Interactive Voice Response System. The Offeror's proposed Option B solution shall include an Interactive Voice Response (IVR) System in order to welcome and route incoming provider calls; convey educational alerts during hold times; and intelligently queue providers until Contractor staff is available. The IVR system will include the ability for the provider to leave a message, during or outside, normal business hours. The Offeror must describe their approach to meet each of the Interactive Voice Response System requirements defined in Attachment F, Requirements Matrix.

The MAXIMUS Provider Services solution is fully integrated with our proven Cisco Enterprise IVR/ACD telephony system, which includes a toll-free number, outbound dialer, voicemail, call and screen recording for quality monitoring, and the automated customer satisfaction survey. This infrastructure is hosted in our premier MAXIMUS data centers in Englewood, Colorado, and Culpeper, Virginia, and includes significant back up and redundancy to prevent technical slowdowns or outages.

MAXIMUS will work with the State to develop customized educational scripts designed to provide callers with automated options for obtaining information pertaining to their specific needs.

Our Cisco Enterprise telephony system enables call recording to monitor inbound and outbound calls, as well as screen recording to monitor data entry activity in all systems. To continuously improve call center services, we review all recordings to assess customer service skills and the accuracy of information provided to consumers. Data entry is monitored by our Quality Specialists, who check to see that the CSR answered questions accurately and entered case notes correctly into the appropriate system. These reviews help us to identify staff who may be candidates for additional education or coaching.

Interactive Voice Response System Requirements

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

ID	Interactive Voice Response System Requirement	MAXIMUS Summarized Response
IVR01	The Contractor shall provide and maintain secure and user friendly interactive voice response (IVR) system with scripts approved by the State to respond to inquiries using a telephone menu and response system.	Our solution is fully integrated with our proven Cisco Enterprise IVR/ACD secure telephony system, which includes the outbound dialer, call and screen recording for quality monitoring, and the automated customer satisfaction survey.
IVR02	The Contractor's IVR system shall have the ability to use educational scripts for callers on hold or waiting in the queue.	MAXIMUS will work with the State to develop customized educational scripts designed to provide callers with automated options for obtaining information pertaining to their specific needs.
IVR03	The Contractor's IVR system shall provide quality monitoring tools and processes to enable a continuous improvement cycle for toll-free call center services that includes: a. Plug-in/double-jack monitoring, b. Silent monitoring, c. Record and review, d. Voice and screen/multi-media monitoring, for call center supervisors, State resources or designated resources.	Our Cisco Enterprise telephony system enables call recording to monitor inbound and outbound calls, as well as screen recording to monitor data entry activity within the MAXIMUS solution. To continuously improve call center services, we review all recordings to assess customer service skills and the accuracy of information provided to consumers. Data entry is monitored by our Quality Specialists, who check to see that the CSR answered questions accurately and entered case notes correctly into the appropriate system. These reviews help us to identify staff who may be candidates for additional education or coaching.

3.10.14.6 Staffing

> 3.10.14.6 Staffing
>
> This section addresses requirements for Provider Call Center staffing. The Offeror's proposed Option B services must include staffing to review provider information, maintenance requests and all supporting materials, in order to verify provider changes, prior to updating the provider records. The Contractor will review and approve or deny low risk, high volume enrollments per Agency criteria. Moderate and high-risk enrollments will be routed to and reviewed by Agency internal staff before a final enrollment decision is made. The Offeror must describe their approach to meet each of the staffing requirements defined in Attachment F, Requirements Matrix.

By applying our experience optimizing staffing levels on similar statewide operations contracts, we have developed a dynamic staffing model to meet the Option B requirements which allows us meet and exceed operational performance requirements. Our CSRs will be fully trained in all steps of the Provider screening and enrollment workflow, from application receipt to post-enrollment site visits. Our dedicated Capacity Planner and Workforce Management Analyst will update this model continuously to optimize staffing levels and balance capacity in the call center.

Within our call center, we have staff members who are trained and competent at completing a myriad of similar call center tasks. The call center has the capacity to accommodate the base level and future surge of staff members to support the State project. MAXIMUS has expertise in predicting surge and seasonality requirements, training and staffing the facility to meet increased demand, and then returning to base levels. For over 20 years, our call center has continued to refine its forecasting capabilities and delivery.

MAXIMUS uses custom-tuned algorithms to develop forecasts to model how many staff members they need to hire to support each project during base and surge events. We continually refine the approach and model a staffing plan as we receive additional transaction volume data to refine and scale our staffing accordingly on an ongoing basis for the duration of the contract. Our staff-forecasting model informs workforce planning, operations, training, and recruitment efforts across all operational areas. The model projects future staffing needs by department based on current and historical workloads and call volumes, i.e. total Call Center volume, average call wait time, rate of abandoned calls, and length of call, open

versus closed trouble tickets. Using these projections, our MT project team and local staffing partners can begin recruitment efforts for identified resource needs, with ample lead-time to supply a full class of screened, qualified employees on the target start date. They monitor the staff-forecasting model regularly to plan for upcoming needs and communicate those needs to staffing partner agencies accordingly. Their flexible staffing model illustrates that the MT project will be fully and effectively staffed, thereby maximizing efficiency and cost savings.

Leveraging our understanding of the MT process and our operations research capabilities, MAXIMUS has developed and initiated an integrated staff planning process as part of our approach to the Provider Services program, as explained previously. We will refine this approach with the State during the DDI phase. The goal of this process is to support an optimized staffing approach, in which the right number of staff come on board when needed, to support program needs. This process uses current and historical data both from the State and from our other projects involving Provider screening and enrollment volumes, performance metrics, contract requirements, and training constraints as inputs to simulation models, which use various types of analyses to produce staff and training projections.

Key Personnel

MAXIMUS will designate one in-state Site Visit Specialist and one additional Site Visit Specialist, who will assist the in-state Site Visit Specialist with site visit coordination and conduct all out-of-state site visit telephonic verification to ensure all SLAs are met per State guidelines. Our Site Visit Specialists will evaluate Provider locations based on the State participatory criteria and work with project staff to prepare materials for Provider site visit reviews. They will also assist with preparing materials to enable project staff to reach a final disposition.

In addition to the Site Visit Specialists and project staff, MAXIMUS has designated a Business Operations Manager to lead overall project operations for Provider screening, enrollment, and monitoring. Specific duties include:

- Establishing goals and objectives that support overall strategies to meet contractual requirements
- Directing and coordinating Provider screening and enrollment operations
- Improving performance, productivity, and efficiency through implementation of best practices
- Managing direct reports
- Planning, developing, and scheduling priorities for achieving goals and contractual requirements
- Reviewing and approving call center productivity and ensuring the review and screening of Provider applications are completed within the timeframe specified in the contract
- Reviewing results of forecasts and modeling exercises to provide direction and guidance
- Assisting the Project Manager in setting and managing the overall strategic and financial direction of the department
- Directly managing call center team supervisors
- Overseeing Customer Service Representatives (CSRs) and managing call center performance ensure to service level agreements are met
- Reviewing and monitoring compliance with guidelines, procedures, rules, and regulations

Staffing Requirements

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

ID	Staffing Requirement	MAXIMUS Summarized Response
STF01	The Contractor shall provide staffing to perform provider enrollment tasks defined by the Agency to include at a minimum: -Receive, review and verify provider information submitted to the screening process; -Verify provider data against Provider databases and the NPPES; -Notify providers to request additional documentation as needed; -Determine provider status; -Update provider record with all necessary enrollment data; -Process and store provider agreements; -Send financial enrollment data to State's financial system; -Activate provider enrollment for benefits/claims transactions in the Benefits Management system; -Review provider information maintenance requests and all supporting materials; and -Verify provider changes prior to updating the provider records. Staffing levels shall be maintained to meet enrollment process SLA's for timeliness and accuracy.	By applying our experience optimizing staffing levels on similar statewide operations contracts, we developed a dynamic staffing model for the Option B requirements that helps us meet and exceed operational performance requirements. Our CSRs will be fully trained in all steps of the Provider screening and enrollment workflow, from application receipt to post-enrollment site visits. Our dedicated Capacity Planner and Workforce Management Analyst will update this model continuously to optimize staffing levels and balance capacity in the call center.
STF02	The Contractor shall provide Provider Enrollment Call Center staffing sufficient to maintain services that meet or exceed the Service Level Agreements for the Call Center productivity. The Contractor shall describe its staffing model that includes the ratio of staffing to Call Center operation volume (including, for example: total Call Center volume, average call wait time, rate of abandoned calls, length of call, open vs. closed trouble tickets).	MAXIMUS proven successful provider operations have given us the experience needed to forecast staffing needs to successfully meet and exceed the Service level agreements. We take pride in delivering best practices and our operations staffing model is based on volume and productivity as well as consider attrition that may occur at any given time. MAXIMUS uses custom-tuned algorithms to develop forecasts to model how many staff members they need to hire to support each project during base and surge events. We continually refine the approach and model a staffing plan as we receive additional transaction volume data to refine and scale our staffing accordingly on an ongoing basis for the duration of the contract. Our staff-forecasting model informs workforce planning, operations, training, and recruitment efforts across all operational areas. The model projects future staffing needs by department based on current and historical workloads and call volumes, i.e. total Call Center volume, average call wait time, rate of abandoned calls, and length of call, open vs. closed trouble tickets. Using these projections, our MT project team and local staffing partners can begin recruitment efforts for identified resource needs, with ample lead-time to supply a full class of screened, qualified employees on the target start date. They monitor the staff-forecasting model regularly to plan for upcoming needs and communicate those needs to staffing partner agencies accordingly. Their flexible staffing model illustrates that the MT project will be fully and effectively staffed, thereby maximizing efficiency and cost savings.

