

State of Montana

Department of Public Health and Human Services

Date
November 16, 2017

Provider Services Module

Technical Proposal
RFP #DPHHS-RFP-2018-0127JT

Contact
Jeff Jarjoura
Vice President, Business Development
Optum Government Solutions, Inc.
11000 Optum Circle
Eden Prairie, MN 55344
T (281) 382-7751
jeff.jarjoura@optum.com

Table of Contents

3. Response to Section 3: Scope of Services 3-1
3.1 PURPOSE AND INTENT 3-1
3.2 STATE VISION, GUIDING PRINCIPLES AND OBJECTIVES 3-3
3.3 MODULARITY APPROACH AND BLUEPRINT 3-6
3.4 TECHNOLOGY STANDARDS 3-12
3.5 MONTANA HEALTHCARE PROGRAMS OVERVIEW 3-15
3.6 MONTANA HEALTHCARE PROGRAMS ENTERPRISE 3-19
3.7 FUTURE MPATH ENVIRONMENT 3-25
3.8 STAKEHOLDERS AND GOVERNANCE 3-26
3.9 HIGH LEVEL SCOPE OF WORK 3-29
3.10 DETAILED SCOPE OF WORK 3-34
3.10.1 Technical and Information Architecture Requirements 3-34
3.10.2 Project Management and System Development Requirements 3-124
3.10.3 Certification 3-248
3.10.4 Operations, Maintenance, and Configuration 3-254
3.10.5 Key Personnel and Resources 3-296
3.10.6 Project Closeout and Turnover 3-310
3.10.7 Project Deliverables and Documentation 3-326
3.10.8 Performance Standards 3-362
3.10.9 Subcontractors 3-387
3.10.10 Enrollment 3-389
3.10.11 Maintenance 3-415
3.10.12 Self-Service Portal 3-465
3.10.13 Option A Provider Services 3-487
3.10.14 Option B Provider Services 3-517
3.10.15 Reporting 3-548

List of Figures

[redacted]

01/17 © 2017 Optum, Inc. All Rights Reserved.

[redacted]

Figure 3.9: Provider Portal User Profile Tab for Provider Information. 3-96
Figure 3.10: Provider Portal Context Sensitive Help. 3-98
Figure 3.11: ECM Architecture. 3-117
Figure 3.12: Optum Provider Services solution. 3-118
Figure 3.13: Optum PMO Team and Administrative Activities. 3-126
Figure 3.14: Sample Communication Plan Table of Contents Activities. 3-128
Figure 3.15: Integrated Project Management and Governance Model. 3-129
Figure 3.16: Project Health Status. 3-131
Figure 3.17: Issue Escalation Process. 3-131
Figure 3.18: Optum Delivery Model. 3-133
Figure 3.19: Design Preview Process. 3-134
Figure 3.20: Iterative Development and Delivery. 3-135
Figure 3.21: Project Management Plan. 3-138
Figure 3.22: Project Governance Framework. 3-142
Figure 3.23: Performance Management Framework. 3-148
Figure 3.24: Optum Risk Management Approach. 3-150
Figure 3.25: Risk Management Process. 3-151
Figure 3.26: Risk Assessment Matrix. 3-152
Figure 3.27: Risk Priority Number Model. 3-153
Figure 3.28: Optum Quality Processes and Standards. 3-158
Figure 3.29: Project Health Status. 3-159
Figure 3.31: Integrated Master Schedule Development. 3-164
Figure 3.32: Change Management Process. 3-166
Figure 3.33: OSAM SDLC. 3-171

[redacted]

Figure 3.36: Sample HP ALM Requirements Repository. 3-179
Figure 3.37: Sample HP ALM Requirements Repository. 3-180
Figure 3.38: Phased Testing Approach 3-184

[redacted]

Figure 3.40: Location of Optum Office Options. 3-188

[redacted]

Figure 3.43: Test Release Plan. 3-205
Figure 3.44: Phased Testing Approach. 3-207
Figure 3.45: Testing Progress Report Example. 3-210
Figure 3.46: Test Summary and Detail Report Contents. 3-211
Figure 3.47: ADDIE Instructional Design Strategy. 3-218
Figure 3.48: Training Plan Table of Contents. 3-220
Figure 3.49: Sample LMS Home Page. 3-221
Figure 3.50: Sample Training Schedule. 3-222
Figure 3.51: Train-the-Trainer Model. 3-224
Figure 3.52: Provider Services Module Release Management Process. 3-231
[redacted]
Figure 3.54: Provider Services module Environment. 3-239
Figure 3.55: Disaster Recovery Program Components. 3-261
Figure 3.56: Optum Service Delivery Model. 3-265
Figure 3.57: Optum Configuration Management and Change Control. 3-270
Figure 3.58: Optum Routine Maintenance Services. 3-273
Figure 3.59: DTR Process Flow at Optum. 3-274
Figure 3.60: Types of Changes. 3-276
Figure 3.61: Key Phases of the Emergency Maintenance Process. 3-277
Figure 3.62: Change Management Process. 3-279
Figure 3.63: Release Management Process Diagram. 3-283
Figure 3.64: Release Planning Process Diagram. 3-283
Figure 3.65: Release Execution and Control. 3-284
Figure 3.66: Release Closure Process. 3-286
[redacted]
Figure 3.70: Communication notification tool. 3-292
Figure 3.71: Optum Cultural Values. 3-297
Figure 3.72: Project Organization Chart. 3-299
Figure 3.73: Sample Turnover Plan Table of Contents. 3-312
Figure 3.74: Sample Timeline of Turnover Activities. 3-313
[redacted]
Figure 3.80: Performance Management Framework. 3-362
[redacted]

[redacted]

Figure 3.86: Optum Provider Services Solution Portal Home Page. 3-392
Figure 3.87: Provider Enrollment Data Prompts. 3-396
Figure 3.88: Provider Enrollment Program Selections. 3-397

[redacted]

Figure 3.91: Provider Enrollment Patient Services Page. 3-400

[redacted]

Figure 3.93: Workflow Tool Criteria Checklist Example. 3-402
Figure 3.94: Single Provider Enrollment Application Covering Multiple Selections. 3-403
Figure 3.95: Provider Physical Location Page. 3-404
Figure 3.96: Provider Service Location Detail Page. 3-405
Figure 3.97: Fee Collection Page. 3-406
Figure 3.98: Workflow Enrollment Page. 3-407

[redacted]

Figure 3.100: Enrollment Status Designations. 3-410
Figure 3.101: Retroactive Enrollment. 3-411
Figure 3.102: Provider Effective Date for Services. 3-412
Figure 3.103: Conditionally Required Resource Materials and Training. 3-413
Figure 3.104: Checklist of Required Materials and Training 3-414

[redacted]

Figure 3.106: Optum ID Registration for NPI Type 1 Provider Type. 3-418
Figure 3.107: Optum ID Registration for NPI Type 2 Providers. 3-418
Figure 3.108: Provider NPI Information on Portal. 3-419
Figure 3.109: Begin and End Dates for Specific Enrollment and Demographic Data. 3-420

[redacted]

Figure 3.111: Capturing and Maintaining Licensure Information. 3-422
Figure 3.112: Provider Licensing, Certifications, and Accreditations Page. 3-423
Figure 3.113: Provider Insurance Page. 3-424

[redacted]

Figure 3.117: Physical, Mailing, and Billing Address Page. 3-429
Figure 3.118: Provider DEA Number. 3-430

Figure 3.119: Provider Ownership Page. 3-431
Figure 3.120: Provider Ownership Page. 3-432
Figure 3.121: Portal Managing Employee Page. 3-433
Figure 3.122: Portal Practice Information Page. 3-434
Figure 3.123: Enrollment Detail and Notes for Provider Files. 3-435
Figure 3.124: Portal Affiliations Page. 3-436
Figure 3.125: Portal Billing Page. 3-437
Figure 3.126: Portal Service Location Page. 3-438
Figure 3.127: Suspensions and Providers under Review. 3-439
Figure 3.128: Patient Services Information. 3-440
Figure 3.129: Provider Taxonomies. 3-441
Figure 3.130: Provider Banking Information. 3-442
Figure 3.131: Workflow Enrollment Criteria Checklist and Automated Provider Notification. 3-443
Figure 3.132: Enrollment Suspension Status. 3-444
Figure 3.133: Credentialing Dates. 3-445
Figure 3.134: Optum ID Activation Email. 3-447
Figure 3.135: Disenrollment and Termination Reasons. 3-449
Figure 3.136: Provider Banking Information Page. 3-451
Figure 3.137: Fee Collection Page. 3-452
Figure 3.138: Application Fee Waiver. 3-453
Figure 3.139: Practice Information Page. 3-454
Figure 3.140: Accreditation and Facility Bed Data. 3-455
Figure 3.141: Provider Medicare/Medicaid Page. 3-457
Figure 3.142: Enrollment Record and Verification of Activities. 3-458
Figure 3.143: Practice Information and Taxonomy Collection Pages. 3-459
Figure 3.144: Link to Other State ID Numbers. 3-460
[redacted]
Figure 3.146: Provider Risk Scores and Specialties. 3-463
Figure 3.147: Provider Review Enrollment Page. 3-464
[redacted]
Figure 3.149: Provider Directory Search Page. 3-467
[redacted]
Figure 3.152: Provider Messaging Inbox. 3-471
[redacted]
Figure 3.154: Provider Portal User Page. 3-473

Figure 3.155: Provider Portal User Profile Tab for Role. 3-474
Figure 3.156: Provider Portal User Profile Tab for Provider Information. 3-475
Figure 3.157: Provider Portal User Profile Tab for Review of Information. 3-476
Figure 3.158: Provider Portal Affiliations. 3-477
Figure 3.159: Billing Provider Affiliations. 3-478
[redacted]
Figure 3.161: Interactive Chat Page. 3-480
Figure 3.162: Key Contact Information for Providers. 3-482
Figure 3.163: Optum Provider Services Portal Public Home Page. 3-483
Figure 3.164: Optum Provider Services Portal Home Page. 3-484
Figure 3.165: Optum Provider Services Portal Registration and Login Page. 3-485
Figure 3.166: Optum ID Page. 3-486
Figure 3.167: Provider Enrollment Confirmation Number. 3-487
[redacted]
Figure 3.169: Self-Service Functions. 3-489
[redacted]

[redacted]

Figure 3.193: Supporting Provider Enrollment Activities. 3-519

[redacted]

Figure 3.200: Agile Development. 3-549

[redacted]

3. Response to Section 3: Scope of Services

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

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

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

3.1 PURPOSE AND INTENT

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

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

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

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

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

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

MPATH is an innovative strategy that will move Department of Public Health and Human Services (DPHHS) to greater levels of MITA maturity, ultimately improving your ability to serve the Montanans that rely on you for care and well-being. While the focus of MPATH is information system modernization, we understand the ultimate objective is empowering people to help people. It is about making sure the State's neediest citizens get the health care they need while being prudent stewards of the State's resources. It is also about easing the burden on and empowering the State's providers so they can focus

on delivering and managing care. We appreciate your mission and it aligns perfectly with ours.

We briefly describe our approach to the Medicaid market and how our strategy aligns with your vision, guiding principles, and objectives.

Optum Medicaid Management Services

Optum has provided administrative, medical management, and analytic services to Medicaid programs for more than two decades. Our extensive capabilities span the entire health care industry. We have taken lessons learned from these experiences, coupled with modern and proven technology, and introduced a new MMIS solution offering. Optum Medicaid Management Services (OMMS) is a strategic enterprise solution focused on addressing problems faced by many states that have attempted to replace or substantially enhance their legacy MMIS. OMMS comprises three core aggregate modules:

Approach

Our solution aligns with DPHHS's vision, guiding principles, and objectives including:

- Automa ion
- Flexibility
- Business and program driven
- Interoperability
- Data integration and centralized data management
- Analytics that leverage the ever evolving and expanding data universe
- Professionals with health and human services subject matter expertise

- **Optum Medicaid Business Services (OMBS)**: Provides Medicaid claims processing and program administration, including provider enrollment, call center, service authorizations, and more
- **Optum Triple Aim Analytic Services (OTAAS)**: Provides the analytics framework, resource capability and cohesive, data-driven environment for Medicaid operations
- **Optum Medicaid Health Services (OMHS):** Provides comprehensive benefit/medical management services tailored to each participant category and each participant's needs

OMMS is highly modularized in design. For states that prefer a turn-key approach that greatly simplifies procurement and implementation they may procure along each aggregate module. For those states, like Montana, that prefer a more granular best-of-breed approach the OMMS modularity framework accommodates that as well. The provider services component of the solution is configurable and scalable to meet your, and future participating states' needs.

Our approach to your MPATH initiative is to systematically align our understanding of your near and long term program objectives to our commercial-off-the-shelf (COTS)-based, MITA-aligned OMMS solutions. We have developed and implemented solutions that align with the MITA framework since its inception and throughout its iterations up to and even beyond the current 3.0 framework.

OMMS complies with the CMS Seven Conditions and Standards. We designed and developed it in full alignment with the CMS Medicaid Information Technology Architecture (MITA) 3.0 business processes, information and technology architectures, capability maturity guidelines, and operational performance metrics.

OMMS comprises commercial COTS components performance-tested in the commercial health care sector. When we say COTS, we mean Pure COTS—that is, no one-off custom-coded applications; no MMIS market code branches; just pure commercially released software from the vendors.

The COTS partners and technologies we incorporate into OMMS are chosen because they are:

- Proven and used widely throughout our enterprise

- Highly interoperable and extensible providing the opportunity to add capabilities without disrupting the integrity of the core software to ingest new releases and upgrades—a critical capability for which Optum is experienced and qualified
- Highly configurable offering nearly endless capability to tailor their use to the specific needs of your MPATH requirements

Adaptability is part of the OMMS fundamental architecture. The use of COTS and Software-as-a-Service (SaaS) applications enables us to adapt the solution to meet your program needs without great design and development effort. Our approach assures that your program will enjoy the latest in technological capabilities in a non-disruptive manner.

3.2 STATE VISION, GUIDING PRINCIPLES AND OBJECTIVES

3.2.1 State Vision

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

3.2.2 Modularity Business Objectives

The MPATH Program objectives include:

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

3.2.3 Guiding Principles

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

Table 3.2.3 MPATH Guiding Principles Guiding Principles	
Flexible Enterprise Technology Platform	Implement flexible, rule-based, configurable components and services to enhance decision-making, increase management efficiency and promotes agile adaptability for new and evolving regulations, programs and initiatives.
Centralized Data Repository	Implement a centralized data warehouse and associated data analytics tools to enable real-time or near-time access to data including clinical data and enhanced reporting that meets changing business and management needs.
Business-driven Enterprise transformation	Business functions must drive technical solutions and the modular MMIS capability must be flexible to meet future needs including new regulations, legislation, and innovations.
Process Automation	Automate manual processes and eliminate human intervention wherever possible and utilize workflow tools to standardize business processes that guide internal and external users through process steps, activities, and tasks.
Data Integration and Interoperability	Promote reusable components by using open architecture and adopting industry and national standards for interoperability, integration, and data exchange.
Data Consistency Across the Enterprise	Utilize a comprehensive data governance process to ensure consistent data management processes and policies across the Montana Healthcare Programs enterprise. Provide data that is timely, accurate, usable, and easily accessible in order to support analysis and decision making for health care management and program administration.
Progressive Technology	Implement services that will allow the State to take advantage of progressive technology (access via mobile devices, mobile apps, instant messenger, etc.) to improve how it interacts and communicates with recipients, providers, and contractors.
Member and Provider Centric Focus	Implement solutions that provides easy to access and comprehensive portal for providers, members and other stakeholders that promotes self-service functionality. For example, claims status and member eligibility inquiries. The solution would leverage role-based security to make sure stakeholders have access to only the information required for their needs.
Cost Efficiency and Effectiveness	Implement a solution that supports future State strategies of paying providers based on the quality of services rather than quantity of services, focus on the member outcomes, and efficiently processing fee-for-service claims.

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

We carefully select the states and projects that align with our mission and direction and then work relentlessly toward mutual success with our clients. The key is alignment. The vision and mission you have laid out for your MPATH Program is a perfect fit for our strategic approach to the market. With Optum, you can count on the fact that we bring extensive experience across *all* domains of the health care industry

DPHHS
Program Mission

Assure necessary medical care is available to all eligible Montanans within available funding resources.

Optum understands that MPATH vendors cannot operate in a vacuum. We must all keep an eye on the State's broader health care transformation vision and work as a team to help make it a reality. That is why we have made a point to meet with and gain feedback from stakeholders from across the State's health care market. Over the past two years, beginning with UnitedHealth Group Executive Chairman Steve Hemsley's meeting with Governor Bullock in 2015, we have met with representatives from the Montana Medicaid Association (MMA), the Montana Hospital Association (MHA), advisors from the Governor's office, and key legislators on the Health and Human Services sub-committee. We also attended relevant legislative committee hearings, including the Legislative

Finance Subcommittee for Oversight of Medicaid Management Information System, and State-Tribal Relations Interim Committee.

In addition, we have followed the progress of Governor Bullock's Council on Health Care Innovation and Reform, and thoroughly reviewed the Montana Health Care Innovation Plan that resulted from this collaborative effort. We take note of the following three priority areas from the plan:

- Physical and behavioral health integration, including substance use, chemical dependency, and mental health integration
- Social determinants of health and disparities among American Indians and other populations
- Health information technology (IT) infrastructure, including health information exchange (HIE) and telehealth[1]

These conversations and observations have informed our thinking and solution design strategies, enabling us to understand your broader strategic objectives as we seek to help you plan and execute tactically. Our proposed solution aligns with these priorities, balancing the interests of the State's broad array of stakeholders, while keeping our eye on your health care transformation vision.

Optum Solutions Align with Your Guiding Principles and Objectives

MPATH objectives and guiding principles inextricably link to validate that the enterprise is empowered to function most efficiently in the near term, while remaining agile to enable a constant and never ending cycle of non-disruptive improvement. This is exactly the design vision behind our MMIS offering and the precepts of MITA. Technology should enable efficient business processes, not define them.

[1] Montana Health Care Innovation Plan, June 2016

3.3 MODULARITY APPROACH AND BLUEPRINT

3.3.1 Modularity Approach

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

3.3.2 Modularity Blueprint

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

Figure 3.3.2.1 MPATH Modularity Groups

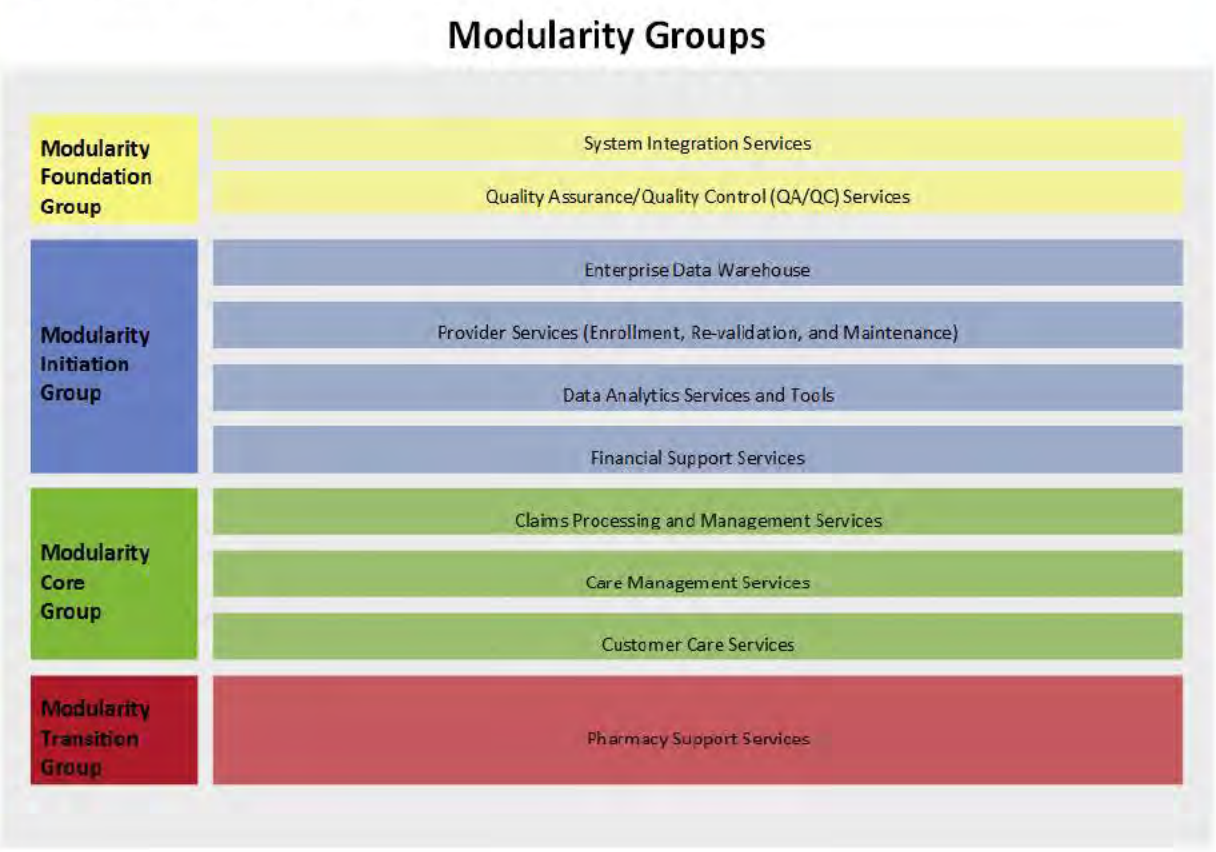
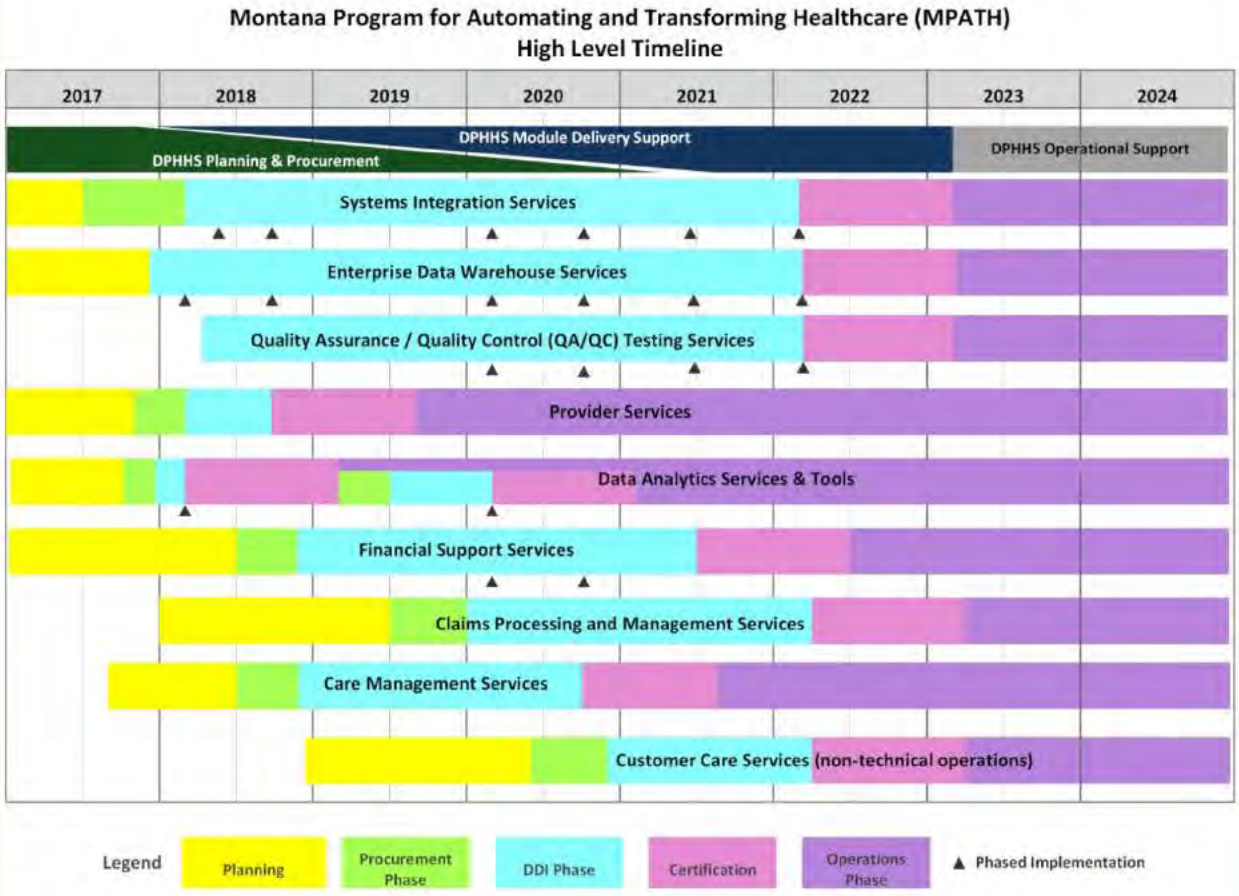


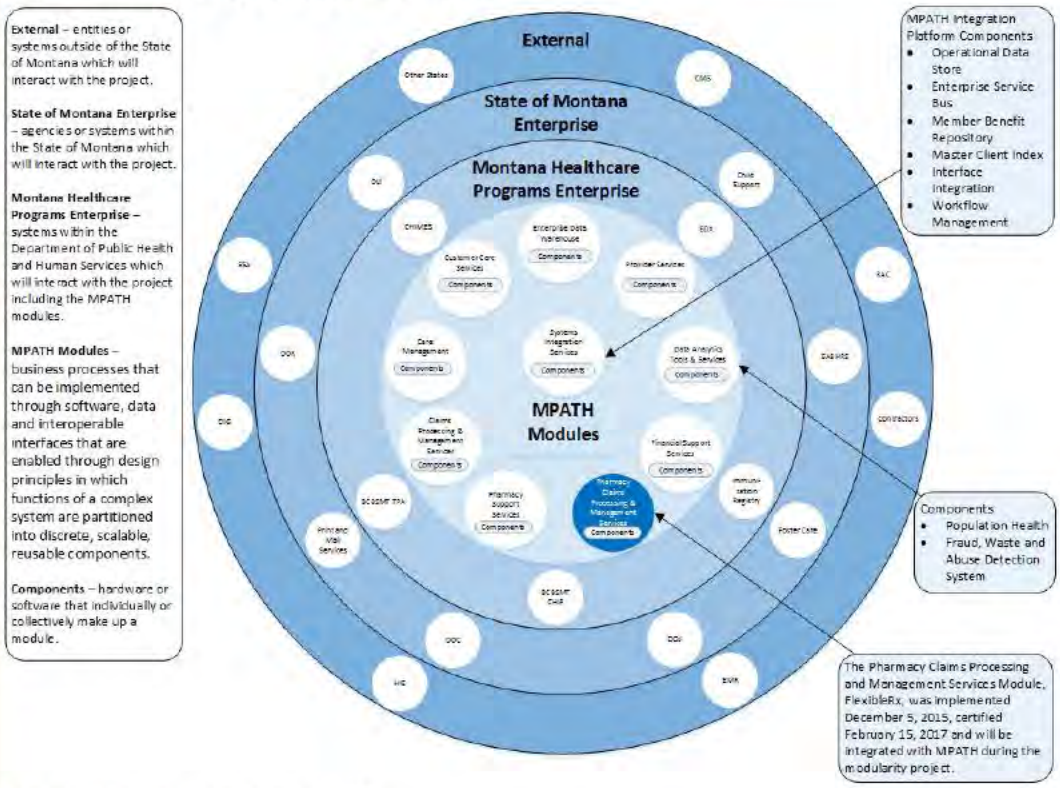
Figure 3.3.2.2 Montana Program for Automating and Transforming Healthcare (MPATH) Modularity High Level Timeline



3.3.3 MPATH Modules

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

Figure 3.3.3 MPATH Integration Layers



Systems Integration Services (SI)

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

Provider Services (PS)

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

Enterprise Data Warehouse (EDW)

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

Data Analytics Services and Tools (DA)

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

Financial Support Services (FSS)

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

Claims Processing and Management Services (Claims)

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

Care Management Services (CM)

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

Customer Care Services (CCS)

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

Pharmacy Claims Processing and Management Services (PBMS)

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

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

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

Pharmacy Support Services (PSS)

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

3.3.4 Exclusions

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

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

DPHHS used the following key principles to make exclusionary decisions:

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

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

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

Table 3.3.4 MPATH Contractor Procurement Exclusions

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

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

✓ **Optum has read, understands, and will comply with each of the requirements in these sections.**

Optum traveled the path with you as you developed your MPATH concept. We worked together with you, CMS, and other State agencies in a public/private sector initiative to better understand how we can most effectively execute on the concept of modularity. We understand MPATH modularity is designed to seek best-of-breed products and services versus a best-of-suite approach. We have gained an appreciation of your program goals and your strong commitment to leveraging innovation, industry expertise, and best practices in order to establish a new standard of excellence in Medicaid program administration.

The provider services capabilities within the solution are configurable and scalable to your current and future needs, as well as other participating states. As noted previously, three core aggregate OMMS modules are comprised of granular solution components. The following describes how OMMS modularity framework aligns with MPATH modularity.

OMBS	OTAAS	OMHS
Provider Services	Enterprise Data Warehouse (DOA)	Care Management Services
Financial Support Services	Data Analytics Services & Tools – Population Health	
Claims Processing & Management Services	Data Analytics Services & Tools – Program Integrity	
Customer Care Services		
Pharmacy Support Services		

3.4 TECHNOLOGY STANDARDS

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

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

Table 3.4 High Level Requirements for the MPATH Program

Requirements	Requirement Definition
Alignment with the Seven Standards and Conditions	Comply with the Standards and Conditions, set forth by CMS, in order to receive enhanced FFP.
Flexible Enterprise Technology Platform	Utilize enterprise architecture governance process that incorporates MITA standards to accommodate future programs and initiatives.
Automated workflow management	Provide centralized, configurable workflow solution that allows for workflow creation, execution and automation.
Enhance program reporting and data analytics	Implementation of Data Analytic tools and services to enable accurate, real-time data and reporting that will meet changing business and management needs. The solution should be enterprise centric, which would enable other health care and program data typically not found in an MMIS to support enterprise decision-making.
Centralized access to data	Provide real-time and centralized access to members, providers, benefit plan(s), claims, and case management data for the Department's programs including Medicaid, Healthy Montana Kids Plus (HMK Plus), Healthy Montana Kids (HMK) (the state's Children's Health Insurance Program CHIP)), Montana Health and Economic Livelihood Partnership Plan (HELP), Mental Health Services Plan (MHSP), Passport to Health, Patient Centered Medical Home (PCMH) and waiver services. Ability to enhance decision-making and increase management efficiencies.

Data integration and interoperability	Provide interfaces and components that are reusable and follow industry and national standards for data exchange. Procured solutions will include exposed APIs for easy integration with other enterprise solutions.
Standard Communication Protocols	Standardized protocols for electronic communication will allow DPHHS to move to electronic options for communications using modern services such as Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) including a Web Portal. In addition, standardization will support the ability to provide messaging in Multilanguage and multi-literate formats.
Progressive technology	Provide progressive technology, e.g., mobile apps, text messaging, etc., that increase communication venues and encourages member and provider interaction with Montana Healthcare Programs.
Automate Manual Processes	Automate a majority of manual processes to replace human interactions with automated configurable business rules.
Administrative Simplification	Adhere to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II).
Mechanized Claims Processing and Information Retrieval Systems Final Rule	Meet requirements specified in the Mechanized Claims Processing and Information Retrieval Systems (90/10) Final Rule (42 CFR 433), specifically related to configuration and customization of COTS software.
Standards and Implementation Specifications for Health Information Technology Final Rule	Modularity approach is aligned with industry standards adopted by the Office of the National Coordinator for Health IT described in Final Rule (45 CFR part 170, subpart B).
HIPAA and HITECH	All solutions and services shall be fully compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-1919) and Administrative Simplification (Subset of Title II) requirements in effect as of the date of release for the RFP and with any changes that subsequently occur, unless otherwise noted. The Contractor shall sign a Business Associate Agreement, included in the contract, which is subject to HIPAA and HITECH regulations CFR 45 parts 160 and 164.

✓ **Optum has read, understands, and will comply with each of the requirements in this section.**

CMS' strategic direction for MITA and the Seven Conditions and Standards guides our solution design. We designed and developed OMMS in full alignment with the MITA 3.0 business processes, information and technology architectures, capability maturity guidelines, and operational performance metrics.

We have developed and implemented solutions that align with the MITA framework since its inception and throughout its iterations up to and even beyond the current 3.0 framework. The following describes each of the seven conditions and how our OMMS solutions align.

Modularity Standard

OMMS is a set of layered services and components enabling a reusable, modular, and highly scalable set of capabilities that will meet the growth and performance demands of DPHHS both today and in the future. To meet the modularity standard, OMMS enables the replacement or addition of individual modular COTS components, as technology and business needs change and the industry evolves.

MITA Condition

OMMS business, information, technical architectures, and capabilities trend toward the higher MITA maturity levels. Our approach for advancing MITA maturity begins with delivering solutions that align with your current maturity model while offering business processes, architecture, and an operations framework that allows an adaptive and deliberate progression into higher maturity levels. We instill this discipline in the design, development, and implementation (DDI) phase and include organizational change components for those elements affected by higher levels of maturity and capabilities.

Industry Standards Condition

OMMS meets the CMS Industry Standards Condition through the designed ability to use industry standards throughout the technical and information architecture. One of our selection criteria for the COTS products incorporated into OMMS was the ability to accommodate and incorporate industry standards. This includes the COTS vendor's ability to adopt and incorporate new industry standards in a timely and reliable manner.