ID	Staffing Requirement	MAXIMUS Summarized Response
STF03	The Contractor shall designate at least one (1) in-state staff position to conduct site visits. This position is considered to be a key staff position. Other staff will need to be available as necessary to meet SLAs for site visits. Please describe how you can meet the requirement with at least two (2) staff positions for site visit coordination.	MAXIMUS will designate one in-state Site Visit Specialist and one additional Site Visit Specialist who will assist the in-state Site Visit Specialist with site visit coordination, as well as conduct all out of state telephonic verification to ensure all SLAs are met. Our Site Visit Specialists will evaluate Provider locations based on the State participatory criteria and work with project staff to prepare materials for Provider site visit reviews. They will also assist with preparing materials to enable project staff to reach a final disposition.
STF04	The Contractor shall designate a Business Operations Manager to lead the Contractor's Business Operations for Provider Screening, Enrollment and Monitoring, including: -Document Management and Workflow Performance -Provider Data Management -Provider Support Services (training and site visits) -Provider Enrollment Call Center -Financial Enrollment Process coordination with State Auditor's Office (SAO) This position is considered to be a key specific management position.	In addition to the Site Visit Specialists and technical project staff, MAXIMUS will designate a Business Operations Manager, to lead overall project operations for Provider screening, enrollment, and monitoring of all provider services and state Service Level Agreements.

Based on the above requirement (STF04) for our Business Operations Manager to lead Provider Support Services including training, we will develop and conduct training related to the following Option B Training requirements.

ID	Option B Training Requirement	MAXIMUS Summarized Response
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	MAXIMUS Operations will work closely with Technical System team to develop a train-the-trainer process that allows the training manager to be ready to train and work closely with all users to ensure they are fully prepared to navigate the web-portal system and learn all functionality pertaining to their user roles.
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.	The MAXIMUS Training manager will work closely with Technical System team to develop all training materials during UAT to ensure that the provider community is fully prepared to navigate the web-portal system and submit their application.

3.10.14.7 Collect and Enter Provider Financial Information in State Financial Systems

> 3.10.14.7 Collect and Enter Provider Financial Information in State Financial Systems
> This section outlines the requirements for the collection of provider financial information and data entry requirements into the State's financial system. The Offeror's proposed Option B services must include the services to support the collection of financial packet/information from providers and enter the information into a state financial system. The Contractor services will include following up with the provider in the event discrepancies are identified by State auditors. Activities would also entail subsequent work from the provider's submission of initial financial information and includes essential updates to financial information. The Offeror must describe their approach to meet each of the requirements to collect and enter provider financial information in state financial systems defined in Attachment F, Requirements Matrix.

MAXIMUS will work with the State to resolve all TIN Mismatch Reports using State-provided reports in concert with data captured in our PDM solution, as well as other ancillary reference sources, as required. Leveraging mutually agreed upon procedures, we will contact Providers who have been identified as

having discrepancies, collect the most accurate, current financial information, and enter all corrections in the State systems.

Financial Information Management Requirements

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

ID	Financial Information Management Requirement	MAXIMUS Summarized Response
SFMS01	The Contractor shall research and resolve all TIN Mismatch Reports which show all Tax ID's that have returned a mismatch error from the TIN Matching process.	MAXIMUS will work with the State to resolve all TIN Mismatch Reports using State-provided reports.
SFMS02	The Contractor's staff will follow-up with providers regarding any discrepancies identified by the state auditor and the IRS regarding Backup Withholding "B" notices, 1099s, including FEINs. Enter any corrections needed in the applicable state financial system.	Using State-provider reports and other data sources, we will contact Providers who have been identified as having discrepancies, collect the required information, and enter all corrections in the State systems as required.

Interfaces

The following table includes our response for this requirement.

ID	Financial Information Management Requirement	MAXIMUS Summarized Response
INR13	The Contractor shall provide an extract of Agency defined data to the Agency data warehouse, at a minimum, weekly.	MAXIMUS will work with the state to create custom extract with State identified data elements. The extract will be sent to the State's data warehouse using Secure FTP or other file transfer protocols supported by the Agency.

3.10.14.8 Option B Performance Requirements

> 3.10.14.8 Option B Performance Requirements
>
> This section outlines the service level agreement requirements for Option B services. The Contractor shall detail in their response their approach to meet each of the Performance Requirements defined in Attachment F, Requirements Matrix. SLAs are also found separately in Attachment J, Service Level Agreements.

MAXIMUS will leverage our extensive expertise managing Provider operations, best practices, and lessons learned to ensure we meet all SLAs as defined by the State.

Option B Performance Requirements

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

ID	Option B Performance Requirement	MAXIMUS Summarized Response
SLA70	Contractor shall ensure that the Agency-defined data extract is supplied accurately to the Data Warehouse. The Contractor shall supply the response file(s) in the format requested by the Agency by the date and time (weekly) agreed upon.	MAXIMUS confirms that the Agency-defined data extract will be supplied accurately to the Data Warehouse in the format and standards requested by the Agency.
SLA71	Contractor shall staff the provider enrollment Call Center toll-free phone lines from 8:00 a.m. to 5:00 p.m., Mountain Time, on all State business days, Monday through Friday (excluding State holidays). The Contractor shall generate a report which includes, at a minimum, the time and date stamp phone lines were open and when phone lines were turned off.	Our Cisco UCCE telephony platform provides out-of-the box reporting on call availability, including time stamps for calls offered and received, as well as reports on overall call center availability and time stamps indicating live call center operational times. The contact center will be staffed and open for live call responses between 8am and 5pm MST, Monday through Friday (excluding State and Federal Holidays).