Leverage Condition

OMMS was specifically designed to meet the CMS Leverage Condition. OMMS is an enterprise-capable solution that has been designed to be scaled up and leveraged across your entire ecosystem. The technology stack supporting our solution is based on commercially available, industry leading technologies beginning with the physical computing and storage platforms and extending up into the operating system layers. The same is true for middleware and database platforms. OMMS components will leverage other data and systems and, in turn, our components will become candidates for other systems to leverage.

Business Results Condition

OMMS meets the CMS Business Results Condition. The Business Results Condition relates to the timeliness and effectiveness of your business processes. You can use the robust analytic tools and methods to isolate business processes and even sub-processes to perform analysis for efficiency and quality improvements. OMMS enables business process automation through configuration of business rules that exist either natively in the COTS components or through a separate rules service. The opportunities to improve business process results can extend beyond the MITA business processes and into all of your programs and other state agencies if so desired. Not only will this enable a capability maturity Level of 4 for the Business Results Condition, it will also work to sustain a Leverage Condition maturity of Level 3 or greater.

Reporting Condition

Through service oriented architecture (SOA) tools, OMMS can expose the data that are necessary for oversight, administration, evaluation, integrity, and transparency. Dashboards, interactive visualizations, and pre-defined reports can be accessed through our highly intuitive Web-based navigation portal. You will have appropriate drill-down capabilities to see the details behind each dashboard measure.

Interoperability Condition

OMMS meets the CMS Interoperability Condition. We understand that the real benefit of interoperability is to allow for a high degree of coordinated interaction in order to maximize value and minimize burden and costs to providers, beneficiaries, and other stakeholders. Interoperability provides for effective, efficient, and timely communication within and externally to other systems. This may include providing interoperability with other MMIS modules as well as future external system needs, such as public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services.

3.5 MONTANA HEALTHCARE PROGRAMS OVERVIEW

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

Table 3.5 Montana Healthcare Programs Member Groups

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

	years old, not have insurance considered to be 'creditable coverage,' meet citizenship or qualified alien requirements, be a Montana resident, and have been screened through the Montana Breast and Cervical Health Program. Countable income cannot exceed 250% of the FPL.
Medically Needy	Certain individuals or families whose income exceeds the Categorically Needy income standards, but who have a significant medical need may be eligible for Standard Medicaid benefits. The individual or family is obligated to incur medical expenses or make a cash payment (spenddown) for the difference between their countable income and the Medically Needy Income Level each month. The resource limit is $2000 for an individual, and $3000 for a couple or family.
Autism Services	This program provides intensive treatment services for Medicaid members up to age 21 with a diagnosis of autism spectrum disorder or related condition.
Montana Medicaid for Workers with Disabilities (MWD)	MWD allows certain individuals who meet Social Security's disability criteria to receive Medicaid benefits through a cost share. The cost share is based on a sliding scale according to an individual's income. MWD resource and income standards are significantly higher than many other Medicaid programs: $15,000 for an individual and $30,000 for a couple; while the countable income limit is 250% of the FPL.
Additional healthcare services	
Medicaid Expansion	On January 1, 2016, Montana expanded healthcare coverage to thousands of state residents through the Montana Health and Economic Livelihood Partnership (HELP) Act. Individuals who receive healthcare coverage through the HELP Act are either eligible for Standard Medicaid benefits or HELP Plan benefits. Help Plan benefits are administered through Blue Cross Blue Shield (BCBS) of Montana, a third party administrator (TPA). Section 9 of the HELP Act includes provisions to provide health care services for individuals who are in the custody of the Department of Corrections or who are residents by commitment or otherwise residents of the following facilities. • Montana State Hospital • Montana Mental Health Nursing Care Center • Montana Chemical Dependency Center • Montana Developmental Center
Mental Health Services Plan (MHSP)	This program provides state funded benefits for individuals who have severe and disabling mental illness and meet income limits establish by the state but do not qualify for Standard Medicaid.
Emergency Alien Medical Coverage	This program provides limited benefits for emergency services such as labor and delivery. Other emergency services may be covered from the time treatment is first given for a condition until that same condition is no longer considered an emergency. These services must be determined an emergency by Medicaid department staff.
Medicare Savings Program (MSP)	MSP benefits may be provided to individuals who are low income Medicare beneficiaries. • Qualified Medicare Beneficiary (QMB) –Medicare premiums, co-payments and deductibles are covered for individuals who have QMB eligibility. • Specified Low-Income Medicare Beneficiary (SLMB) – Medicare premiums are covered for individuals who have SLMB eligibility. • Qualified Individuals (QI) – Part B premium payments are covered for individuals who have QI eligibility.

Montana Waiver Programs	Montana has a number of waiver programs that provide services to supplement existing Standard Medicaid benefits that include the following waivers:
	• Section 1115 waivers
	  ○ 1115 Plan First
	  ○ 1115 Health and Economic Livelihood Partnership (HELP) Demonstration
	  ○ 1115 Basic Waiver for Additional Services and Populations
	• Section 1915 (b) waivers
	  ○ 1915(b) Health and Economic Livelihood Partnership (HELP)
	  ○ 1915(b) Passport to Health
	  ○ 1915(b)(4) Montana Big Sky Waiver Case Management

	○ 1915(b)(4) Montana Autism Evaluation Services • Section 1915 (c) waivers ○ 0208 HCBS Comprehensive Services Waiver for Individuals with Developmental Disabilities ○ 1915(c) Montana Big Sky ○ 1915(c) HCBS Severe Disabling Mental Illness (SDMI)

3.5.1 Montana Healthcare Programs Benefits

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

Table 3.5.1 Example of Standard Medicaid Covered Services

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

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

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

✓ **Optum has read, understands, and will comply with each of the requirements in these sections.**

The proven technology we are proposing is a critical enabling factor to the success of this project; however, it is the people, project organization, and extensive experience that we bring to this engagement that will ultimately help us achieve your vision. DPHHS needs a collaborative partner that not only understands technology, but also the business of Medicaid.

3.6 MONTANA HEALTHCARE PROGRAMS ENTERPRISE

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

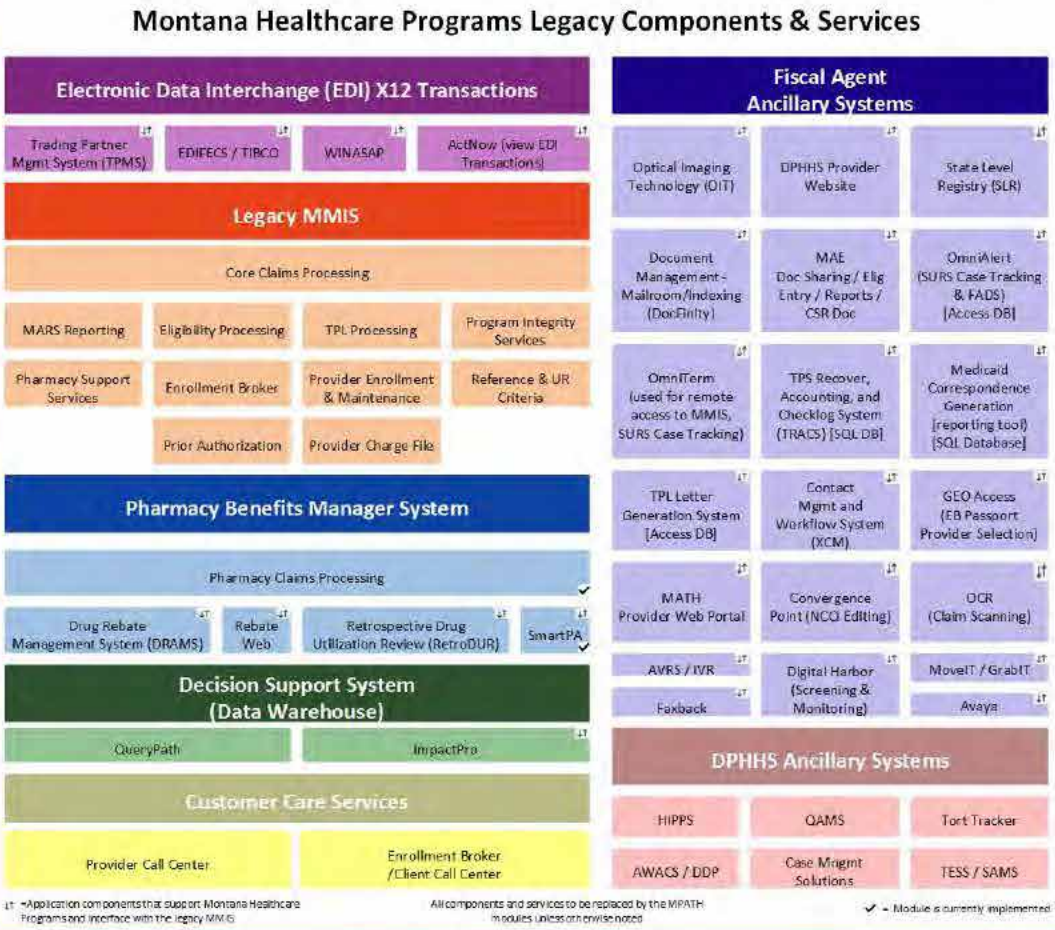
3.6.1 Current MMIS Environment

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

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

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

Figure 3.6.1 Montana Healthcare Programs Legacy Components and Services



3.6.2 Legacy Components and Services

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

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

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

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

Trading Partner Management System

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

EDIFECS/TIBCO

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

WINASAP

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

ActNow

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

3.6.2.2 Pharmacy Benefits Management System Components/Services

FlexibleRx

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

Drug Rebate Analysis and Management System (DRAMS)

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

Rebate Web

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

Retrospective Drug Utilization Review

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

Smart PA

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

3.6.2.3 Decision Support System Components/Services

Query Path

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

Impact PRO

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

3.6.2.4 Customer Care Services

Provider Call Center

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

Enrollment Broker/Member Call Center

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

3.6.2.5 Fiscal Agent Ancillary Systems

Montana Access to Health Web Portal

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

Automated Voice Response/Integrated Voice Response System

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

FaxBack

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

Avaya

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

Digital Harbor

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

Optical Imaging Technology

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

Optical Character Recognition

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

DPHHS Provider Website

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

DocFinity

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

Montana ACS Extranet

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

OmniAlert

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

OmniTerm

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

Third Party Recovery and Checklog System

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

Medicaid Correspondence Generation Tool

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

Third Party Liability Letter Generation Tool

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

State Level Registry

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

Conduent Case Management

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

GEO Access

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

MoveIT/GrabIT

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

Convergence Point

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

3.6.2.6 DPHHS Ancillary Systems

Health Insurance Premium Payment System

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

Quality Assurance Management System (QAMS)

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

Tort Tracker

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

Agency Wide Accounting Client System (Developmental Disabilities Services)

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

Case Management Solutions

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

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

Therap-This system is used for incident reporting.

The Eligibility Screening System

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

Substance Abuse Management System

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

Web Infrastructure for Treatment Services

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

✓ **Optum has read, understands, and will comply with each of the requirements in these sections.**

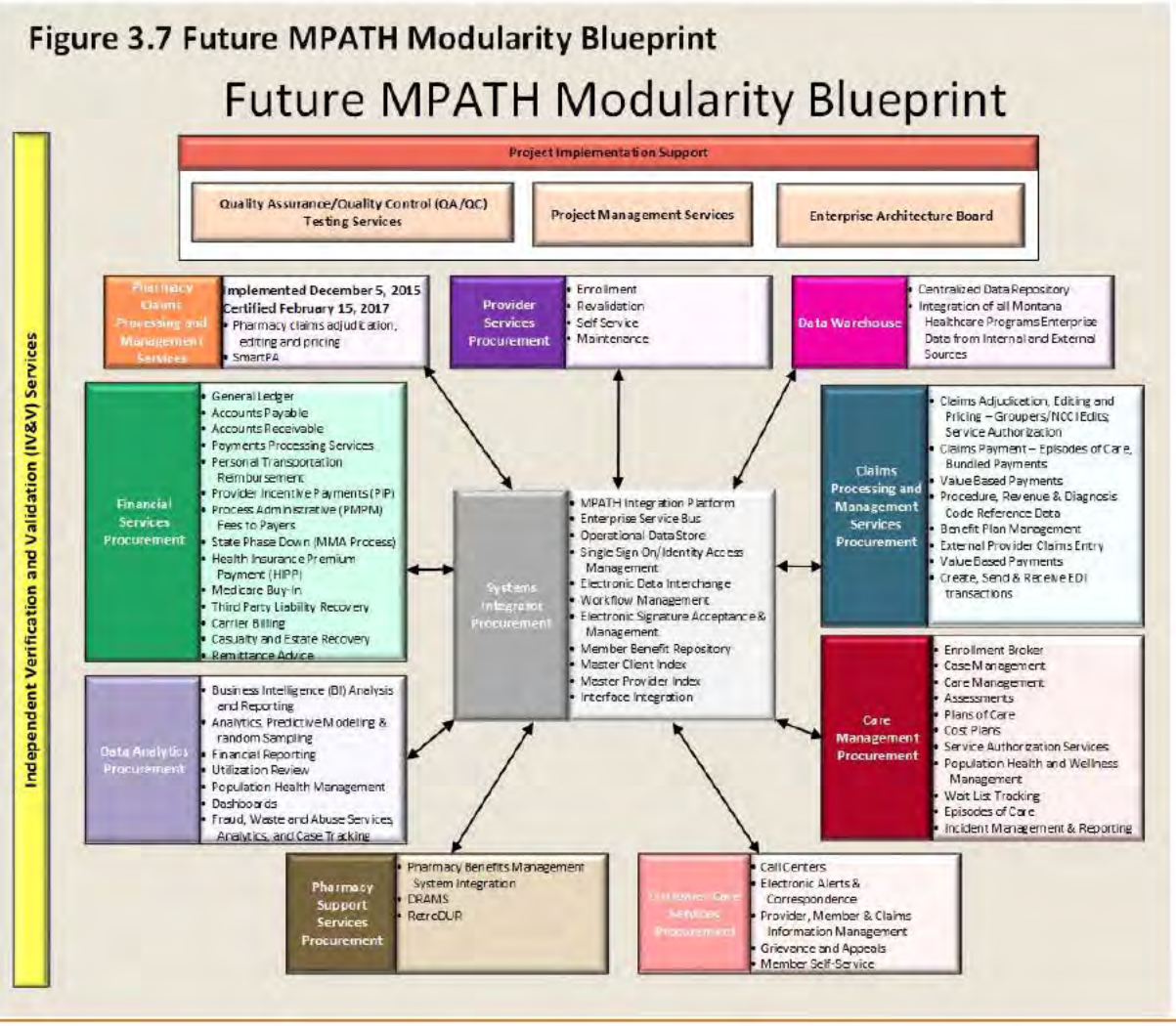
As you move away from siloed, sub-system components to SOA, MMIS modernization becomes inherently incremental. Therefore, it is essential that new systems seamlessly integrate with existing legacy components until such time they are decommissioned.

3.7 FUTURE MPATH ENVIRONMENT

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

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

Figure 3.7 Future MPATH Modularity Blueprint



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

Optum understands that a modular approach to implementation means new systems must integrate with existing legacy components. OMMS is designed with interoperability and flexibility in mind. Our extensive understanding of legacy Medicaid environments enabled us to design a solution that is lightweight, flexible, and modular, meeting the needs of today and in the future.

3.8 STAKEHOLDERS AND GOVERNANCE

3.8.1 Governing Stakeholders

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

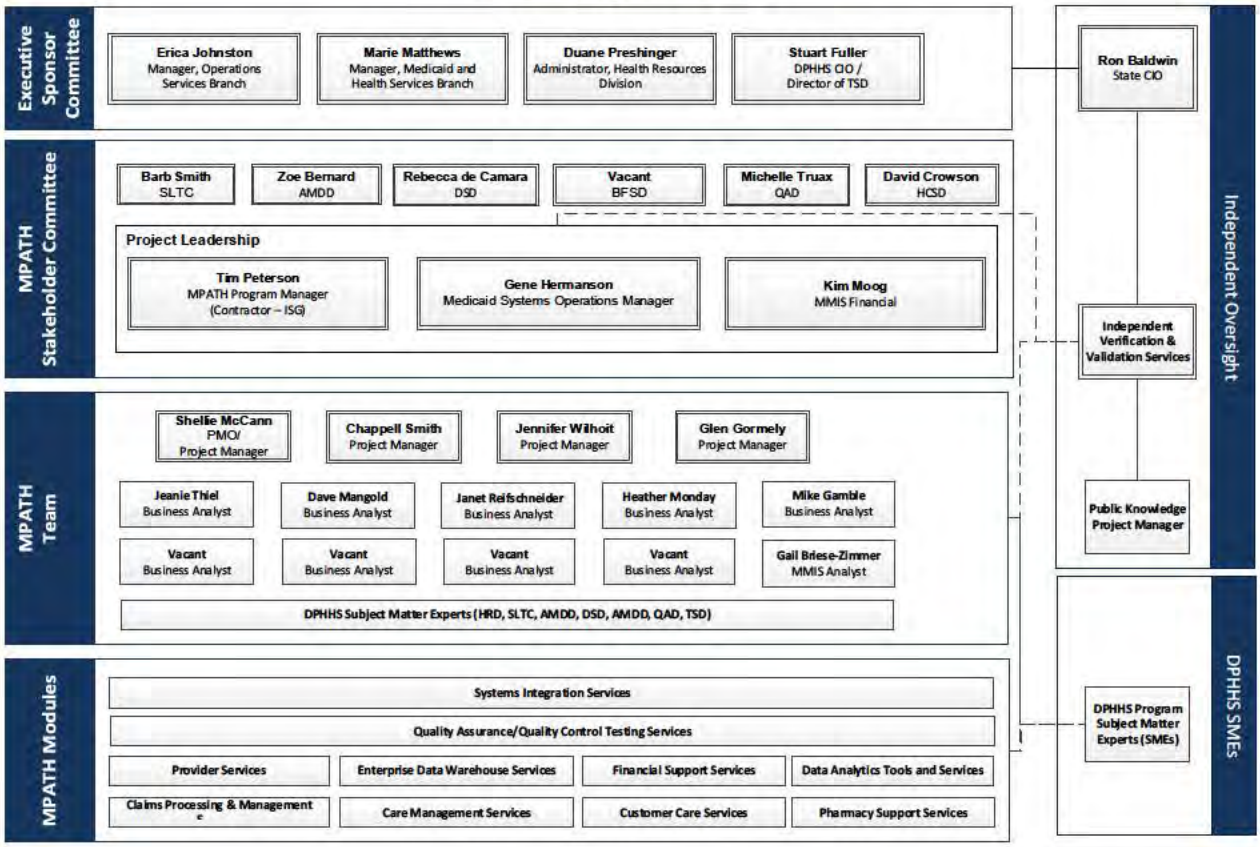
Center for Medicare and Medicaid Services (CMS): CMS is the government entity responsible for authorizing enhanced federal funding for the design, development and installation or enhancement of a state's MMIS. The Mechanized Claims Processing and Information Retrieval Systems (90/10) Final Rule, effective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

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

1. The Medicaid and Health Services Branch of DPHHS is responsible for contractual administration and Fiscal Agent management responsibilities.
2. The Human and Community Services Division (HCSD) is responsible for Member eligibility determinations.
3. The Business and Financial Services Division (BFSD) is responsible for the accounting and financial functions of Montana Healthcare Programs.
4. The Health Resources Division (HRD) is responsible for overseeing and managing the Acute, Physician and Hospital programs. The care management, Healthy Montana Kids (HMK) and Montana Health and Economic Livelihood Partnership (HELP) programs are also located in this Division.
5. The Senior and Long Term Care Division (SLTC) is responsible for overseeing and managing the Nursing Facility Services and Home and Community Based Services programs.
6. The Addictive and Mental Disorders Division (AMDD) is responsible for overseeing and managing the adult mental health, behavioral health, home and community services, and chemical dependency programs. The State funded MHSP is also located in this Division.
7. The Quality Assurance Division (QAD) is responsible for all activities related to Program Integrity and third party liability programs.
8. The Disability Services Division (DSD) does not currently reimburse providers through the MMIS system. However, the DSD will be utilizing the new systems and services procured via the MMIS Replacement Program. This division is responsible for overseeing the Developmental Disability, HCBS waiver and the Children's Mental Health program.
9. For additional information on the State programs and a DPHHS organization chart, please refer to the DPHHS website at https://dphhs.mt.gov/Portals/85/Documents/bureauorgchart.pdf

Table 3.8.1 MPATH Program Structure

Department of Public Health and Human Services
MPATH Program Structure



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

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

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

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

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

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

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

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

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

3.8.2 Impacted Stakeholders

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

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

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

✓ **Optum has read, understands, and will comply with each of the requirements in these sections.**

Optum understands that MPATH encompasses several concurrent projects with parallel work streams being executed by multiple vendors. Inherently, an interwoven fabric of dependencies is between MPATH vendors, external stakeholders, and State departments that must be managed on an enterprise level. It is our experience that project governance is one of the most difficult challenges in this new world of modularity. Optum is recognized for setting the standard for success in managing complex multi-vendor and multi-stakeholder projects.

We have engaged various stakeholders to understand your broader strategic objectives and stakeholder environment. We understand the importance of a governance and delivery approach that balances the interests of your stakeholders, both internal and external. That is why we have made a point to meet with and gain feedback from stakeholders from across the State's health care market.

Our governance approach is multi-layered. The project vision, direction, and priority setting are established at the top-most layer, strategic governance. Then, at the enterprise governance

layer, the vision materializes with the development of enterprise level governance principles. These governance principles help us actualize the vision with the development of the performance metrics, reviews, and reporting in the managerial layer. Each layer further refines and defines the governance model that will be followed throughout the life of the project and managed in the operational governance layer.

Our project team and project manager are supported by our corporate leaders and steering committee. This provides oversight and direction to help our project team align the Optum governance framework to the MPATH Program project governance model.

A good example of this is when we took over as general contractor and technical systems integrator (SI) for the troubled healthcare.gov project in October 2013. Some say that effort was unequalled in its combination of risk and national visibility. The U.S. Department of Health and Human Services Office of Inspector General (DHHS-OIG) recently summarized the project and lessons learned at the August, 2017 Medicaid Enterprise Systems Conference (MESC) saying *"…the breakdown of healthcare.gov was perhaps the most high profile IT failure in American history."*

We stepped in as the project's new leader and overall technical SI. The DHHS-OIG reports that: *"A key decision by CMS during this time was to hire QSSI (an Optum company) as technical systems integrator to serve as an advisor in coordinating technical tasks and resources. By all accounts, this action led to greater coordination between and among contractors and CMS technical staff, and enabled project leaders to more quickly and clearly identify and correct problems and allot resources."*

Optum created a badge-less environment and a culture where bad news could be reported anytime by anyone, regardless of employer or job rank. We used many techniques to get the team moving together and out of unproductive finger-pointing and defensiveness. For example, Optum established a process-driven, collaborative environment to standardize processes and schedules to come into compliance with the CMS PMO's Integrated Master Schedule. We established a cadence for providing a forum for vendors and stakeholders to get together and provide visibility into upcoming changes, risks, issues, and key milestones.

We know how critical it will be for us to work cooperatively with your chosen SI, and all other module providers. We are sensitive to your challenges in managing the MPATH Program and will align our resources and governance model to your governance structure and project entities. Our aim for the MPATH Program is to foster open communications, a spirit of cooperation, and a positive working environment.

3.9 HIGH LEVEL SCOPE OF WORK

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

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

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

so that data and documentation are routed to appropriate unit responsible for decisions on provider enrollment applications. In addition, providers may complete periodic updates and revalidation of their enrollment information via the self-service web portal.

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

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

Additional Provider Services Option A

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

Additional Provider Services Option B

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

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

At Optum, we recognize your objectives to procure provider functionality and services as part of your MPATH effort. We approach your initiative with clear goals – to meet your requirements as stated in the RFP, contributing as a partner in your MPATH program. As your partner, we use our proven innovative strategies to deliver the scope of work for provider enrollment, management and services, on time, and with an experienced, talented team.

To meet your comprehensive requirements, we propose the Optum Provider Services solution. It comprises a technology solution, complemented and supported operationally by our Business Process-as-a-Service (BPaaS) operations methodology.

The Optum Provider Services solution supports and aligns with the MITA 3.0 provider management business area processes, and provides comprehensive management of provider information, including eligibility and enrollment, communication, grievance and appeals, and outreach. We recognize your goals to achieve the "to be" vision based on your MITA State Self-Assessment (SSA). Our solution readily meets those goals, which include the following:

- A Web-based solution for provider management, communication and outreach
- A solution that will collect provider information/attachments necessary to support provider services
- A solution that has automated workflows for provider management
- A provider self-service portal
- A solution that meets NIST security standards, as well as federal and State requirements

Our provider management activities use repeatable, proven practices, focusing on outcomes. One of the tenets of our approach to service excellence is working together with our internal and external users in the overall service operations arena, in a structured and consistent manner. We then strengthen our solution by providing you with a team who has the experience, expertise, and qualifications needed for highly efficient services.

Our extensive health services experience and technical offerings demonstrate that we have the knowledge and skills to help you achieve your goals and objectives for improving health care for Montanans. Our single focus is health care.

Guiding Principles and Objectives

Our proposed solution meets your guiding principles for implementing services that will help you take advantage of progressive technology, and improve interactions and communication with members, providers, and related contractors. Benefits of our solution and approach include the following:

Cost effective: Optum provides you with a cost effective and efficient solution that will support your future strategies for provider management services. We can reduce the cost of implementation using easily configurable, technologies that lower the overall cost of implementing and operating the solution. Our proven effective services strategy and our approach to excellence focus on measurable operational outcomes while maintaining quality.

Benefits

Our solution aligns well with DPHHS guiding principles and objectives that include:

- Cost and value
- Efficiency in data management
- Flexible framework
- Technologies that include vendor-hosted secure environments
- Ease of use

Efficiency in data management: Our data management and governance of data provides consistent data that is timely, accurate, usable, and easily accessible to support you and your administration. The Optum Provider Services solution promotes reusable components by using open architecture and industry and national standards for interoperability, integration, and data exchange. Our solution architecture has been designed to support business-driven functions and the flexibility that easily adapts to an ever-changing health care landscape, new regulations, legislation, and innovations. Scalability of our infrastructure will automatically handle any changes in provider volumes.

Flexible framework: The Optum Provider Services solution is a flexible, rule-based, configurable solution with the services to augment decision-making, increase management

efficiency, and promotes agile adaptability for new and evolving regulations, programs, and initiatives.

Provider Services Solution High Level Scope of Work

Because we are well positioned in the health care market, our solution provides you the benefit of the newest ideas and current industry features within our software and services. In the following table, we present a summary of your scope of work and a high-level summary of the associated value provided by the Optum Provider Services solution.

High-level Summary of the Montana Statement of Work	Value Provided by the Optum Provider Services Solution
Overall provider enrollment and maintenance solution that will accept and process applications through a Web-based provider self-service tool	• Gives providers a cohesive experience across business functions • Can connect to multiple (virtually any) data sources giving the State flexibility • Is easily scalable • Is proven in the marketplace to manage high volumes of users without a degradation in performance
Workflow driven to allow both internal and external users to follow defined business processes to ensure the user experience is optimized and established policies are followed	• [redacted] • Features an extensible and scalable platform • Provides end-to-end visibility and greater transparency
Automated screening and monitoring in compliance with Federal regulations 42 CFR 455.436	• Performs hands-off compliance supporting more efficient operations by using role-based security
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	• Enables reporting on virtually any data elements needed to support operations • Standardized reports that have been refined to provide the detail required to provide decision makers with the tools they need to drive business innovation [redacted]
High degree of configurability to: • Allow enrolling providers to enroll in one or more program types using a single environment event • Collect conditional enrollment and maintenance data that is configurable by provider role • Support real-time edits allowing providers to submit corrections to applications • Allow or prevent provider enrollment based on a variety of characteristics	• Our portal is designed with flexibility, configurability, and program evolution in mind. We built it on a framework, which eliminates the limitations of the past while enabling business needs of today and beyond. • The flexibility of the consolidated solution allows providers to enroll in one or more program types during a single enrollment event. • The solution provides editing that enables providers to quickly submit accurate, corrected applications. • Our solution provides the capability to inspect enrollment criteria based on configuration.
Preference for a "cloud solution"	• Our solution is deployed in a truly [redacted] This will enable DPHHS to experience a lower total cost of ownership, while reducing downtime caused by system failures.

High-level Summary of the Montana Statement of Work	Value Provided by the Optum Provider Services Solution
	• Our solution supports [redacted] and visual abilities, simplify deployment, and enables greater control over parameters. • Our comprehensive virus scanning capabilities provide an additional layer of data protection for your health care information.

[redacted]

The Optum Provider Services solution provides many options for the scope of work. Our commitment to a seamless and effective end-user experience for providers is not just providing a knowledgeable, dedicated staff and a solid, innovative technical solution—it is constantly seeking new ways to serve you better.

NASPO Participation

We recognize and appreciate the State's forward-looking approach to participating in the NASPO. Providing the highest standard of excellence and cooperative contracting provides an important and unified focus to deliver the best value, and reliable competitively-sourced contracts. We look forward to our participation as a NASPO vendor in being able to supply our baseline solution to members of the consortium.

We understand and acknowledge that the pricing of optional services is to be separate in order to align with the optional functionality and services guidelines of NASPO.

Provider Services Option A

The Optum Provider Services solution for Option A delivers a complete provider management solution for future and current State Medicaid providers. Our self-service provider portal is an important gateway for providers to interact with the State's Medicaid Program. This services-based model allows us to provide comprehensive self-service provider services. The comprehensive and streamlined approach combines the best practices of both the fee-for-service (FFS) and managed care models and includes the following:

- Self-service member eligibility and limit verification inquiry
- Self-service claim status inquiry
- Claims-based medical history
- Flexibility to view, upload, and download files
- Online provider appeal request
- Self-service primary care case management (PCCM) member display
- Online access to enter claims

Within our Provider Services solution for Option A, we focus on an easy-to-use portal that promotes self-service functionality within a secure role-based platform. We complement our

solution using our Optum Integration Layer (OIL) to integrate with the MPATH integration layer. In the event that MPATH integration is not production ready, we will use alternate, equivalent methods to support our solution.

Provider Services Option B

Our Option B solution augments our provider services solution by offering a provider operational foundation that includes tools, manuals, processes, and measures that were built and refined over the last two decades. These services include:

- Conducting provider site visits
- Including reference documentation
- Providing technical help desk support and a provider services call center
- Staffing
- Collecting and entering State Auditor's Office financial information
- Providing a provider services call center management system and integrated voice response system/automated voice response system

The Optum Provider Services Option B solution gives you the additional value of our extensive health services, workflow capability, our Virtual Call Center knowledge and skills, and provider oversight.

In the sections that follow, we provide our response to your Provider Services solution scope of work.

3.10 DETAILED SCOPE OF WORK

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

3.10.1 Technical and Information Architecture Requirements

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

Optum acknowledges that the requirements in the Detailed Scope of Work Section 3.10 will apply to the life of the contract with DPHHS unless otherwise noted. We will execute this scope of work as defined in our proposal Attachment G Provider Pricing, aligned with Schedule B and the DDI Payment Milestones.

Collaborative Effort with Systems Integration Services Contractor

It is critical for us to work cooperatively with the Systems Integrator and other module providers. We will work with the contractor on connectivity of our integration layer into your MPATH integration platform. We look forward to helping design the supporting interfaces. Optum has a

demonstrated track record of being successful in a multi-vendor environment. For example, in Massachusetts, the Commonwealth engaged us as the primary SI for the Commonwealth's Health Connector insurance exchange. Optum had already been providing technology and operations support for the Health Connector. Our role was expanded to manage the complex environment that included technology vendors and systems from multiple Commonwealth agencies. Our cooperation with SI includes many of our enterprise data warehouse contracts. This includes the States of Michigan, New Jersey, California, and Illinois, where we manage complex, multi-vendor/multi-agency environments to consolidate health and human services (HHS) data from various sources.

Our proposed technical solution for the MPATH includes a services-based design for data exchange, engineered to provide various capabilities, in an efficient and communicative manner. By leveraging our integration layer, in conjunction with the MPATH Integration Layer provided by the Systems Integrator, we will easily transfer data to and from DPHHS assuring the data will arrive at its intended destination at the intended time.

Technical and Information Architecture Scope of Work

Our event-driven solution uses service technologies and event-driven architecture principles. This enables developing extensible, easily monitored, and de-coupled solutions. The integration solution framework in place today at Optum integrates capabilities spanning applications across the health care landscape. Currently, our integration frameworks support more than 400 million transactions per business day, representing the integration of thousands of services across technology platforms.

We provide configurable transformation rules to deliver a highly flexible and scalable solution. Each module is integrated through the integration layer. Using a set of standard application-programming interfaces (APIs), each module is replaceable, and a unique team manages each module for maintaining updated releases. These products enhance access and delivery by providing open standards-based and service-capable components. The extensibility of the architecture offers multiple entry and exit points into our solution. This promotes flexibility through our integration architecture, with the reuse of business processes and business rules, and using common interfaces.

The Optum Provider Services portal has been developed with our core architectural principles in mind—adaptability, scalability, and flexibility. This enables us to adapt to changing state and regulatory requirements and customize with content management tools rather than technology builds to meet a state's specific needs.

Key Features of our Technical Solution

The solution is modular, including multiple COTS and SaaS products that enable the delivery of Medicaid services using a BPaaS model. We use the following architectural principles.