ID	Option B Performance Requirement	MAXIMUS Summarized Response
SLA72	Contractor shall respond to telephone and written inquiries with a researched response, or with an accurate resolution to the inquiry within two (2) business days. This SLA covers the 25% of telephone inquiries that are not able to be resolved during first contact. The Contractor shall generate a report to track request date against the response date. The Agency will perform monitoring of the accuracy and consider document availability factors.	MAXIMUS commits to responding to telephone and written inquiries with a researched response, or with an accurate resolution to the inquiry, within two (2) business days. Telephone-based calls and written inquiries that are not a function of the 75% first call resolution will be dispositioned to a research queue in our solution. The queue settings tag the task and initiate a countdown on the due date for a response. The research queues prioritize tasks according to their approaching deadlines to ensure the required SLAs are met. As due dates approach, our solution for Business Intelligence reporting platform automatically flags the tasks and alerts supervisors that expedited work must be done to achieve the standard.
SLA73	Contractor shall respond to telephone and written inquiries with a researched response, or with an accurate resolution to the inquiry with at least ninety-seven percent (97%) accuracy. This SLA covers the 25% of telephone inquiries that are not able to be resolved during first contact. The Contractor shall generate a report to track request date against the response date. The Agency will perform monitoring of the accuracy and consider document availability factors.	Telephone-based calls and written inquiries that are not a function of the 75% first call resolution will be dispositioned to a research queue in our solution. The queue settings tag the task and initiate a countdown on the due date for a response. The research queues prioritize tasks according to their approaching deadlines to ensure the required SLAs are met. As due dates approach, our solution for Business Intelligence reporting platform automatically flags the tasks and alerts supervisors that expedited work must be done to achieve the standard. The completeness of the response is a function of our QA review. To achieve a 97% standard of accuracy, MAXIMUS will QA nearly 100% of all tasks for conformance. While this is a costly endeavor, the quality standards proposed by the State are high and necessary redundancy is required. Consistent with our approach to continuous quality improvement (CQI), exceptions to the timeliness of resolution and accuracy performance requirements will be reviewed for opportunities for refresher training, team meeting reminders, and support documentation refinement.
SLA74	Contractor shall process to completion all approved provider enrollment financial information documents into the applicable state financial system e.g., the Wyoming Online Financial System (WOLFS), with at least ninety-nine percent (99%) accuracy. The Agency will conduct monitoring of the accuracy of keyed financial information within the applicable financial system, e.g., WOLFS.	MAXIMUS commits to completing all approved provider enrollment financial information documents into the applicable state system with at least a 99% accuracy. Data entry is monitored by our Quality Specialists, who check to see that the CSR entered data correctly into the appropriate system.
SLA75	Contractor shall process to completion 100% of all approved provider enrollment financial information documents into the applicable state financial system e.g., the Wyoming Online Financial System (WOLFS), within two (2) business days of provider approval. The Contractor shall generate a report to track received financial information to process against actual processed documents.	MAXIMUS commits to completing 100% of all approved Provider enrollment financial documents into WOLFS, or other applicable state systems, within two business days of provider approval. Our solution will generate the necessary reports to track this information, which will be reviewed by a Supervisor or higher 100% of the time.
SLA76	Contractor shall ensure that less than one percent (1%) of total monthly calls should be escalated to the Agency for resolution that are clearly within the scope of work of the Contractor. This does not apply to subject areas where the Agency and the Contractor have agreed in advance require Agency determination. The Contractor shall track at a minimum: percentage of calls escalated to the Agency, reason for escalation, and outcome. This Operational Report will be provided to the Agency monthly.	The contact center staff will utilize call scripts based on policy and procedures agreed to with the State, which will articulate what is within the scope of the CSR. This information will be reinforced in remedial training and supervisor coaching. Any escalations to the State will require supervisor level approval, and all escalations to the state are subject to a quality review process so we can identify and correct gaps in the policy. Escalations will be tracked using our DecisionPoint for Business Intelligence (BI) reporting platform and provided to the Agency on a monthly basis.

ID	Option B Performance Requirement	MAXIMUS Summarized Response
SLA77	Contractor shall complete one hundred percent (100%) of all moderate and high risk provider pre- and post-enrollment onsite screenings within seven (7) business days. The Contractor shall generate a report to track moderate and high risk providers ready for a site visit against the number of site visits actually performed within the seven (7) business day window.	MAXIMUS commits to completing 100% of all moderate-and high-risk Provider pre- and post-enrollment onsite screenings within seven business days. We will use our DecisionPoint BI reporting platform to track our performance against this SLA.
SLA78	Contractor shall ensure the onsite screening checklist will be completed and keyed into the applicable provider profile within the solution with ninety-seven percent (97%) accuracy. The Agency will perform monitoring of the accuracy of entry and completeness of the checklist.	MAXIMUS commits to completing and entering the on-site screening checklist into PDM with a 97% accuracy.
SLA80	Contractor shall ensure researched and resolved TIN Mismatch Reports will be corrected in the solution with ninety-nine percent (99%) accuracy. The Contractor shall generate a report to track resolved provider TIN against the original TIN mismatched report. The report will include time and date stamps.	MAXIMUS commits to researching and resolving all TIN Mismatch Reports with 97% accuracy, Using our DecisionPoint BI reporting platform, we will generate reports to track these resolutions according to the requirements of the State.
SLA81	Contractor shall ensure the total number of busy signals, disconnected calls, and abandoned calls measured against the total inbound calls shall not exceed five percent (5%) per day. The Contractor shall generate a report to track all inbound calls against answered calls, including abandonment rate, hold time before initial answer, time placed on hold after call is answered, average talk time, and speed to answer--at a minimum, and for each phone line	Our IVR provides near 100% availability so callers should never experience a busy signal. By virtue of our VOIP infrastructure and enterprise model, MAXIMUS maintains more than enough capacity to support the ongoing requirement for the State. MAXIMUS commits to a 5% or less per day for busy signals, disconnected calls, and abandoned calls. MAXIMUS will provide the State reporting on inbound calls, calls offered (answered), abandonment rate, and average talk time and speed to answer, as well as hold time for each skill set in the center. Our Cisco UCCE reports to this level out of the box and our DecisionPoint BI reporting platform offers the analysis and visualization layer for consumer facing reports.
SLA82	Contractor shall ensure the average speed to answer must be less than or equal to sixty (60) seconds, after the caller makes a selection in the IVR. The Contractor shall generate a report to track all inbound calls against answered calls, including abandonment rate, hold time before initial answer, time placed on hold after call is answered, average talk time, and speed to answer--at a minimum, and for each phone line.	MAXIMUS commits to an Average Speed of Answer (ASA) of 60 seconds or less, and will provide the State reporting on inbound calls, calls offered (answered), abandonment rate, and average talk time and speed to answer, as well as hold time for each skill set in the center. Our Cisco UCCE reports to this level out of the box and our DecisionPoint BI reporting platform offers the analysis and visualization layer for consumer facing reports.
SLA83	Contractor shall be able to pull specific phone call recordings (inbound and outbound calls) when given the date and time, and provide them to the Agency upon request.	MAXIMUS associates call recordings agents who support the calls. If the State knows the agent who fielded the call and/or the time and date that the call occurred, specific calls can be pulled from the database, which will be provided to the Agency upon request.
SLA84	Contractor shall ensure provider questions and concerns are resolved seventy-five percent (75%) of the time upon first contact with the Call Center. The Contractor shall supply the metrics to the Agency, monthly (at a minimum) to demonstrate first call resolution.	MAXIMUS prides ourselves on first call resolution standards. We train our CSRs to respond to the full spectrum of inquiries regarding the Provider enrollment process and are confident we can attain the 75% standard for first call resolution.
SLA85	Contractor's Call Center staff will document, in Customer Relationship Management (CRM) system, all the information they provide to callers during first contact, and any subsequent follow-ups, one hundred percent (100%) of the time. The Contractor shall make available to the Agency view access into the CRM (expected: three (3) view-only seats).	MAXIMUS is using our purpose built system for the CRM requirements of this bid. Our solution provides fields for tracking consumer meta data such as name (first and last), DOB, call type, phone number calling from, preferred phone number, email, language preference, call reason, time stamps, record ID, Staff ID, customer ID, and call notes. Each call is logged and case notes filed with full view audit history to the Agency.