Architecture Principle	Details
SaaS	• A vendor-hosted secure environment • Eliminates the need for State agencies to incur the expense of purchasing and maintaining servers and software • Enables agencies to significantly reduce the cost of using and maintaining software because Optum bears the responsibility of developing and maintaining the software and infrastructure on which the solution runs
Multi-tenant	• Securely serves multiple tenants (State agencies) in a single instance • Focuses on configuration rather than customization

Architecture Principle	Details
	• Enables DPHHS to efficiently take advantage of COTS product advancements
Open technology and standards based	• Uses J2EE and W3C open standards rather than proprietary technology
Support leading industry standards	• Supports data standards, such as Electronic Data Interchange (EDI) X.12, Health Level Seven International (HL7), and HIPAA, to enable data exchange between various Medicaid Management Information System (MMIS) enterprise systems • Supports accessibility standards (Section 508c) • Uses data transport formats, such as XML, JSON, and CSV
Security and privacy	• Protects data (data at rest security, data transport security) • Provides identity and access management • Runs in a CMS MARS-E and IRS 1075-complaint environment • Runs frequent vulnerability scans to identify any vulnerabilities in the application, operating system, or network and provides immediate remediation actions
Integration and interoperability	• Uses a service framework to enable integration within the Optum Provider Services solution • Provides interoperability with the State systems using Web services and APIs

Key features of our solution architecture include:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

We provide a high-level diagram of our solution in Figure 3.1.

[redacted]

Technology Benefits

[redacted]

[redacted]

Advantage

The scalability, configuration, and deployment automation promote capability through the following:

- Independent versioning
- Testing isolation
- Standards-based interoperability technologies
- Industry standards in technology and interfaces

Technical Architecture Layers

Our technical solution for provider services is engineered for the future, and it is built with security compliance and extensibility as primary features. The Optum Provider Services solution complies with the most current security standards, including HIPAA, CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E), Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) Special Publication 800-53, and Federal Information Processing Standards (FIPS-199 & FIPS 200), as well as many others.

Our solution complies with the CMS Seven Conditions and Standards to enable DPHHS to meet the demands of MITA, HIPAA, and the DPHHS Medicaid environment. Our solution consists of a layered architecture and interfaces that follow MITA principles.

In the sections that follow, we describe our detailed response to the Optum Provider Services solution and content in Attachment F, Requirements Matrix.

3.10.1.1 Compliance

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

Best Practice

Our expert teams routinely review mandates, keep up with new policies, and formulate security and privacy program practices that remain fully compliant and current with health care industry standards and federal and state requirements.

We have extensive experience with the unique requirements affiliated with the health care industry. Adhering to laws, regulations, and standards from federal and state sources can be a challenge to any state program. When combined with the maintenance of your applications' sensitive and protected information, it becomes a massive work effort with complex and sometimes differing rules. As the nation's largest health services company, Optum has dedicated resources to accomplish this task. We help relieve our customers of the burden of having to understand and navigate these complex and overlapping regulations and standards. Our team simplifies this comprehensive maze of requirements by harmonizing laws, regulations, standards, and customer requirements, and applying a tiered-methodology to clarify precedence, overlap, and redundancy.

Based on our work supporting state health care programs throughout the United States, we have developed a thorough understanding of the shared requirements and unique needs that occur within a state Medicaid program. We have reviewed your RFP, including the specific compliance requirements and data types specified. We determined that the Provider Services module requires compliance with information security regulatory and control standards that include:

- Privacy Act
- HIPAA
- FISMA
- NIST 800-53
- FIPS
- CMS Acceptable Risk Safeguards (ARS)
- CMS MARS-E
- IRS 1075 for Federal Tax Information (FTI)
- DPHHS security policies
- Optum security policies

The Optum Provider Services solution data elements will include personally identifiable information (PII), protected health information (PHI), and other sensitive information. Building on our expertise in this area, we designed our solution to support compliance with these federal and state privacy and security regulations.

Optum has experience applying, implementing, and maintaining CMS ARS, CMS MARS-E, IRS 1075, and HIPAA security control standards. Our capabilities in this area have proven successful in many critical federal and state government health care technology solutions. Our customers successfully achieved first-attempt receipt of Authority to Connect (ATC) / Authority to Operate (ATO). These ATCs and ATOs require both a security control self-assessment and third-party assessment of the implementation of security and privacy controls within these

control standards. These assessments verify and validate the security controls have been implemented and that they are operating as intended.

Our continuous monitoring program for CMS control standards further provides our customers with the knowledge and comfort that the confidentiality, integrity, and availability of their solution and sensitive PHI data are securely maintained over the life of the project.

We have made long-term commitments and investments in support of MITA alignment. We designed and built our solution to comply with MITA and satisfy the Seven Conditions and Standards. At the heart of CMS's direction for the Seven Conditions and Standards is the need for MMIS flexibility, adaptability, and extensibility.

In the following section, we provide our responses to the RFP requirements for applicable to compliance as identified in RFP Attachment F, Requirements Matrix.

CMP01 The Contractor shall, upon request by the State or at the end of the contract, transfer or destroy all documentation in the custody of the Contractor. The Contractor shall provide the transferred records and data in a format agreed upon by the State.

After contract termination or at the request of the State, we will transfer or destroy all project documentation in our custody. We will manage your documentation based on a combination of factors. Then, we will document these factors in the Turnover Plan, which we will develop and deliver to DPHHS for review and approval. These factors include the following:

- Transition to any successor contractor
- Applicable law regarding the retention of government information, as defined in the RFP
- Applicable law and any privacy and security regulations and State policies regarding the retention and/or destruction of sensitive government information, including, without limitation, PHI, PII, and FTI

As a leader in the health care industry, Optum understands the importance of protecting client data. We have established policies and security controls that are fundamental and encompassing for the protection and management of all client data. We have implemented enterprise-wide data retention and destruction policies for the protection and destruction of all data assumed from the State. Our media disposal and sanitization requirements support compliance to NIST Special Publication 800-88: Guidelines for Media Sanitization. These policies state that hard and soft copies of all protected information must be destroyed prior to disposal, or disposed in a secure manner in compliance with applicable federal, state and international laws and contractual commitments. We record a certificate of destruction for all records destroyed to provide an accurate record tracing and inventory of client data. We also provide all data to the State in the agreed-upon format and stipulated in the BAA.

CMP03 The Contractor shall notify the State in writing within five (5) business days following initial detection of suspected fraud or abuse and provide supporting documentation.

We will notify the State in writing within five business days after we initially detect suspected fraud or abuse and provide the supporting documentation. Optum understands and appreciates the impact fraud and abuse can have on a State Medicaid program. We will develop a comprehensive plan to address the issues your programs may face. Our close involvement with provider and member information will give us an important opportunity to discover aberrant Medicaid program activity. We will provide you with timely, credible, and reliable information.

During implementation, we will work with you to define a business process or align our business process with yours to establish a workflow queue and email group for sending notifications to your Medicaid Fraud Control Unit (MFCU). Working together, we will define the policies and

procedures we will follow to notify the State, the claims unit, the call center, or other groups of suspected fraud or abuse. If we identify potential fraud and abuse during our reviews or other means, we will proceed through our internal due diligence processes to confirm the initial discovery of inappropriate use. If we confirm the discovery, we will add a new item to the workflow queue. Using the workflow, we will generate an email to MFCU, write free-form text notes, assign or reassign the workflow item, or send the item back to operations following our agreed-upon procedures.

CMP04 The Contractor's solution shall have full integration of the MITA initiative with business, architecture and data required to support the State's healthcare programs.

The Optum Provider Services solution embraces the MITA Business Model and Architecture framework. Our solution will provide you the best value and support of enterprise perspectives, performance, and interoperability standards for your MITA goals for technology.

Enterprise perspective: We designed and developed our solution with an enterprise perspective. The integration services powered by OIL include communication protocols for integration with systems and sources of data across the solution ecosystem. OIL also enables communication with other ESBs or data hubs and provides flexibility to adapt to your changing needs over time.

Performance driven: Our management rigor coupled with our solution architecture enable us to drive the performance of the DPHHS solution to meet and exceed service level agreement (SLA) targets. We achieve this through rigorous application of management principles. These principles include, project and risk management, change control and release management, coupled with responsive and adaptable systems that enable proactive issue detection and resolution.

Flexibility: Our solution adheres to MITA guidelines and the principles of modularity. To achieve alignment with MITA, our solution leverages proven COTS and SaaS components. This modular approach provides flexibility to modernize over time as COTS components can be interchanged without compromising the integrity of the overall solution.

Interoperable: OIL drives interoperability through its library of core integration capabilities, canonical data model, and the use of proxy services, OIL leverages the integration library and allows rapid design, development, testing, and integration of new services. All modules and systems that attach to the ESB need only be capable of communicating with an OIL proxy adapter.

A canonical data model is used to communicate between different data formats. It can reduce costs, standardize on a common reusable data format, and minimize dependencies when integrating applications that use different or non-conforming data formats. If a new application is added to the integration solution, only transformation between the new application and the data model has to be created, independent from applications that already participate. Using a canonical data model enhances the re-usability of services and simplifies the integration architecture. Figure 3.2 illustrates a hypothetical scenario of interfacing between any external system and our solution through OIL.

[redacted]

CMP05 The Contractor shall adhere to data retention requirements cited in 45 CFR 164.316 and Administrative Rule 37.85.414. The Department may require a longer retention period on an exception basis to support ongoing business needs (e.g., TPL recovery and drug rebate).

Optum has established policies and security controls that adhere to data retention requirements cited in 45 CFR 164.316 and Administrative Rule 37.85.414. These policies state that data will

be retained for at least six years in a secure manner in compliance with applicable federal and state laws. Our policies enforce the retention of information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. We can implement longer periods of retention of records based on business needs and client exceptions as necessary.

CMP06 The Contractor shall have written policies governing access to, and duplication and dissemination of all individual or entity information.

We have a written data security policy in place governing our access, duplication, and dissemination of information on individuals or entities. We can share this policy with DPHHS on request. The policy requires us to use and disclose data only as permitted by applicable laws, regulations, individual authorizations, customer contracts, and company policies.

Our data security policy applies to our employees, contactors, and business organizations within our enterprise (including affiliates and subsidiaries). The policy also applies worldwide to data used and disclosed by us or on our behalf. Every Optum employee is required to comply with these policies.

CMP07 The Contractor shall comply with all sections of the Americans with Disabilities Act (ADA), Section 508 of the Rehabilitation Act and ensure user interface standards account for the various forms of colorblindness.

We will comply with all sections of the ADA, Section 508 of the Rehabilitation Act, and validate our user interface standards for the Optum Provider Services solution accounts for the various forms of colorblindness.

Our proposed solution uses modern Web browsers to deliver the user experience. Our solution complies with all applicable federal, State or other applicable regulations, guidance and laws as you require. Optum conducts considerable business in the federal, state, and local public sectors in conformance with their regulations and standards.

The internal and external Web pages of the Optum Provider Services solution are rendered through mature commercial applications that contain compliance statements for Section 508 of the Rehabilitation Act of 1973. We also have an extensive process for accessibility testing encompassing the following:

- **Definition:** Accessibility is usability for the different ways people access the Web. Web accessibility means that people with disabilities can perceive, understand, navigate, and interact with the Web, and that they can contribute to the Web.
- **Development:** Optum has a dedicated center of excellence for user experience, the UX Design Studio (UXDS). UXDS is team of more than 150 designers, researchers, user interface developers, accessibility experts, and other professionals who provide guidance to developers on user experience and accessibility. Our developers have access to the latest tools, trainings, templates, and frameworks recommended by experts to support accessibility.
- **Usability testing:** Usability is the central focus of our approach to Web interface design. The U.S. Department of Health and Human Services Research-Based Web Design and Usability Guide is our blueprint during the Design Phase. Following the Design Phase, we will use automated and hands-on tests to test our user interface on key features of usability. These will include the ease in finding key information, page flow, print layouts, response time, ability to complete tasks, and desktop browser/mobile usability.

  During the Testing Phase, we will follow a Usability Testing Protocol to perform hands-on testing of the user interface. The unit, regression, and integration testing will cover all

configuration changes and custom development to meet the State's needs. This will include identifying personas and fictional representative users who share attributes with your typical users. We will use these personas for multiple test scenarios throughout the testing process and will enumerate critical tasks, both for the user and stakeholder. From the task list, we will create a Usability Testing Protocol that contains the non-biased moderator script and testing criteria. In addition, we will usually perform testing as a one-on-one experience between a tester and a moderator, and we will record and analyze results and share with the development team. This methodology will help us verify that the interface we deliver meets your users and stakeholders' needs. Optum runs a dedicated User Interface Experience (UIX) lab to help project teams meet interface requirements. The project team will have access to the UIX and its personnel, as needed.

We have a dedicated team that tests Web pages for accessibility. The team evaluates each page against a list of almost 100 practical checkpoints covering WCAG 2.0 Levels A and AA success criteria and Section 508 guidelines (including Software and OS 1194.21, Web and Applications 1194.22, Video and Multimedia 1194.24, Functional Performance 1194.31). In addition, the team evaluates each page with automated and manual checks of function, content, zoom/resizing, color and others using a combination of mouse with monitor, keyboard-only and screen reader with keyboard to represent a range of experiences.

- **Accessibility testing:** Our accessibility testing will validate that the analytics solution we deliver is accessible to individuals with disabilities. It will also verify that they can interact with the system as needed.

Beginning in the Design Phase, we will perform Section 508 compliance reviews on user interfaces. Our graphic designers understand the needs of users with visual disabilities. They know how to create a wide variety of accommodations for these users. After the Design Phase, we will perform automated and manual testing of Web tools to validate full accessibility compliance further.

CMP08 The Contractor and its services, work products and final deliverables provided by the Contractor applicable to the services described in the scope of work shall be knowledgeable of and in compliance with pertinent State and Federal Statutes, CIO Promulgated Rules, State IT policies, rules, and standards for required system hardware, software and development tools and processes, and operational procedures when completed and accepted by the Department. The Contractor shall also be aware of upcoming changes to existing rules and regulations as well as new rules and regulations that may impact the scope of work.

Our past experience and successes supporting clients in the government space strengthens our understanding of all Federal Statutes, CIO Promulgated Rules, State IT policies, rules, and standards. This experience and extensive understanding of all mandated policies and rules enables us to provide the capabilities to support all such policies in our tools, processes, and operating procedures. We adhere to and continually update all mandated rules and policies using a multidisciplinary team approach. We leverage extensive continuing education and training resources to keep our security and compliance teams ahead of any changes, updates, or redrafting of defined rules and policies.

CMP09 The Contractor shall adhere to recognized best practices during the execution of the scope of work including the latest version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series related to cyber security.

Optum maintains a knowledgeable and experienced multidisciplinary team of experts focused on compliance and Information Assurance best practices for cyber security. We have mature risk management, compliance, and audit programs that help maintain a strong security posture.

We research, document, and develop all security controls using the latest versions of the NIST Special Publication series documents. We monitor the NIST Websites to address any new or emerging publications to gather the most current guidelines and support the implementation of those guidelines to secure the confidentiality, integrity, and availability of all information technology systems.

CMP10 The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions-MITA Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data.

We support and share your goal of maintaining compliance with the "to be" vision of MITA 3.0 Conditions and Standards-MITA Condition and current MITA version to advance in MITA maturity for your business, architecture, and data. We developed the Optum Provider Services solution to completely align with the MITA business, information, and technology architectures. By making this investment and commitment, we keep our products and services current with emerging technologies and industry standards in the MITA 3.0 formats. This enables us to support the approval process and significantly enhance the MITA SSA process. We have supported the MITA vision and guidance since its inception. It drives our services and provides the framework for the systems and processes we produce.

The Optum Provider Services solution will comply with all of the CMS Seven Conditions and Standards. At the heart of CMS's direction for the Seven Conditions and Standards is the need for MMIS flexibility, adaptability, and extensibility. Our solution maximizes these features, delivering high-quality, predictable, and secure services.

We built the Optum Provider Services solution on configurable and extensible COTS products relevant to the Medicaid mission. Each COTS component has a roadmap for its functionalities to stay relevant in the market and to comply with federal regulatory and industry requirements. The COTS roadmaps often have the regulatory needs planned into their maturation process before our state customers request the solution change. Most regulatory changes are handled through COTS Product Lifecycle Management (PLM) release implementations and system configuration changes as needed.

CMP11 The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions - Industry Standards Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The Contractor shall ensure alignment with, and incorporation of, industry standards, HIPAA, privacy and transaction standards; accessibility standards, and standards that provide greater accessibility for individuals with disabilities and standards under the Affordable Care Act.

Our solution supports the MITA Industry Standards Condition. A key benefit of our SaaS-based solution is it provides technology that stays current with industry changes. We will apply and maintain upgrades on a regular schedule in our foundational COTS products, delivering non-disruptive currency with federal standards and regulations. If required, we will apply a change release between the predefined releases to maintain federal or state compliance. Our solution will maintain compliance with current federal HIPAA, Health IT, HITECH, and ACA regulations at implementation and throughout the life of our contract with DPHHS.

The Optum Provider Services solution complies with the following standards:

- We created our solution leveraging HIPAA EDI standards like X.12 5010, XL7, NCPDP D.0; support industry standard code sets, including ICD-10-CM/PCS, CPT, and HCPCS; and industry methodologies, such as National Correct Coding Initiative (NCCI).
- Our project management methodology follows the PMI Project Management Body of Knowledge (PMBOK®) Guide, the Carnegie Mellon University, and the Software

Engineering Institute (SEI) principles described in the Capability Maturity Model Integration (CMMI) framework.

- Our solution adheres to American National Standards Institute (ANSI) and Information Technology Infrastructure (ITIL) standards where applicable.
- We built our solution architecture using industry-recognized The Open Group Architecture Forum (TOGAF©) standard framework and supporting tools.
- We use common protocols and transaction standards for our interfaces. Our solution's security measures incorporate requirements from HIPAA, CMS, PCI, and other prevailing control authorities.
- Our portal framework complies with Section 508 and Web Content Accessibility Guidelines (WCAG) 2.0 and maintains compliance through periodic reviews.

CMP12 The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions - Leverage Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The Contractor shall promote sharing, leveraging, and reuse of healthcare technologies and systems within and among states.

Optum designed the Optum Provider Services to align with MITA 3.0 and comply with the CMS Seven Conditions and Standards, including the Leverage Condition.

At the heart of CMS's Seven Conditions and Standards are system adaptability, flexibility, and extensibility. Our solution maximizes all three, delivering high-quality, predictable, and secure services for DPHHS.

In general, our solution can quickly change automated workflow configuration based on roles, security levels, and specific criteria or qualifying events. All workflow changes are captured and can be used in audit process reporting. Using numerous data elements, we can create any number of workflows and route them to the appropriate queues as necessary. Our supervisors monitor these work queues using aging reports to verify no work is lost in the queue. They manage the queues and distribute workloads accordingly to meet operational SLAs.

The highly configurable solution components enable us to expediently define and manage rules and workflows for provider enrollment and re-validation and provider configuration, all without developer intervention. This means quicker response times to implement changing requirements helping DPHHS achieve timely accurate outcomes.

Aligned with MITA 3.0

The MITA 3.0 framework describes a structure for you to implement your solution aligned to a defined architecture framework. This framework includes three parts: 1) Business Architecture (BA); 2) Information Architecture (IA); and 3) Technical Architecture (TA). Each of these MITA architectures aligns with the CMS Seven Conditions and Standards. By leveraging the Optum best practices and technology advancements, along with industry standards, the processes and guidelines used to build the Optum Provider Services solution provides a cohesive method for meeting Medicaid objectives.

Our solution's modular design incorporates best practices and lessons learned from our successful operation of commercial systems and Medicaid FFS systems. As an integrated, modular COTS-based solution with open systems architecture, the solution is scalable and extensible. When extensibility is required, we can add or remove service components to satisfy specific business requirements as they evolve over time. As service volumes increase or decrease, our solution can scale to meet processing demands. The Optum Provider Services solution also provides DPHHS with a solution that delivers extensive interoperable capabilities

to share and exchange data with exchanges, public health departments, and other local, state, and federal health and human services agencies.

MITA Business Architecture

The Optum Provider Services solution will provide DPHHS with a set of services, through the Service Layer, that help achieve your business goals and objectives.

We used the business categories in each of the 10 MITA 3.0 Business Areas as the primary source for capturing and further defining the Medicaid enterprise business processes and IA requirements for managing FFS providers.

MITA Information Architecture

The key information system elements contained in our solution's Data and Application Layers include the information itself, the applications that use the information to enable the business processes, and combining applications and information to support the enterprise's business functions. Together, the MITA business and IA map enterprise data to business processes. The MITA IA also serves as the bridge between the MITA business and the MITA technology architectures by providing the framework to move from the MITA business information requirements to the MITA technology message requirements. The Optum Provider Services solution and processes align closely to the MITA IA framework as follows:

- [redacted]

The core Provider Services approach includes a common reporting database to support operational and state reporting capabilities. Administrators can schedule reports, automatically generated daily, weekly, monthly, quarterly, annually, or user-defined based on business need. Reports are rule/role driven allowing the accessibility of each report to be defined at the user level.

MITA Technical Architecture

The Optum Provider Services solution and processes align closely to the MITA TA framework.

Technical management strategy: The enterprise architecture of the solution is based on the MITA and Optum BA capability models. For our solution, we focused on using COTS applications to the greatest extent possible. Our approach was to integrate the various applications using SOA components, built around SOA standards, to provide the loose coupling, and increased agility to change as the market changes. Our vendor-hosted NIST-compliant approach is built on established infrastructure and security models to help us gain the performance and security needed to keep information safe.

Business services: The Optum Provider Services solution's business services follow the MITA 3.0, BA. This has enabled us to align to CMS's goals and objectives, remain technology neutral, and provide the performance and flexibility we will need to support DPHHS.

Technical services: We designed our solution to be a multi-tenant solution with modularity and interoperability as a core architectural tenant. We have flexibility to change one component without having to change other related components. The ability to abstract the interfaces between applications gives us flexibility, agility, and security that we require from our solution.

Technology standards: Our technology stack aligns to the MITA TA technology standards reference model. Our solution has standards identified at each of the layers that enable consistent integration and interoperability.

Technical Capability Matrix (TCM): Most of the solution aligns to the MITA 3.0 level 3 - 4 technical maturity capabilities. We have used the assessment of our solution against the TCM as one of our considerations for building the product and service roadmap to drive advanced MITA maturity capabilities.

CMP13 The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0 Standards and Conditions -Business Results Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The Contractor shall support effective communications with providers, and the public.

The Optum Provider Services solution supports the MITA Business Results Condition. We have a record of returning business value for our customers' investments. Our reliable solutions store and process granular data before transformation, remain balanced, and have full traceability to source systems. Our data centers process more than two billion claims per year with better than 99 percent accuracy. We also electronically transmit more than $100 billion in annual payment value to a network of more than one million health care providers. Additionally, our Virtual Contact Center supported more than 300 million calls in 2016.

Based on an innovative SaaS model, the Optum Provider Services solution delivers significant business value and savings to DPHHS, including:

- A provider portal promoting self-service functionalities
- Near real-time transaction processing
- Key Performance Indicator (KPI) dashboard reporting and performance management
- Complete audit trails for transparency in provider enrollment and credentialing

CMP15 The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0-Standards and Conditions- Interoperability Condition or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The Contractor's solution shall ensure seamless coordination and integration with components, other systems and allow interoperability with health information exchanges, public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services and federal data sources.

The Optum Provider Services solution supports the MITA Interoperability Condition by using [redacted] The Services Layer supports the business processes for reusability and maintainability. Each product performs a specific function within the solution architecture.

Technologies supporting our solution include an externally published Web services and API catalog, a unified gateway using Web portals, standards-based HIPAA Gateway, and security services. Common protocols and transaction standards and files include:

- W3C SOA-compliant SOAP message with Web Service Definition Languages (WSDLs)
- Clearly defined XML message structures for data passed through a Secure File Transfer Protocol (SFTP) Gateway
- 837I/P/D, 835, 834, 270/271, 276/277, 278, and 274 transactions
- HL7 and other standards for connecting with HIEs
- Other EDI and file interoperability standards

During implementation, we will work with you, your other vendors, and your stakeholders to identify all integration opportunities and design implementation plans for each one. During operations, we will accommodate new integration services and opportunities, as they are developed to support interactions with other entities as your enterprise matures.

Optum established a Community of Practice (CoP) devoted to clinical interoperability. The professionals involved with the CoP work to adopt best practices at Optum and educate staff on interoperability. This focus on interoperability allows us to develop the Optum Provider Services solution technologies and an approach to implementation that provides seamless coordination and integration with other agencies and organizations.

CMP16 The Contractor shall be knowledgeable of and support the Department to maintain compliance with the "to be" vision of MITA 3.0-Standards and Conditions- Modularity Standard or the latest MITA version that requires states to align to and advance in MITA maturity for business, architecture and data. The Contractor's solution shall use a modular, flexible approach to systems development, including the use of open interfaces and exposed Application Programming Interfaces (API); the separation of standardized business rule definitions from core programming; and the availability of standardized business rule definitions in both human and machine-readable formats.

The Optum Provider Services solution supports the MITA Modularity Condition. We designed and built our solution on SOA principles, and it uses modern SOA tools and methods. The design and function includes both open interfaces and exposed APIs. Business rules are deliberately separated from core programming and functional components. We have thoroughly vetted and tested each COTS product to provide configurability for business processes, rules, and functions. We selected each one to perform a specific function within the Optum Provider Services solution. [redacted]

[redacted]

The Optum Provider Services solution can serve as an ESB and integrate with existing ESBs. It isolates the components into user interface, programmatic administration, shared service, and management service modules to maximize reusability and scalability.

We employ a specific selection process for each COTS product and replace components seamlessly as technology and business processes demand. The Optum architecture team uses the Impact Evaluation Tool (IET) to validate how well one or multiple solutions meet business requirements. We use this method to select the optimal solution based on objective decision-making with a full understanding of the pros, cons, and risks. Our enterprise architecture team leads this review, which is a collaboration with the IT and business teams. The process involves listing the requirements needed for the solution, assessing total solution impact (including both business and IT), and assigning specific weighting on the importance of the requirements. The resulting calculations appear under each solution option, enabling an objective decision for the right solution fit. We use this process throughout Optum to identify best-in-class solutions.

We also use this process to add new tools and capabilities to our solutions without affecting current components. In this way, we can offer state-specific solutions to meet the objectives of the Medicaid Enterprise System (MES) roadmaps without compromising the design and core services.

The Optum Delivery Model integrates key project disciplines and standards-based project management methodology with our proven SDLC, the Optum Scalable Agile Method. Enabled through Agile development, we can independently update, upgrade, or even sunset individual components of the solution without affecting other components and services. Our solution is modular in each aspect of the standard, providing flexibility and configurability. It also promotes the maturity of the Modularity Standard by reusing business processes and business rules and using common interfaces.

CMP17 The Contractor must provide the Department with compliance assurances for the Contractor scope of work.

Because of our commitment to excellence and past support of government clients, we understand the compliance assurance requirements inherent in the scope of work. We will provide assurances that compliance with those requirements is fully met.

CMP18 The Contractor shall be fully compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-1919) and Administrative Simplification (Subset of Title II) requirements in effect as of the date of release for the RFP and with any changes that subsequently occur, unless otherwise noted.

We implement HIPAA regulations as specified by the U.S. Department of Health and Human Services (HHS), Office of Civil Rights (OCR) in the Code of Federal Regulations (CFR) Title 45, Subchapter C, Part 165, Subpart E (Privacy of Individually Identifiable Health Information).

Optum has an extensive HIPAA compliance program that includes the following:

- Dedicated resources to monitor HIPAA legislation and support timely implementation
- An enforcement program to check for HIPAA compliance and a training program that requires Optum employees to successfully complete required HIPAA training programs
- Monitoring of ongoing compliance with the components of HIPAA administrative simplification that have been promulgated by the U.S. Department of Health & Human Services

CMP19 The Contractor shall enter into a Business Associate Agreement (BAA) prior to the initiation of work. The Contractor and the Department acknowledge and agree that the Business Associate Agreement is subject to HIPAA, and the HIPAA implementation regulations thereunder, and the Health Information Technology for Economic and Clinical Health Act (HITECH), and the HITECH implementation regulations thereunder. Under the Agreement, both parties are responsible for security and privacy compliance and must take advantage of the appropriate security capabilities and measures and adequate data validation, as well as have appropriate policies and procedures in place to minimize or prevent unlawful access by any person who may have access to the entire database.

Optum will establish Business Associate Agreements (BAAs) or contractual agreements with any subcontractors having access to data subject to protection by HIPAA and HITECH, and with the State. This will occur following contract signature and before starting work.

CMP20 The Contractor shall ensure all information not specifically identified as Protected Health Information (PHI) or Personally Identifiable Information (PII) as defined under HIPAA and/or HITECH is treated as privileged communications, held confidential, and must meet the terms and conditions specified in the RFP, BAA and Contract.

Optum maintains a knowledgeable and experienced multidisciplinary team of experts focused on compliance and information assurance best practices for cyber security. We have mature risk management, compliance, and audit programs that help maintain a strong security posture. We research, document, and develop all security controls using the latest versions of the NIST Special Publication series documents. We monitor the NIST websites to address any new or emerging publications to gather the most current guidelines and support the implementation of those guidelines to secure the confidentiality, integrity, and availability of all information technology systems.

CMP21 The Contractor shall ensure that except as provided by law, no information in the possession of the Contractor about any individual shall be disclosed without prior written consent.

Optum understands the responsibility to protect confidential and proprietary information assets. This commitment is integral to the relationships we have with all of our clients and vendors. We also understand the sensitivity and seriousness of PHI and PII data. To this end, we implement strict guidelines and data controls so that only qualified individuals have access to private data. We will not share or disclose any data without prior written consent.

Our policies, procedures, privacy practices, incident management, and protocols relative to the protection of information assets (both confidential and proprietary), mandate that employees attend annual HIPAA training and are all responsible for protecting the confidentiality and privacy of all data.

CMP22 The Contractor shall follow all applicable technical standards for site and system security policies and procedures to protect the Department's healthcare data and information systems.

Optum supports many government clients and has the experience and expertise necessary to implement a comprehensive security posture. We incorporate industry best practices and risk assessment guidance found in frameworks, such as the NIST 800-53, CMS MARS-E and CMS Acceptable Risk Safeguards (ARS). This defense in-depth approach to information security protects the confidentiality, integrity, and availability of client data and information systems. Our technical and system security policies adhere to the level of security compliance mandated by the governing framework.

CMP23 The Contractor's data management approach and operational policies shall meet HIPAA, HITECH, ARRA and other federal and State privacy and security requirements.

We meet security and compliance controls required by HIPAA, HITECH, ARRA, as well as other applicable federal and State privacy and security requirements. Our data management approach is based on industry best practices.

CMP24 The Contractor's solution shall be compatible with multiple standard browsers in accordance to the State's IT Standards which can be found in the Procurement Library. The solution shall allow access from standard browsers without requiring specialized plug-ins or applets to function.

As the following table shows, the Optum Provider Services solution is technology-neutral and poses no client system limitations. Because our portals are accessible from the DPHHS website using a browser, our solution does not require a specific operating system or additional plug-ins and controls.

System Requirements	Limitations
CPU Limitations	None
Operation System Limitations	None
Web Browser Compatibility Limitations	None
Framework, Plug-in or Application Requirements	None

Our solution supports industry-standard Web browsers[2] that include the following:

- Microsoft Internet Explorer 7.0 or higher
- Mozilla Firefox 3.6 or higher
- Apple Safari 3 or higher
- Google Chrome 10 or higher
- Opera 43

CMP25 The Contractor shall retain, all original paper documents for fifteen (15) calendar days from the date the documents are received and have been scanned, indexed, stored in the ECM and meet verification process standards. Original documents may be destroyed once indexed and stored in the ECM and the retention period is met in accordance with State and Federal guidelines.

In compliance with your requirements, we will retain all original paper documents for 15 calendar days from the date the documents are received and have been scanned, indexed, stored in the ECM and meet verification process standards. After 15 days, we will work with our partner, SourceHOV, to destroy the documents.

Document management is a critical function for transaction processing systems. For the Provider Services module in particular, inbound mail receipt, sorting, and scanning are key activities in the project requirements. For the Optum Provider Services solution, the Optum Remote Mail Office (RMO) will manage inbound mail services through our partner SourceHOV. We will use SourceHOV COTS software to provide integrated fax services. Our Enabling Services team will be responsible for document management. We will integrate this function through our core solution offering. As a result, these capabilities will present to the provider as a single approach.

CMP26 The Contractor shall maintain an auditing system and employ accounting/auditing procedures and practices that conform to GAAP and GAAS. All charges applicable to the contract shall be readily ascertainable from such records.

Our corporate culture, which all Optum employees must represent in our daily work, includes a strict adherence to ethical standards. This includes the standards defined by our organization,

[2] According to **netmarketshare.com**, the above listed browsers cover 98 percent of Internet traffic (https://www.netmarketshare.com/browser-market-share.aspx?qprid=2&qpcustomd=0).

our customers, and federal and state regulations including Generally Accepted Accounting Principles (GAAP) and Generally Accepted Auditing Standards (GAAS). We maintain strict financial and operational auditing and compliance controls including the segregation of operational duties. These controls support the separation of functions and employees to maintain the security of financial information.

Based on your response to vendor questions, we understand and acknowledge that this requirement is related to the financial transactions processed by the Provider Services module. In addition to operational and auditing financial controls, our solution includes and auditable record of all financial transactions processed by the system. All transactions are maintained, along with the system process or user that performed the transaction, all dates associated with the transaction, and any change made to financial data. Access to this financial audit information is readily available to authorized DPHHS staff through our electronic payment gateway component of the solution.

CMP27 The Contractor will ensure that all technologies implemented are in compliance with any End User Licensing Agreements or other licensing arrangements.

The Optum Government Contracts, Legal Department, and Enterprise Sourcing and Procurement organizations review the technologies proposed in all government contracts with applicable subject matter experts (SMEs) conversant with the technology and use cases of the technology. As part of that review, these organizations consider the scope of third-party software and review other technology arrangements to confirm that Optum has obtained the necessary rights from the vendor to propose usage by Optum and/or our government customers for the particular contract. In addition, our proprietary software and technology undergoes a similar review regarding having the proposal response and eventual contract reflect appropriate end user license and/or SaaS use and access terms given the use case contemplated for the offering. Through such review, we confirm what steps, if any, are needed, to comply with any End User Licensing Agreements or other licensing arrangements.