ID	Option B Performance Requirement	MAXIMUS Summarized Response
SLA86	Contractor shall survey no less than every 10th caller to rate the quality, timeliness, and other service delivery elements carried out by the Call Center. Callers shall report Call Center satisfaction at or above eighty percent (80%). The Contractor shall combine caller satisfaction scores to determine the average satisfaction percentage score. Score and surveys will be provided to the Agency, monthly.	MAXIMUS conducts a post-call survey in the IVR, which is an efficient and cost-effective way of gathering valuable feedback from consumers. Consumer responses are documented and provided to management and the Agency, on a monthly basis for review and analysis. The results are also incorporated into continuous improvement of our service delivery. MAXIMUS will offer the survey to 100% of callers and are confident we can attain a 10% response rate.
SLA87	Contractor's staff will perform provider enrollment duties including, but not limited to tasks within requirement STF01. Duties and tasks will be completed with ninety-seven percent (97%) accuracy. The Contractor shall generate a workflow report that tracks tasks and duties against completed work. Report will be provided to the Agency, monthly. The Agency will perform monitoring for accuracy of completed tasks.	MAXIMUS commits to ensuring staff complete all required Provider enrollment duties with a 97% accuracy. Using our reporting platform, we will generate a workflow report that tracks tasks and duties against completed work and will provide these reports to the Agency on a monthly basis. Quality control review will identify all errors and MAXIMUS will report those errors to the State. Consistent with our CQI approach, we will use those errors as opportunities for refresher training, team meeting reminders, and resource documentation refinement.
SLA88	Contractor's staff will perform provider enrollment duties including, but not limited to tasks within requirement SFT01. Duties and tasks will be completed within an average of two (2) business days and 100% completion of all tasks within five (5) business days unless specifically stated in a separate SLA. This applies to each period (e.g.: incomplete application returned to the provider). Factors outside of Contractor control, such as the response time by the provider to request for additional information, are not considered. The Contractor shall generate a workflow report that minimally tracks: task time-stamps (incoming and completed), tasks against completed work, average time to complete each task, and time taken by the provider to supply additional information or make corrections. Report will be provided to the Agency, monthly. The Agency will perform monitoring for timeliness and accuracy of completed tasks.	MAXIMUS commits to ensuring staff complete all required Provider enrollment duties within an average of 2 business days and 100% completion of all tasks within 5 business days unless specifically stated in a separate SLA. Using our DecisionPoint BI reporting platform, we will generate a workflow report that tracks task time-stamps (incoming and completed), tasks against completed work, average time to complete each task, and time taken by the provider to supply additional information or make corrections. These reports will be provided to the Agency on a monthly basis.
SLA89	Contractor shall ensure ninety-five percent (95%) of all incoming documents received, staff site visit documentation, and/or other applicable documentation must be scanned into the system within two (2) business days. The remaining five percent (5%) of documents must be scanned within five (5) business days. The Contractor shall generate a report to track all incoming documents. The report will include time and date stamps for when a document was received and when a document was scanned. The Contractor shall conduct internal quality checks on the documents scanned.	MAXIMUS agrees to this standard. Using our Hyland OnBase scanning and imaging solution MAXIMUS will scan 95% of all incoming documents received within 2 business days and the remaining 5% within five business days from receipt at the processing center. Hyland creates a digital image of the document and associates it with a case in the PDMS. We can report on inbound documents through our Decision Point for Business Intelligence platform to include the time and date stamps associated with each document received.
SLA90	Contractor shall staff the provider enrollment Call Center and maintain staff for site visits at the level agreed upon in the contract. Staffing includes all key and non-key staff. The Contractor and Agency shall agree to the number of FTE within the contract. A FTE is measured as two thousand and eighty (2,080) hours.	MAXIMUS uses advanced staff modeling and forecasting tools to simulate program operations. We are experts in the industry and staff our projects appropriately to both provide quality outcomes for consumers and cost effective delivery while using tax dollars. MAXIMUS will staff the operation to the appropriate levels based on the demand of the program, committing fully to the standards that determine successful contractual performance. While we do not commit to mandatory line staff levels due to the flexibility we require to meet operational needs, we do commit to all of the key staff provisions set forth in this requirement.

ID	Option B Performance Requirement	MAXIMUS Summarized Response
SLA91	Contractor will have forty-five (45) calendar days to fill an appropriate staff position or key staff position with a permanent resource even when a qualified substitute is in place. The Contractor shall notify the Agency when management and key positions are vacated, subsequently filled by a qualified replacement, and finally filled by qualified permanent staff.	MAXIMUS commits to filling staff and key staff positions with a permanent resource within 45 days. We will notify the Agency of any changes to management and key staff positions.
SLA92	Contractor's Call Center staff will notify the provider of discrepancies within one (1) business day of any discrepancies identified regarding the Backup Withholding "B" notices, 1099s, including FEINs. Staff will attempt to notify the provider via phone call. If the provider was not reached by phone, Call Center staff will perform a second attempt to rectify the discrepancy through email. Upon resolution, Call Center staff will correct the discrepancy within the applicable state financial system, such as the Wyoming Online Financial System (WOLFS), with ninety-nine percent (99%) accuracy within two (2) business days of receipt of the resolved discrepancy. The Contractor shall generate a workflow report that tracks tasks and duties associated with discrepancies identified by the SAO and IRS regarding Backup Withholding "B" Notices, 1099s, including FEINs, against completed work. Report will be provided to the Agency, monthly. The Agency will perform monitoring for accuracy and timeliness of completed tasks.	MAXIMUS will work with the State to resolve all TIN Mismatch Reports using State-provided reports and other data sources as required. Using these reports, we will contact Providers that have been identified as having discrepancies within 1 business day, with a follow-up attempt the second business day. Once he we collect the required information, we will enter all corrections in WOLFS or other States' systems with a 99% accuracy within 2 business days of resolving the discrepancy. Using our DecisionPoint BI reporting platform, we will generate a workflow report that tracks that tracks tasks and duties associated with discrepancies identified by the SAO and IRS regarding Backup Withholding "B" Notices, 1099s, including FEINs, against completed work. These reports will be provided to the Agency on a monthly basis.

3.10.15 Reporting

3.10.15 Reporting

This section addresses reporting requirements. The Contractor's solution shall provide an established library of standardized operational reports as well as the ability to create a wide array of configurable detail level and summary level reports, dashboards and queries. The Offeror must describe in their response their approach to meet the Reporting requirements defined in Attachment F, Requirements Matrix.

Efficiency

The MAXIMUS Provider Service Solution is packaged with an analytics and reporting platform. Our solution uses two COTS products: Microsoft SQL Server Reporting Services (SSRS) and MicroStrategy Business Intelligence engine. These two applications serve closely related purposes and play a very important role in Provider application processing. The solution contains interactive dashboards and an analytics platform. The reports in the MAXIMUS Provider Services Solution provide insight into the application data with data visualizations and reports. The reports provide for on demand sorting, filtering, and formatting of column values and headers. The reports can be run automatically, saved periodically, and purged per the user's need. MAXIMUS supports reports using pre-built defined parameters. This is done by using the parameterized queries supported by MicroStrategy.

At the core of our configurable reporting capabilities is the business intelligence suite implemented with MicroStrategy. The business intelligence suite provides authorized users with powerful reporting capabilities. The basis for the reporting functions is the database structures that store all information about the enrollment and screening process and the data about a provider and a uniquely defined reporting layer that makes standard and ad hoc reports easy to create and maintain. Our solution uses a combination of standard reports, dashboard reporting and online data to support the administration of the Provider management business area. These reporting processes provide operational and management users with all

required information about the overall enrollment status across the program as well as a more detailed status by Provider type, business flow and even individual Providers.

The output of all reporting functions is available online and allows for export into 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. As part of implementation planning, MAXIMUS produces and maintains an online report distribution list and schedule to reflect updated State decisions on format, media, and content, including distribution to other State-approved Trading Partners and State staff. The system allows for ad hoc query capability on Provider related data. The system also provides for on demand and batch reports that allow users to generate listings of Providers in various sort orders.

The reporting capabilities built into our solution allow us to design and configure all reports specified in the RFP and deliver them to the State on a schedule specified by the State. We will work with the State during the Gap Analysis sessions to configure the content and format for each required standard report, and we will update the current list of standard reports if changes occur prior to implementation.

Exhibit 3.10.15-1: MAXIMUS Approach for Reporting presents a high-level summary of our reporting approaches and methods and describes the benefits of our approach to the State.

Technical Factor	MAXIMUS Approaches and Methods	Benefits to the State
Batch Reporting	All standard reports required by the State can be batch-generated and available for viewing through the web portal	Project staff can access standard reports, dashboard reporting views, and online data to support project oversight and management
On Demand Reporting	Project and State staff will have online access to reports with flexible input parameters that allow users to request a specific report, view, and download the report in any desired format.	Real-time access to Provider screening and enrollment data by staff minimizes the need for ad hoc report requests
Ad Hoc Reporting	Our solution has flexible query capabilities to facilitate access to all data stored within the database system filters, comprehensive search capabilities, and export functionality enable ad hoc reports to be generated on demand. We also support dynamic capabilities for conducting queries of the Provider database and generating ad hoc reports	Once trained on the system's query and reporting capabilities, staff will be able to query the database and generate reports We will designate staff responsible for responding to State ad hoc report requests within required timeframes State staff will have the ability to access and query all Provider data in real time

Exhibit 3.10.15-1: MAXIMUS Approach for Reporting. *The MAXIMUS Provider Services Solution supports various reporting mechanisms according to the need.*

MAXIMUS will work with the State during the JAD sessions to develop the content, parameters, and format for each required standard report. The current list of standard reports is updated if changes occur prior to implementation.