CMP29 The Contractor shall comply with Affordable Care Act Section 1104 Administrative Simplification, and Section 1561 Health IT Enrollment Standards and Protocols.

The Optum Provider Services solution supports the sections listed in this requirement (i.e., Section 1104 Administrative Simplification, and Section 1561 Health IT Enrollment Standards and Protocols) of the ACA. We designed our solution to meet regulatory standards and applicable laws to achieve the goals for these sections, which include the following:

- **Administrative simplification:** We are committed to help relieve the administrative burden on providers. We can help accomplish this goal by making sure the Optum Provider Services solution enables electronic exchanges of data with groups and entities, such as providers, stakeholders, other states, and federal agencies.
- **Support of electronic exchange of data:** We use XML/JSON/X.12 formats as applicable.
- **Intuitive user interface:** Our intuitive provider portal has various help features and answers to frequently asked questions that enable providers to have essential information readily available during enrollment. These features can help reduce the number of help desk calls from providers and increase their self-sufficiency.
- **Simplification of documents:** We will work with DPHHS to simplify enrollment documents and reduce paperwork for providers.

- **Streamlined process:** The Optum Provider Services solution provides a streamlined enrollment process for providers to apply, recertify, and manage their eligibility information online.
- **Multi-channel communication:** Our solution provides notification of eligibility, recertification, and other provider communication regarding eligibility using various communication channels. These include email and mobile phones.

CMP30 The Contractor's solution shall ensure that all data necessary for legal requirements is retained.

We will retain government information that is necessary or useful to fulfilling our document retention obligations defined in the RFP, the contract, and applicable law. To the extent that retaining government information is not necessary, Optum will transfer the government information to DPHHS or a designee, destroy, or otherwise delete the government information if technically feasible to do so. If not technically feasible to do so, we will provide DPHHS with a certification summarizing the government information that we cannot return, destroy, or delete. Optum will include a statement indicating that such government information will remain protected until the applicable government owner otherwise releases such information into the public domain.

CMP32 The Contractor shall provide a mechanism to purge source documents in accordance with HIPAA security provisions and State requirements.

[redacted]

3.10.1.2 Security

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

Protecting the confidentiality of your data is a top priority for Optum. Our solutions follow industry best practices and security requirements of applicable standards and regulations. We integrate security into our architecture throughout our solution design process. Because security is not static, we continue to refine security to minimize security risk and assure our commitment to confidentiality, integrity, and availability.

This approach enables us to identify and verify the regulatory requirements and controls required to meet compliance throughout our partnership with you.

[redacted]

[redacted]

The remainder of this section contains our responses to the RFP requirements applicable to security as identified in Attachment F, Requirements Matrix.

SEC01 The System shall provide a physical and electronic environment that uses public key infrastructure to verify all transactions and the identity of all users and denies access to unauthorized users. For example:

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

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

[redacted]

[redacted]

SEC02 The Contractor shall ensure that any data being transmitted or transported either physically or electronically will be encrypted.

[redacted]

SEC03 The Contractor shall ensure that any unneeded hardware, software, and licenses have been decommissioned.

As discussed previously, we work with our contracts, legal, and sourcing and procurement organizations to maintain the correct licensing for hardware and software infrastructure components. We complete a process to confirm that all infrastructure components are needed to support the contract and performance metrics, and that any unnecessary infrastructure is identified and removed through our decommissioning process. Software and hardware decommissioning is treated as an IT project, and IT teams are tasked to complete decommissioning without any incident. Plans to decommission components are drafted well in advance of removal, and are thoroughly tested. When the testing is successful and approved, the infrastructure component is decommissioned according to the approved plan.

SEC04 The Contractor shall protect all government data from loss or unauthorized disclosure.

Data is protected against loss by industry best practices, a blend of applicable regulatory obligations, and customer considerations. We harmonize standards and regulations to support compliance requirements. Solutions are developed based on the harmonized standards, regulations, and customer requirements. A wide array of technical and physical processes, infrastructure, and software protect resiliency, transactions, and data. Our hosting environment is a virtualized environment comprising the following high-level safeguards:

- Virtual, logical, and physical isolation
- Data class isolation
- Encryption of data at rest and data in transit
- Active monitoring of software vulnerabilities
- Strong authentication controls at both an application and service level

SEC05 The Contractor's solution shall streamline electronic transactions by incorporating electronic and digital signatures compliant with HIPAA and other State and federal statutes.

[redacted]

[redacted]

SEC06 The Contractor's solution shall provide tools (e.g., alerts or reports), which identifies usage anomalies or users who may have misused the system.

[redacted]

SEC07 The Contractor's solution shall automatically maintain an audit trail of users, including database administrators, who pass through or view a record, regardless of whether data is changed.

[redacted]

SEC08 The Contractor's solution shall have security audit trail reporting capabilities (e.g. security, level, locale, IP address, user ID, before and after changes).

[redacted]

[redacted]

SEC09 The Contractor's solution shall ensure the audit trail that cannot be modified.

Our solution has controls in place, which prevent logged security events and audit trails from being edited or altered when captured. Auditing is enabled in every tool and interface throughout the solution. These audit logs are saved to a central log repository and retained for regulatory purposes and additional review.

SEC10 The Contractor's solution shall contain information determined by the Department and must meet Health Information Technology for Economic and Clinical Health Act (HITECH) audit standards.

Optum maintains a strong security posture to safeguard your data. At a minimum, we will maintain audit logs as addressed by the HIPAA/HITECH auditing standards and security framework or greater. Our solution follows the relevant security policies and processes regarding audit controls to reduce the risk of outside compromise, as addressed by the following:

- Section 164.308(a)(5)(ii)(C): Log-in monitoring
- Section 164.312(b): Audit controls
- Section 164.308(a)(1)(ii)(D): Information system activity review

Logs are collected in the normal course of activity within every solution component.

SEC11 The Contractor shall perform risk assessments per the Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach NIST SP 800-53 Rev 4. Risk assessments shall be completed on an annual basis and when additions or changes to functionality impact the security framework, architecture or when a new vulnerability exists.

Our experience supporting government clients provides us with a strong foundation and deep understanding in applying the CMS ARS and NIST 800-53 frameworks to our solutions. We use balanced risk management and threat analysis strategies to drive our information security program, and we design our privacy and security protocols to support compliance with various federal and state privacy and security regulations, including HIPAA, IRS 1075, CMS MARS-E, CMS ARS, and NIST 800-53.

We perform annual self-assessments and risk assessments on our information systems and when there are significant changes to functionality that may impact the security framework or architecture. We update policies and procedures annually or sooner based on changes in laws, regulations, guidance, or the threat landscape. We implement continuous monitoring practices and model changes to the information system security posture on the security controls recommended and/or mandated by CMS, IRS, and NIST 800-53.

SEC12 The Contractor's solution shall manage role-based permissions and provide a National Institute of Standards and Technology (NIST) compliant identification, authentication and accounting solution.

We provide full support for NIST-compliant identification, authentication, and accounting of users and roles, including RBAC from a centralized point. All system users will have a user name and password. No guest access will be allowed. All default accounts will be disabled or renamed. The solution will maintain a limited group of administrators with full access and limit the distribution of certain administrative responsibilities and rights, such as the ability to reset

user passwords or install software, to authorized groups and organizational units. Additionally, administrator accounts will be separate and distinct from general user accounts.

Users fall into one or more roles, where each role corresponds to a discrete set of job functions. With the Provider Services module, a system with significant and complex protected information, each role's set of job functions must be restricted to the systems and data required for business needs.

The Optum Provider Services solution uses role membership to control what applications users can access, the data they can see, and what actions they can take on that data.

A user will authenticate to the module using a single sign-on (SSO). Our solution will query a Lightweight Directory Access Protocol (LDAP)-enabled central SSO for user authorization based on the credentials presented on the user device. After granting authorization and establishing an access level, the system will allow user access at the predetermined role level.

All components will use an SSO/RBAC mechanism so that all personnel are governed by the same set of security policies. Using this approach, we implement security driven by your requirements and follow a consistent approach to user-based security controls. Similarly, the change management process provides a defined, consistent mechanism for configuration changes to access- levels, rules, or policies.

The ETL components support RBAC as well using the same SSO and role mechanisms as the user-facing components. If ETL-specific roles are required, these can be defined during the requirements phase.

We will work with you during the requirements phase to define:

- Roles
- Permissions, access grants, and resource quotas for each of the roles
- A matrix matching job titles to security roles and the creation of permission definitions for each
- Policies and procedures for providing for exceptions to the above, including such special restrictions as time and workstation limitations

We will document and maintain all of the security-related requirements, policies, standards, procedures, and supporting information in the Security Plan for the Provider Services module. The plan will reinforce the principles described above relating to the role of our SDLC in defining the security requirements and our security model's layered defense strategy to protect your most valuable assets and their usage.

SEC13 The Contractor's solution shall have multiple layers of external and internal security that provide administrative, physical, and technical mechanisms to protect sensitive or confidential information used in performing the responsibilities and duties defined for the module scope of work.

[redacted]

SEC14 The Contractor's solution shall not include any code of unknown origin.

No code of unknown origin exists within our solution, which comprises COTS software components. The COTS products are not customized. Any product or code added to the solution is validated against the vendor-supplied integrity hash to assure validity.

SEC15 The Contractor shall provide an independent third party to perform penetration testing within six (6) months prior to implementation. Penetration testing must also be performed by an independent third party on an annual basis and when additions or changes to functionality impact the security framework, architecture or when a new vulnerability exists. Penetration Test Report results shall be supplied to the Department and any major or critical vulnerabilities mitigated.

An independent third party performs penetration tests annually. Additional ad hoc penetration tests can be performed by request. Summary reports are available 30 days after receiving the request. An ad hoc test will occur within six months before implementing the solution. We will provide the results of the test to DPHHS. We will also mitigate any critical vulnerability identified during the test.

SEC16 The Contractor shall provide the primary and disaster recovery facility(s) which will ensure security, performance and disaster recovery requirements outlined in the module scope of work.

Optum will provide a Tier III-compliant data center for disaster recovery. This data center maintains the same security levels and performance standards as our primary data center. Disaster recovery requirements will be met as outlined in the scope of work.

SEC17 The Contractor shall maintain policies and procedures for security clearance and staffing controls for allowing access to confidential information and/or to restricted areas within the Contractor's solution.

[redacted]

[redacted]

SEC18 The Contractor shall maintain adequate technical support/staffing to provide 24x7x365 coverage.

We have technical support and staffing to monitor our applications 24 hours a day, seven days a week, 365 days a year. Our Security Operations Center delivers a coordinated operational approach through high quality prevention, detection, and remediation activities. All enterprise information systems (websites, applications, databases, data centers and servers, networks, desktops, and other endpoints) are monitored, assessed, and defended. The Security Operations Center provides the following services:

- Reactive security
  - Post-incident review, containment, eradication, and remediation
  - Security Incident and Event Management (SIEM) Logging Review
- Proactive security

- Platform KPI baselines
- 24-hour monitoring, 365 days a year

- Predictive security
  - Anticipating future threat vectors
  - Intelligence gathering and sharing with application teams

SEC19 The Contractor's data encryption solution shall meet Federal Information Processing Standard (FIPS) 140-2 and at a minimum use AES 128 encryption.

[redacted]

SEC20 The Contractor shall ensure that all data, regardless of its location, is encrypted at rest.

All data within the solution, regardless of its location, will be encrypted at rest. We will implement encryption as addressed by data classification through compliance, regulatory, and governance guidelines within our solution. Properly classified data is protected by deploying prevailing encryption techniques, such as FIPS 140-2 validated technologies for data in transit and at rest. Minimum mechanisms deployed include the following:

- We encrypt all data during transmission between the Web browser and the Web server using Transport Layer Security (TLS). This includes all individually identifiable health information, financial information, and messages sent using the Secure Messaging option.
- We use standard encryption algorithms, such as the AES or RSA SecurID and message encryption key size and length, such as GCM. Key lengths vary by encryption cipher types, symmetric and asymmetric. Symmetric encryption algorithms use a minimum key length of 256 bits, while asymmetric algorithms use a minimum key length of 2,048 bits.
- We also encrypt backup tapes, disk arrays, laptop disk, and removable media.

SEC21 The Contractor's transmission security shall use TLS 1.2, SHA 2 with a minimum of a 2048 bit key.

All data is encrypted during transmission between the Web browser and the Web server using TLS. Proper ciphers will be enabled to comply with this requirement. Symmetric encryption algorithms use a minimum key length of 256 bits while asymmetric algorithms use a minimum key length of 2048 bits.

SEC22 The Contractor will provide a completed Security Audit Report with results to the Department by the 30th (thirtieth) of September each year. The Security Audit Report must include either an electronic data processing (EDP) systems audit using SSAE 16 at a minimum level service organization control (SOC) 2 Type II or a NIST 800-53 rev 4 assessment at a "moderate" system risk control level. The Contractor shall provide a mitigation plan for all reported deficiencies. Major and critical deficiencies must be corrected within forty (40) calendar days of the report submission to the Department.

Optum agrees to provide an annual Security Audit Report to the State according to the timelines defined in the RFP. We take an aggressive approach to continuous monitoring, based on risk tolerance, which maintains clear visibility into assets and awareness of vulnerabilities. We hold our subcontractors to the same rigorous standards. Our solution follows the continuous monitoring practices outlined in CMS ARS, which is based on a NIST 800-53 moderate baseline. Our FedRAMP-certified vendor conducts continuous monitoring to maintain

compliance with FedRAMP. This process includes ongoing technical vulnerability detection and remediation, remediation of open compliance-related findings. It also includes an independent assessment (at least annually) of a selection of security controls by a third-party assessment organization.

SEC23 The Contractor's solution shall provide security features that support increasing the complexity of the authentication and authorization as the sensitivity of the data or functionality increases.

Our solution includes the following standard security features that support increasing complexity and sensitivity of authentication and data:

- Unique user names for each system user
- Authentication with complexity and expiry credential requirements
- Identity proofing
- Strong password (minimum of eight characters, one upper case, one lower case, one numeric, and one special character)
- Password reset using three challenge response protocols
- Account lockout after three failed attempts
- Minimum two-factor authentication enforced
- Enforced session inactivity of all logins, logoffs, and unsuccessful attempts
- Password encryption requires the use of variable key length with a minimum of 256 bits

SEC24 All Contractor's module components shall adhere to any applicable the Department system

We will adhere to any applicable DPHHS security practices, configurations, and procedures. We will adhere to the Security and Privacy Controls Requirements, the State of Montana Information Technology Strategic Plan, the Enterprise Architecture and Software Standards, the IT Policies, MCA Code 2-17-534, and MCA Code 2-17-114, as noted in the RFP.

Optum manages and supports a robust Information Security Program. Our protocols are based on industry practices, all applicable regulatory obligations, and customer considerations. Policies and standards are used to manage the specific requirements and basic premise of general computing, audit, and security controls.

The Information Security Policies and Standards represent the foundation of security applied to and within the Optum proprietary network infrastructure and critical application services. We review these controls annually. End-to-end penetration testing is optional and can occur after each major code revision to make certain vulnerabilities are not introduced into the solution. Monthly vulnerability and security scans are performed to maintain our security baseline.

Our solution leverages a wide array of processes, infrastructure, and software to verify and confirm the security of the environment, transactions and data. The solution leverages a virtualized environment where:

- Customer data is physically and logically isolated from other services.
- Isolation of different data classes is controlled through tightly managed firewalls between tiers.
- Data in motion and at rest is encrypted.

- Transaction integrity is managed through secure service protocols as well as secure service gateways.
- Software vulnerabilities are actively monitored through Web application firewalls.
- Strong authentication controls are employed at both an application and service level.
- Strong infrastructure policies and procedures are regularly scanned and updated to protect against newly identified threats.

SEC25 The Contractor's solution shall provide the ability to grant authorization through role-based security (create, delete, modify and view) access to user interfaces, reports, data elements/field level, and menu items.

We provide full support for RBAC. Users fall into one or more roles, where each role corresponds to a discrete set of job functions. For a system with significant and complex protected information, each role's set of job functions must be restricted to the systems and data they require based on business needs. Our solution uses role membership to control the user interfaces, reports, and menu items a user can access, the data a user can see, and the actions a user can perform on that data.

SEC26 The Contractor's solution shall allow access and role changes to be made in real-time with appropriate authorizations.

Our solution supports real-time updates to any security access or change. Anyone with the proper authorizations can perform security updates to access levels or roles. Our solution also supports the DPHHS security requirements for SSO access for users, developers, and administrators. All components in our solution are interoperable with an authoritative source supporting LDAP.

A user can authenticate using SSO wherever applicable. Our solution will query an LDAP-enabled central SSO for user authorization based on the credentials presented on the user device. Upon granting authorization and establishing an access level, our solution will allow user access at the predetermined role level. Likewise, when authorizations are changed or revoked, new assertions will provide an update to access levels.

SEC27 The Contractor's solution, in order to protect the database from SQL injection attacks, shall access the database from the application through a standard database abstraction layer.