3.10.15.1 Standardized Reports

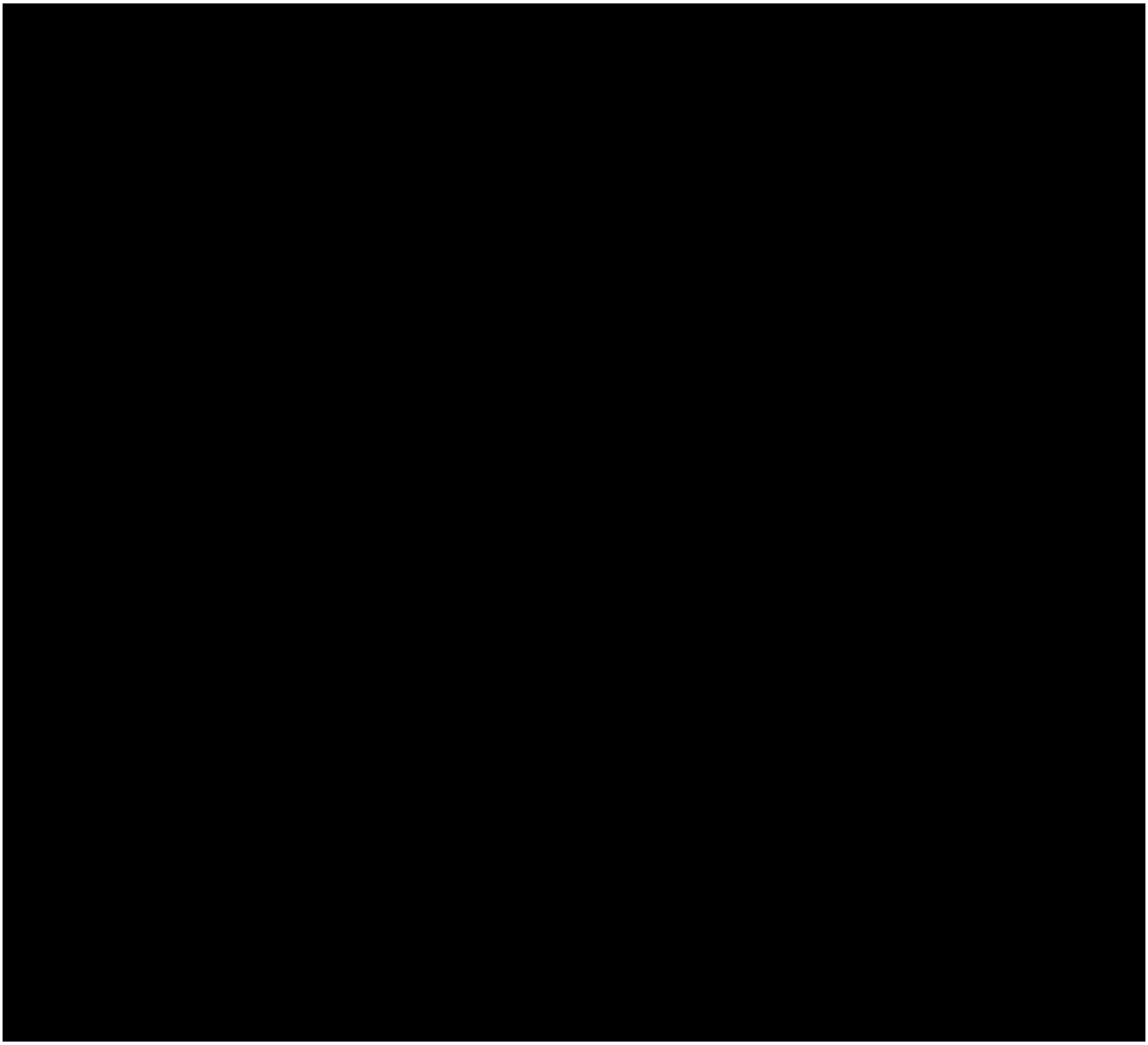
Exhibit 3.10.15.1-1: MAXIMUS Provider Services Solution Standard Reports lists the numerous standardized reports packaged within our Provider Services base solution. Existing reports are presented and verified, with changes documented during the design phase of the project. MAXIMUS works with the

State to identify the report parameters and relevant data elements that should be collected, parsed, and displayed on the resulting report. We are able to support a variety of customized reports based on program needs. Our solution has the flexibility to accommodate the exchange of data in any mechanism the State prefers. Our Open Interface Framework module (discussed in *Section 3.10.1–Architecture*) will allow for the import and export of the data in any file exchange protocol preferred by the State. We also provide on demand reports for authorized users to 'pull' required data from our solution in real time using the on demand reporting function. The search and display capabilities produce accurate, complete, timely data and information.

Agency executives with an authorized user role are able to login to the system and view the system dashboard as their homepage. The dashboard presents a real-time view at an aggregate level of the status of all Providers in the system and allows the user to drill down to view details for each Provider. Users are able to export report results into a variety of formats, including excel and PDF, as well as data options based on State-approved access that are easily configurable by State-authorized end users to accommodate future needs.

MAXIMUS understands the changing nature of business and information needs and that standardized reports may need to be modified periodically. We will promptly respond to requests for changes from the State or other State-approved Trading Partners. Any changes to standardized reports are made utilizing the established change control process. Required reports are available to the State online for viewing or printing, and we can integrate our solution with external workflow products to automatically forward reports to authorized State staff.

CONFIDENTIAL



In addition to the standard reports already existing within our solution, MAXIMUS understands the requirements for additional reports as listed in the RFP that need to be developed. Many reports listed already exist in the solution and MAXIMUS is able to leverage existing reports to satisfy the requirements for additional reports.

3.10.15.2 Batch Reporting

As part of the design phase, MAXIMUS works with the State to identify reports that should be created on a scheduled basis and automatically forwarded to State staff. We provide these batch reports on a State-approved schedule throughout the support period of the contract, as deemed necessary by the State. The standard reports that are included in our solution provide the basis for reporting that is dependent on daily processing. We work with the State during the design phase to review the batch reporting requirements in conjunction with our existing reports to determine what information should be included in the batch

CONFIDENTIAL

reporting. We will develop additional reports as specified in the RFP in a format that is agreeable to the State. Reports that are approved by the State in the design phase are included in our batch reporting process during the support period.

Our Provider Services module is designed to minimize the need for batch reporting and paper reports. Real-time access to Provider screening and enrollment data, including the ability to review all Provider data received by the project, the history of data changes, application fee data, and any documentation associated with the enrollment or revalidation of Medicaid Providers is accessible to State users through the portal. We work with the State to accommodate any requests for batch reports. However, we believe our online reporting capabilities offer a more effective and efficient means to access the most up-to-date Provider data and may replace the need for many of the batch reporting requirements.

3.10.15.3 Online Reporting

The vast majority of the reporting capabilities of our Provider Services module are designed to make data accessible to the State through real-time dashboards and other online reporting functions. Through these online processes, MAXIMUS project staff members, as well as designated State representatives, have ready access to up-to-the-minute information on all program data including a summary of all registrations in the system, regardless of status. Users are able to view the status of new applications and initial/ongoing revalidations, and the dashboard displays the aging of each application based on the workflow step or status of the application.

Our Solution provides an intuitive interface that enables all users to query and retrieve data on a variety of selection criteria.

Summary information on the total number of applications is displayed along with the totals for each of the work queues. Queue aging columns included on the dashboard provide additional information on the applications in the various queues, including the length an application or revalidation has been in a queue. *Exhibit 3.10.15.3-1: MAXIMUS Provider Services Solution Dashboard* shows a section of one of the many available dashboards in our solution.

CONFIDENTIAL

Counts reflected in the dashboard function as hyperlinks; users are able to click on the links for each count in the dashboard to drill down and view details of the Provider. The dashboard is fully configurable, and we will customize the application status descriptions to reflect those required for the State. The dashboard provides the State access to online reports that show required reporting elements, including:

- Work in queue
- Work completed by staff
- Aging statistics
- Status of each application and length of time in that status

By providing designated State users with direct access to data through online screens, we are able to minimize the number of ad hoc report requests since State users can readily view real-time Provider screening and enrollment data at any point in time. This includes the ability to review data received, the history of data changes, fee information, and any documentation associated with enrollment or revalidation. In addition, online filters and comprehensive search functionality enable authorized staff to

CONFIDENTIAL

customize the data views, and data can easily be exported to a variety of office automation products including Microsoft Office and Adobe software.

Our solution includes a data repository that supports data reporting required by DPHHS for analyzing program performance. All data obtained during all phases of the application, screening, and maintenance steps is stored indefinitely and is easily accessible by authorized users. Using the robust search capabilities, users are able to query data on a variety of search parameters and extract the information into Excel, PDF, or Word format to meet the specific needs of the State.

Exhibit 3.10.15.3-2: MAXIMUS Provider Services Solution Query Capabilities illustrates an example of the query capabilities in our solution that facilitate real-time online reporting as well as ad hoc reporting. It shows how the Provider selection screens provide a detailed look at program information as well as link directly to the Provider screening and enrollment workflow.

CONFIDENTIAL

The Provider Search screen can be sorted by any of the fields in the header row of the grid. At a glance a user can tell which Providers have been under review for the aging period selected, the date of their last status change, and the worker to which the review is assigned. The Provider Search screen is an excellent example of how online data can be used as an extremely powerful management and reporting tool.

3.10.15.4 Error Reporting

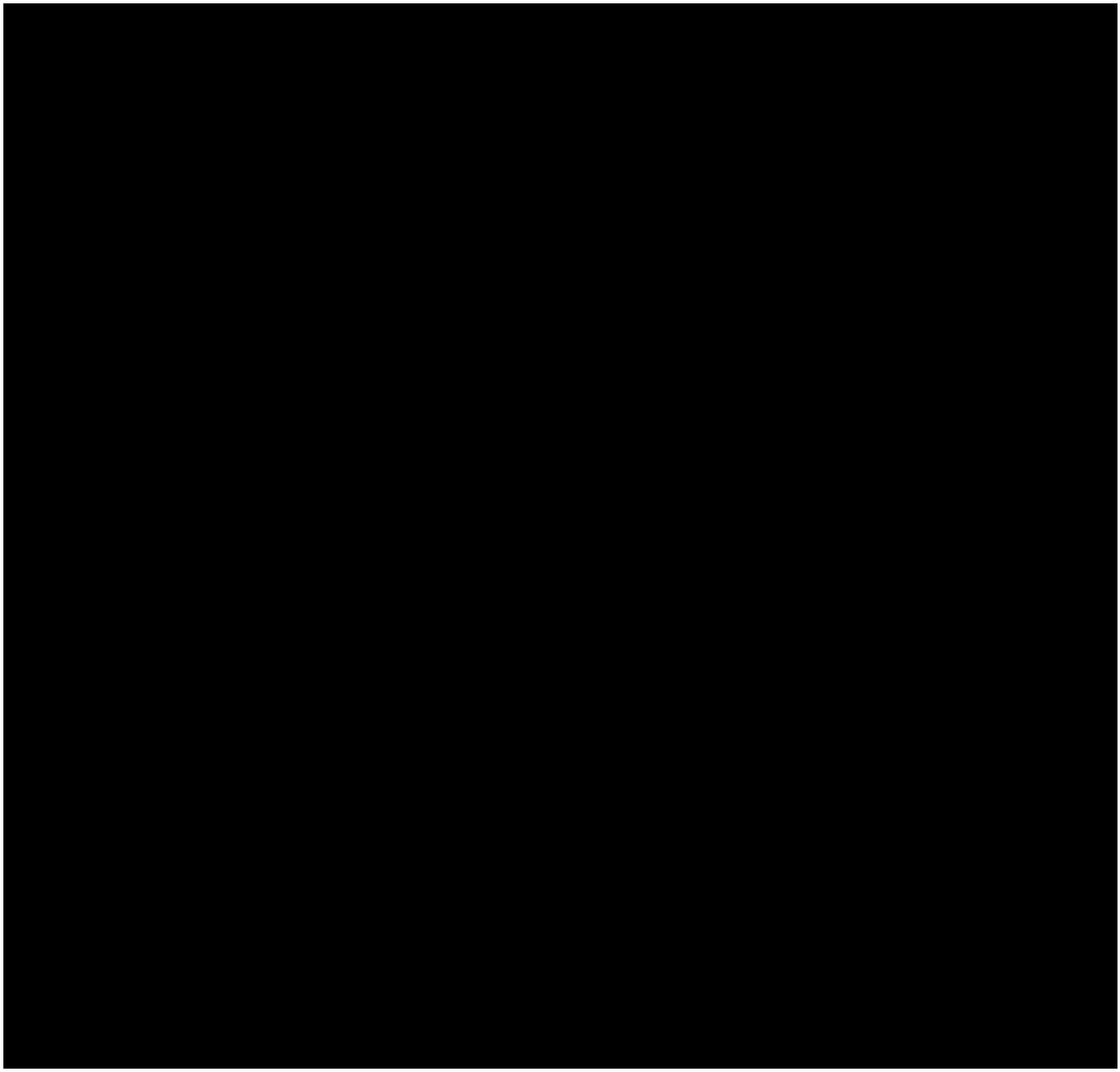
MAXIMUS is open and transparent in its error reporting procedures throughout all phases of the project and during the system support period. Our Provider Services Solution is packaged with several error reports that provide real time statistics on the status of key processes in the system. One notable example of our error reporting functions is shown in *Exhibit 3.10.15.4-1: MMIS Interface Management Report*.

CONFIDENTIAL

The MMIS Interface Management Report is an on demand report that authorized users are able to request via the web portal. We can also configure this report to be generated and sent automatically to a predefined set of users.

The MMIS Interface Management Report allows a user to view the status of the MMIS interface for a single day or over a period. The report provides a complete audit of all transactions sent to the MMIS and identifies any transactions that may be processed as an exception on the MMIS, per the rules defined for the MMIS interface. The status of each individual transaction (Provider) is tracked within the system and summarized in this report. During the daily procedure to process the responses received from the MMIS, out solution automatically notifies all appropriate users if there has been an exception in the processing of a Provider. The project support team is proactive in keeping the State and incumbent vendor apprised of all system exceptions and errors, and especially those associated with the MMIS interface.

CONFIDENTIAL

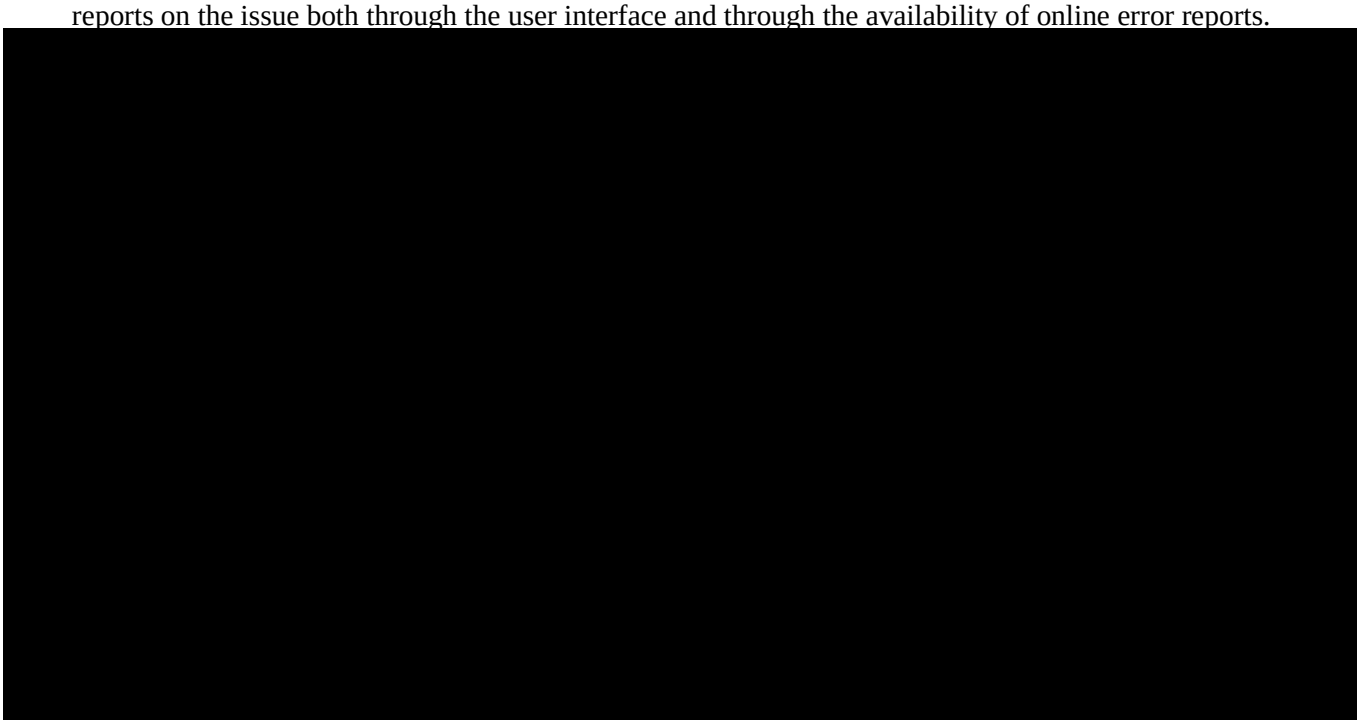


The MMIS send and receive steps are tracked within the Provider Services module workflow for the Provider. In addition to the report discussed above, our solution tracks each Provider's status and displays the error to the end user as part of the workflow process. *Exhibit 3.10.15.4-2: MAXIMUS Provider Services Solution Interface Error Handling & Reporting* shows an example of what the enrollment specialist might see in the case where the Provider may not have been successfully processed by the MMIS. The screen shown in *Exhibit 3.10.15.4-2* provides an example of what the end user might see when a Provider is not processed correctly from the MMIS. Such errors are infrequent but can occur. When they do, our solution is proactive in reporting on the issue. MAXIMUS technical support staff are aware of the issue through automated alerts within the system and the authorized user is also immediately aware of the issue through the user interface. Users can then take action to correct the data for the

CONFIDENTIAL

CONFIDENTIAL

Provider, re-approve the Provider, and re-send the Provider to the MMIS. As mentioned previously, MAXIMUS has better than a 99 percent success rate in the processing of transactions in our most recent District of Columbia implementation. In the rare cases where exceptions occur, the system actively reports on the issue both through the user interface and through the availability of online error reports.



MAXIMUS proposes to use AppDynamics as the main tool for monitoring the health and performance of the application.

3.10.15.5 Report Creation and Customization

Our experience working with Provider enrollment systems across different states gives us the insight necessary to design our data models and self-service ad hoc reporting functions to specifically meet needs the needs of DPHHS. We have used our knowledge based on past implementation experience to create a reporting framework that is easy to create new reports. As shown in *Exhibit 3.10.15.5-1: MAXIMUS Provider Services Solution Report Structure*, all new reports are inherited from a template report that has the standard information including banner, header, footer, title etc. All our reports have an area for adding parameters, paging, report run date etc. MAXIMUS will work with DPHHS to define the kind of template that is needed for the needs of the state and will accommodate them as part of DDI Phase.

CONFIDENTIAL

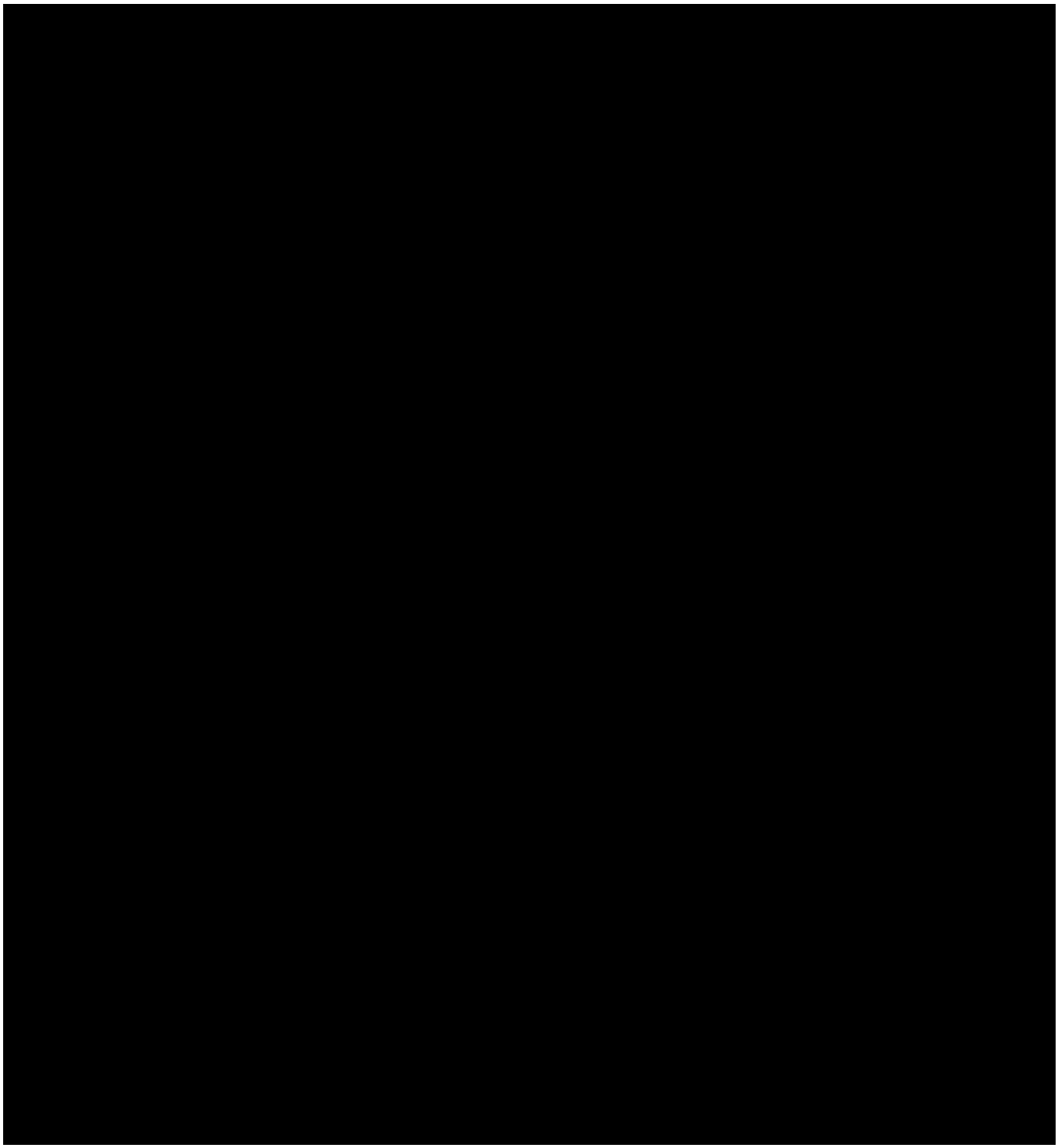
CONFIDENTIAL

Our Reporting module interface enables DPHHS staff members to create their own views of existing reports as well as new reports by mixing and matching data fields and parameters such as date, type, age, or action type. All basic quantitative parameters included in required reports will be available for ad hoc reporting. Our application throughput dashboard report is shown in *Exhibit 3.10.15.5-2: MAXIMUS Provider Services Solution Executive Dashboard Example*.

Because this functionality is built using a MicroStrategy presentation layer, it includes an intuitive drag and drop functionality and a large selection of visualization options such as graphs, charts, maps, and grids. The user can even select their own colors and fonts. MicroStrategy is one of the leading providers of business intelligence visualization software.

CONFIDENTIAL

CONFIDENTIAL



In most cases, DPHHS users do not need to create new reports from scratch, but instead leverage predefined templates to create new reports and analyses. Users may also drill down on particular reporting elements to present more detailed data down to the transaction level. A user can create their own view of dashboards and reports using a wide array of pre-defined widgets. This can include a summary level dashboards or detailed level reports.

CONFIDENTIAL

For those modified or created reports that may be needed again, users can save these schematics for future access by user role or privately through their own account. They can even set alerts to inform them when certain thresholds are met. Because much of the data will be updated in near-real time, these alerts may even be on the same day. For example, if a DPHHS user wanted to see if exemption-related calls spiked due to specific text message campaign about auto-assignment, they would set an alert to let them know if these call types exceeded the average by a set amount.

3.10.15.6 Report Distribution

Authorized state and vendor staff log into our solution via the same web portal to access a combination of standard reports, dashboard reporting views, and online data to support their oversight responsibilities for direction and management of the project. Real-time access to screening and enrollment data gives State staff the ability to review all Provider data received by the project, the history of data changes, application fee data, and any documentation associated with the enrollment or revalidation of Providers in the State's Medicaid program.

The MAXIMUS reporting engine allows users to search for reports based on different criteria. A user can log into our solution, go to reporting page, and search for reports. The reports can be executed on-demand and exported to various formats like PDF, excel and other formats as needed. These exported documents can be saved into ECM. The reports are print-ready and a user may choose to print a report or portions of it as needed.

Our solution also allows for generating reports on a scheduled basis. A user can set a schedule on a report to be emailed or stored in ECM. The user can set the email address to be a specific user or a distribution list.

As our solution is implemented for Montana, more and more reports will be accessible on the user reporting dashboards and available to download in multiple format options such as comma-separated values (CSV), portable document format (PDF), or Microsoft Excel. All applicable reports are accessible to DPHHS staff and other operations staff at all times over a standard Internet connection.

3.10.15.7 Reporting Requirements

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

ID	Reporting Requirement	MAXIMUS Summarized Response
REP01	The Contractor's solution shall include a query tool that allows users to easily query data necessary to support state healthcare programs business needs.	At the core of our configurable reporting capabilities is the business intelligence suite implemented with MicroStrategy. The business intelligence suite provides authorized users with powerful reporting capabilities. The basis for the reporting functions is the database structures that store all information about the enrollment and screening process. We also create a uniquely defined reporting layer that makes standard and ad hoc reports easy to create and maintain.
REP07	The Contractor's reporting tool shall provide the ability to design and execute a queries using one or more wild cards (e.g., %, *,?) and operators (e.g. =, , >, >=, <, <=, IN, BETWEEN, LIKE, IS NULL or IS NOT NULL) to provide data when searching or reporting.	Our solution allows the use of wild cards and operators as part of designing and executing queries. In addition to these, dashboard reports allows conditions to show different kinds of graphical elements and advanced functions to change colors based on a value of a variable.

ID	Reporting Requirement	MAXIMUS Summarized Response
REP23	The Contractor's solution shall maintain reporting services that are backward compatible, and the reports functionality is preserved over major or minor releases or the contractor will provide migration support to move reports forward.	The MAXIMUS reporting platform is built to be backward compatible with the reports, and during the major and minor releases we will confirm the reports are working and provide migration support if they needs to be changed.
REP31	The Contractor's reporting solution shall support initiation of reports through various methods including on-demand, scheduled requests (including non-business hours), and event-driven requests with distribution of the report results to specified secure locations.	Our reporting subsystem allows for initiation of reports including on-demand and scheduled and will distribute report results to specified secure locations. These secure locations include secure FTP, email etc.
REP32	The Contractor's reporting solution shall allow users to search on criteria including report names, report filters, and data elements included in the report in a library or repository of reports.	All the reports are indexed based on names, filters, and descriptions. They are included in the report library and users can search for reports based on these criteria.
REP36	The Contractor's reporting solution must display standard report header and footer information (e.g., report number, report title, page number, date) on all reports.	All our reports have a standard structure. MAXIMUS will work with DPHHS on identifying the changes needed to the standard structure and will conform to these requirements.
REP37	The Contractor's reporting solution shall provide the ability to store system generated reports in the Enterprise Content Management (ECM).	Our reports can be exported into several formats and can be stored into ECM. This is currently done with all outbound correspondence.
REP38	The Contractor's reporting solution shall allow a user to manually save report output to the ECM.	Our reports can be exported into several formats and can be stored into ECM.
REP39	The Contractor's solution shall provide efficient navigation (e.g., the ability to move forward and backward in the solution).	All our reports follow a template to allow the user to easily navigate pages and navigate from and into a report.
REP42	The Contractor's reporting solution shall allow authorized users to view, sort, export and print dashboard and report data in a variety of formats (e.g., HTML, Excel, TXT, CSV, PDF, or character delimited).	Our solution provides ability to print a full report or parts of the report. It provides a preview of the print to show it is print ready. We support all required formats such as PDF, Excel, CSV, TXT, and so on.
REP64	The Contractor's solution shall provide the ability to access and use all current and historical data for reporting purposes.	All the data from ODS will be sent to and stored in the reporting data store. All current and historical data is stored in the reporting data store for reporting purposes.
REP103	The Contractor's solution shall have the capability to display data in a variety of formats (e.g., standard reports, graphs, charts, maps, dashboards) without the need to export data to another tool.	Our industry leading reporting engine provides various formats to create dashboards and reports. The formats include Summary, Details, Charts, and graphs.
REP104	The Contractor's solution shall have the ability for authorized users to selectively retrieve, view, export, and print reports (or portions of reports).	Our solution has role-based access to reports. Based on the user role, a user will be able to see the reports that belong to them and perform operations accordingly. One can set permissions to reports to allow a particular role to view but not to export or print a report.
REP107	The Contractor's solution shall have the capability to allow authorized users to view query parameters along with query results.	Our template-based approach to reports allows for creating reports that have different fields including query parameters. We will work with DPHHS to identify all the necessary fields needed in the report template for query results.
REP110	The Contractor shall update dashboards in real-time or on a schedule approved by the State.	All dashboards are real time or near real time. The details for these will be discussed with DPHHS on a schedule approved by the State.
REP111	The Contractor's solution shall allow authorized users to design, save and share configurable dashboards and reports.	Our solution has role-based access to reports. One can set permissions to reports to allow a particular role to view and another role to save, share, and configure reports.
REP112	The Contractor's solution shall provide report, dashboard and query templates for authorized users to modify and reuse.	Our solution allows for drag and drop of query templates. This allows for creating customizable dashboards and reports for users to modify and reuse.
REP116	The Contractor's solution shall provide an established library of standardized operational reports as well as the ability to create a wide array of configurable detail level and summary level reports, dashboards and queries.	Our solution comes with a library of standardized operational reports, provider reports, and CRM reports, and will have the ability to create a wide range of configurable detail level and summary level reports, dashboards and queries.

ID	Reporting Requirement	MAXIMUS Summarized Response
REP118	The Contractor's solution shall have the capability to produce reports or display output data by National Provider Identifier (NPI), proprietary ID, or by a subset of the provider's practice or taxonomy.	Our solution can produce reports based on different fields of a provider record including NPI, proprietary ID, or by a subset of the provider's practice or taxonomy.
REP128	The Contractor's solution shall provide ad hoc query capability for retrieval of data relevant to specific operational and program business units.	Our solution has ad hoc query capabilities for retrieval of data relevant to specific operational and program business units.
REP129	The Contractor's solution shall provide an online adhoc reporting tool that allows authorized users access to provider and trading partner data (e.g., provider enrollment status, alphabetic and numeric provider listing, re-certification listing, revalidation listing, group affiliation listing, provider classification listing, and category of service listing).	Our online ad hoc reporting tool allows authorized users access to provider and trading partner data (e.g., provider enrollment status, alphabetic and numeric provider listing, re-certification listing, revalidation listing, group affiliation listing, provider classification listing, and category of service listing).
REP130	The Contractor's reporting tool shall provide current and historical information about user access. The report shall include both standardized data in addition to allowing user input of run criteria such as user IDs, roles/privileges/authorizations, and configurable from and to dates.	We have user access reports that show user access of various system functions. All reports have default parameters and allow specific user inputs on which to drill down.
REP131	The Contractor's solution shall track and have the capability to report both summary and detail level information pertaining to provider enrollment, disenrollment, termination, re-enrollment, revalidation, and recertification.	Our library of reports has detail and summary level of information pertaining to provider enrollment, disenrollment, termination, re-enrollment, revalidation, and re-certification. In addition to this, there are filter criterion like provider type, provider category, etc. to allow for looking up provider enrollment information based on various categories.
REP132	The Contractor's solution shall provide the functionality to identify, track and report the number and type of individuals associated with a provider or trading partner application (e.g., provider, facility, owner, managing employee and/or board member) including screening and monitoring results.	Our report library has reports related to groups and their affiliations, trading partners, owners, screening and monitoring results.
REP133	The Contractor's solution must provide Provider Transaction Error Reporting that includes the error, the date and time the error was identified, and the provider file(s) effected.	Our report library has reports that detail transactions, the date on which they are sent, the status of the transaction results. These can be filtered by successful, cancelled and error transactions.
REP134	The Contractor's solution shall have the ability for users to query using date and/or date ranges for scheduled and ad-hoc reporting.	Our reports have date and date range filters wherever applicable for scheduled and ad hoc reports.
REP135	The Contractor's solution shall provide the ability to report on electronic payments received through the Provider Services module (i.e., provider application fees).	Our report library contains details related to application fees, the payment method, waivers applied, etc., and users can filter them on different criteria.
REP136	The Contractor's solution shall provide the capability to archive and discontinue. The solution shall be capable of purging reports in compliance with the Federal and State retention policies.	Our solution is capable of purging reports in compliance with Federal and State retention policies.