[redacted]

SEC28 The Contractor's solution shall be easy-to-use and provide a user interface that allows authorized users to edit, create, and implement role-based and group-based security at the data element/field level for authorized users based upon individual characteristics or functional security groups.

The portal will be your SSO access point to tools, reports, and dashboards—all within a common framework. The portal will provide an intuitive and seamless user experience, built around ease-of-use and simple-to-navigate features. Authorized users will be able to edit, create, and implement security for data elements and authorized users and groups.

SEC30 The Contractor must limit access to its off-site facilities; including storage facilities. The Department has the right to perform physical security audits of the Contractor's off-site and on-site facilities at the Department's discretion.

[redacted]

SEC31 The Contractor shall establish security and privacy standards and standard operating procedures. These standards include HIPAA, Federal Information Security Management Act (FISMA), Privacy Act, Federal Tax Information (FTI), and other Federal and State laws, regulations, and policies. The Contractor shall also establish business and technical protocols to ensure that the transmission and storage of information remains secure.

We understand our responsibility to protect sensitive and proprietary information of the State and the State's constituents and clients, while maintaining the confidentiality, availability, and integrity of our information systems and associated data. We manage and support a comprehensive information security program through the consistent implementation of a mature, layered approach to data protection and security. This dedication to data protection and security is integral to the relationships we have with our customers and vendors.

We design our privacy and security programs and standards to support compliance with various federal and state privacy and security regulations. These include HIPAA, FISMA, FIPS, NIST 800-53, CMS MARS-E, CMS ARS, and IRS 1075. Our resulting policies and procedures are

reviewed and updated annually or sooner, based on changes in laws, regulations, guidance, or threat landscape.

We employ industry best practices and implement FIPS 140-2 validated encryption algorithms, such as the AES and RSA security to support data encryption in transit and at rest.

SEC38 The Contractor's solution shall employ malicious code protection mechanisms at IT systems entry and exit points, at workstations, servers, and mobile computing devices on the network to detect and eradicate malicious code.

We follow strict security measures to minimize risk. Optum will protect the entry and exit points, including workstations, servers and mobile computing devices (where applicable), on our networks from malicious code. We include safeguards to confirm that all activity is logged and tracked, including code execution. We employ both signature and heuristic monitoring to capture and mitigate malicious code execution.

Rules created in our security products will allow the system to automatically block actions or behaviors based on the defined conditions when anomalies are detected. Rules can be configured to monitor or block a large number of conditions including certain types of traffic such as a SQL injection, traffic from a certain IP address or user, or traffic or queries following a certain pattern. Rules can also trigger event sequences such as alerts to administrators or other identified staff.

We will recommend initial rulesets for implementation. These will monitor for anomaly detection including threats on the OWASP Top 10 list, irregular query patterns, database administrator activity, escalation of privileges, and other common threats. We will work with you to refine and tune these rules to minimize false positives and create trace logs that provide actionable information.

New threats and vulnerabilities continue to emerge. As the threat horizon changes, our staff will continue to monitor the threat level to our solution and will recommend new rules for configuration and implementation to protect your data assets.

SEC39 The Contractor's solution shall use foundational technical standards such as X.509 Certificate format and Public Key Cryptography Standard (PKCS).

Optum uses X.509 certificate format for all encryption and authentication mechanisms.

SEC41 The Contractor shall collaborate with the Systems Integration Services Contractor to integrate the Contractor's solution into the State's integration platform for single sign-on and federated identity management.

We will work with the Systems Integration Services Contractor to integrate the solution into the State's integration platform. Optum supports both Identity Providers (IdP) and Service Providers (SP) capability. SSO is enabled based on Level of Assurance and level of data access necessary to support the data classification. Access to information systems and information is managed using prevailing identity and access management technologies. SSO eases the burden of accessing applications across domain boundaries by federating identities.

To maintain secure, appropriate, and timely access, Optum will leverage the State's current Identity and Access Management (IAM) solution.

SEC42 The Contractor shall have an overall data security process that supports data security auditing.

Our data security policies include comprehensive auditing capabilities. Auditable events baselines are determined by regulatory requirements, such as HIPAA, or by oversight organizations, such as CMS and IRS. CMS and IRS requirements are standards based on the NIST 800-53. Auditable events in the solution include the following:

- Password changes
- Failed logons
- Failed access related to information systems
- Administrative privilege usage
- Account creation
- Account modification
- Third-party credential usage
- System shut down and reboots
- System errors
- Logging on perimeter
- Devices, including firewalls and routers
- Log packet screening denials originating from untrusted networks
- Packet screening denials originating from trusted networks, proxy use denials, user account management
- Modification of packet filters
- Modification of proxy services

We will work with the State if there are any additional events that we need to log and/or correlate. The audit logs will be protected from alteration and retained for at least 90 days.

SEC44 The Contractor must be compliant with the security processes outlined in the "Security and Privacy Controls Requirements" document that has been included in the Procurement Library.

Optum has reviewed, and will comply, with the security processes outlined in the Security and Privacy Controls Requirements document in the Procurement Library. We understand our responsibility to protect sensitive and proprietary information, while maintaining the confidentiality, availability, and integrity of our information systems and associated data. Optum takes a methodical, measurable approach to determine the applicable IT security and privacy control requirements for DPHHS. We achieve this by applying controls based on a tiered-methodology applied in the following manner:

1. We consider federal regulations and laws.
2. We review DPHHS's mandates and the State's IT security policies and procedures.
3. We consider our own policies and procedures.
4. We consider contractual agreements with the State.

Whichever law, regulation, standard, policy, or contractual agreement is most stringent will take precedence in our implementation. This is a harmonized approach to risk management and IT security and privacy compliance. It provides a strong security posture that is easily understood.

SEC45 The Contractor shall monitor system activity and prevent and detect intrusion, hacking, unusual activity, or system compromise. The Contractor shall immediately report any incidents of such, regardless of the outcome to the state, activate a Department approved communication strategy, perform mitigation activities, and provide continuous status updates to the Department until the issues are resolved to the Department's satisfaction. Only authorized contractor personnel may override system security alerts and edits.

We develop proactive security controls to prevent intrusion, hacking, unusual activity, or system compromise. After implementing, we monitor our controls to assure the design is working as intended. Only authorized personnel may override or edit any system security alert.

Optum uses the most current anti-viral software to prevent network intrusions that could potentially lead to disaster events.

All network connections, whether outbound or inbound, are filtered through a corporate approved firewall; layers of firewalls are isolated from internal network connections. The firewall is configured to protect against unauthorized intrusions and limit external access to the internal company networks. Proxy technology, content filtering, traffic inspection, advanced persistent threat, malware detection and prevention, DLP, and other security technologies are part of a layered security infrastructure deployed on the network. All components are part of our Security Operations Center monitoring and incident response program.

We provide routine IDS testing and IPS for the solution. Intrusion detection system/intrusion prevention system functions are layered with firewalls and other devices to monitor the network and selected infrastructure at the boundary ingress and egress points and boundary borders to collect essential information and to track specific types of transactions of interest to you.

We monitor events on the information system and detect information system attacks. Our monitoring and incident response teams are available 24 hours a day, seven days a week to address any potential security threats.

Our responsibilities include incident detection, forensic investigation, incident notification, and prevention. Our team assists with vulnerability scans and remediation of threats and reviews new application deployments to minimize introduction of new threats into production environments. Security incident response capability includes:

- Coordinating incident detection, analysis, containment, mitigation, recovery, and final reporting efforts to resolve security and privacy incidents in a timely fashion upon incident identification
- Participating in activities and decisions between cross-functional workgroups to develop security/privacy incident response requirements, conduct gap analysis, recommend compliance action plans, perform reporting, track trends in security and privacy incidents, and provide process improvement recommendations
- Security information event monitoring, integrated with security analytical services, to detect attacks across Optum services
- Coordinating notification to required entities as an outcome of an incident related to security and privacy
- Responsibility for notifying customers and members if confirmed breaches of confidential information, according to applicable laws, regulation and contractual stipulations occur

Our SIEM solution aggregates logs to a centralized location. Security events are monitored based on agreed service levels.

Our monitoring and incident response programs will provide reporting for security audits and compliance activities. Tracking data will be made available in the form of summary dashboards or detailed reports as scheduled activities or created on demand.

Optum will work with the State to define and approve the incident and problem management process flows. Our specialized focus on high severity incidents are based on prescribed SLAs and excellent communication. We will work with the State for content of the escalation notification artifacts making sure to capture all relevant information, using an accurate list of required recipients who require notification.

SEC46 The Contractor shall provide and operate solutions that terminate access immediately and/or generate alerts for conditions that violate security rules, unauthorized attempts to access data and system functions, and system activity based on security parameters.

We will terminate access immediately for any condition that violates security rules including unauthorized or improper system use. Additionally these actions will generate alerts for further review. Alerts can be sent by email or will be available for review in our SIEM dashboards. We operate in material compliance with relevant State and federal security laws and regulations related to the services we provide. We continually track and analyze new and existing privacy legislation, at the State and federal levels, and update existing security processes as appropriate to support compliance.

Optum follows strict security measures to make certain that the risk of breaches is minimal. We include safeguards to confirm that all activity is logged and tracked. Our solution and data hosting meets CMS compliance as guided by HIPAA, NIST 800-53, CMS MARS-E, and CMS ARS for maintaining audit trails within the infrastructure and the application. Auditable events in the solution include password changes, failed logons, failed access related to information systems, administrative privilege usage, PIV credential usage, account creation, account modification, and third-party credential usage.

We provide routine intrusion detection testing and prevention for the solution. Intrusion detection system/intrusion prevention system functions are layered with firewalls and other devices to monitor the network and selected infrastructure at the boundary ingress and egress points and boundary borders. It collects essential information and tracks specific types of transactions of interest to you.

We monitor events on the information system and detect information system attacks. Our monitoring and incident response teams are available 24 hours a day, seven days a week to address any potential security threats.

We will work with you define realistic security rules to minimize risk of unanticipated security events.

SEC47 The Contractor's solution shall ensure that only authorized users have access to systems and data, by requiring the following:

- Unique authentication credentials identifiable to each user of the system, not allowing for the re-use of credentials;
- Authenticates the receiving entity prior to a system initiated session, such as transmitting responses to case inquiries;
- Maintenance of key user information as part of a user profile including user ID, name, employer/state agency,
- Identity verification information, and an indicator of employee versus contractor;

- Multi-factor user authentication and the ability to restrict or permit a user's access to system functions, features, and processes based on the user's assigned roles based on business need and user security profile and a unique user ID and password and including a read-only access level;
- Column and row-level security access, data classification schemes, and/or the designation of data at multiple levels (e.g., case, individual) as restricted or sensitive (e.g., substance abuse treatment data) with the ability to define and implement exclusion controls on a per-user or user-group basis within a multi-level organizational structure, (e.g., external agencies and Appeals units).
- A method for authentication of all internal and external users and systems and the ability to deny access to all invalid users and systems;
- Encrypted passwords in storage and in transmission;
- The capability to automatically suspend users who have not accessed the systems within a time period specified by the Department;
- The termination of authorized sessions after a time period of no activity specified by the Department, with a warning message displayed prior to the session timeout;
- Enforce a sufficient level of authentication and identification against fraudulent transmission, imitative communications, and deceptive communications by validating the transmission, message, station or individual; and
- A method for designated security administrators to set and modify user security access profiles.

[redacted]

[redacted]

SEC48 The Contractor shall provide to the Department, upon request, a listing of all users having access to the Contractor's module components and/or data with details regarding the access granted to each user.

We will generate a report listing all user access upon request. The report will contain the tools to which the user has access, the level of access granted, the last time the access was used, and

the date the access was granted. These reports can be run on demand or scheduled regularly for audit purposes. We will work with you at least yearly to complete an entitlement review to verify system access levels are as required and expected.

SEC49 The Contractor shall provide and operate solutions for security incident reporting and mitigation mechanisms. The Contractor shall preserve and report specified audit data when security violations are detected and mitigated.

We use many different tools to detect potential malicious behavior, unauthorized access, and the presence of malware. Types of tools we employ throughout the network and application stack are SIEM, file integrity, database, and antivirus tools. Our tool selection enables us to configure triggers for specific security and privacy events. After these triggers are activated, a configurable action then occurs, such as automated notifications, application/database shutdowns, or account locking. Upon notification, our security team takes further action to research and analyze the warning suggested by the trigger.

We implement these tools and design triggers to meet industry best practices, as well as laws, regulations, and client-specific requirements. These triggers include the following:

- Application/system shutdowns and restarts
- System reboots
- Multiple unsuccessful logon attempts
- Change of file permissions or privileges
- Password changes for service accounts
- Creation or modification of privileged user groups
- Changes to database or records outside of the application interface
- Starting or stopping of audit functions
- Use of batch files to copy or make changes to applications or databases
- Changes in security rules

Additionally, our best practice recommendations incorporate key planning procedural steps, such as those suggested above relating to incident response. These include:

- Verify the Privacy and Security Plan is complete and functional
- Validate controls are in place before invoking contingency plans
- Layer the network and infrastructure architecture using purposeful VLANs and access control lists (ACLs)
- Verify access logging capabilities remain uninterrupted
- Verify there is monitoring 24 hours a day, seven days a week, with alerting in place and up-to-date communications procedures
- Invoke contingency plans, when necessary, with bare minimum access levels to make certain controls are in place and working

We will preserve and report specified audit data to DPHHS or their designee when security violations are detected and mitigated within the CMS ARS and HIPAA mandated time frames.

SEC50 The Contractor shall comply with NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices where required by CMS to protect confidential information stored on end user devices.

[redacted]

SEC51 The Contractor shall comply with NIST Federal Information Processing Standards (FIPS) Publication 180-4: Secure Hash Standards as required by CMS for use of secure hash algorithms.

[redacted]

SEC52 The Contractor shall comply with NIST Federal Information Processing Standards (FIPS) Publication 186-4: Digital Signature Standard as required by CMS for use of secure algorithms in digital signatures.

Optum will comply with this requirement. We will encrypt all data in motion and at rest using electronic and digital signatures per HIPAA and state law. Examples include:

- Digital Signature Standard (DSS)
- Rivest, Shamir, and Adelman (RSA)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

SEC53 The Contractor shall comply with the Harmonized Security and Privacy Framework - Exchange Reference Architecture Supplement Version 1.0 and as required by CMS.

We will comply with the appropriate security requirements for data analytics as outlined in the CMS MARS-E Volume 1: Harmonized Security and Privacy Framework - Exchange Reference Architecture Supplement. Our solution implements industry-standard security best practices and complies with applicable federal and State laws and policies. Frameworks include HIPAA, IRS 1075, NIST 800-53, CMS MARS-E, and CMS ARS, among others.

SEC54 The Contractor shall comply with the OASIS Web Services Security - Simple Object Access Protocol (SOAP) Message Security Version 1.1 Specifications as required by CMS to build secure web services to implement message content integrity and confidentiality.

Our solution will use Extensible Markup Language (XML) Encryption standard for message-level encryption and decryption of XML data. We will use SOAP 1.1 protocol standard for data messages exchanged in Web services communication over the application layer protocol, such as HTTP, as we plan to implement the functionality using SOAP-based Web services. We will encrypt portions of the XML data messages, as required.

SEC55 The Contractor shall respond to all risks identified through the periodic security risk assessments with a CMS Information Security Program Plan of Action and Milestones (POA&M) containing clarifying information, a

proposed mitigation strategy if necessary, a timeline for implementation, and shall work with the Department to successfully execute the POA&Ms.

Optum will meet this requirement. Our balanced risk management strategies drive our information security program to help us maintain a strong security posture. Per CMS ARS, we perform annual self-assessments on our information systems based on our System Security Plan (SSP).

Our SSP defines the State's information system boundary. This system boundary includes a description of the State's information system, technologies, user roles with access privileges, architecture diagrams, system interconnections, and system categorization.

Each security control in the SSP will have an associated implementation statement describing how the safeguard has been met. Based on these implementation statements, test cases will be developed to assess, review, and evaluate the implementation status of each control. These test cases are developed and performed by an organizationally separate audit and compliance team and captured in a Security Test and Evaluation (ST&E) plan. We capture the results of the ST&E in a Security Assessment Report (SAR).

We document in a CMS Information Security Program Plan of Action and Milestones (POA&Ms) any findings that result in a control being partially implemented or not yet implemented. We track POA&Ms through remediation and mitigation processes. Optum will work with the State to successfully execute the POA&Ms in a timely manner.

SEC56 The Contractor shall ensure all contractor and subcontractor personnel providing services under this contract are familiar with and comply with the Business Associate Agreement and the privacy and security policies included in the RFP.

Optum will establish BAAs or contractual agreements with any subcontractors having access to data subject to protection by HIPAA and with the State. The content of the BAA will be consistent with the State's standard Business Associate Addendum.

SEC57 The Contractor shall provide logical segregation of the Contractor's solution, components, and network connections with other entities and prevent any unauthorized disclosure of the States' data.

[redacted]

SEC58 The Contractor's solution code shall never run from a system level account with unlimited privileges such as "root" or "administrator".

We will comply with this requirement. We will not run any code from a system-level account or any account with root or administrator privileges. All of our team members will have individual accounts to complete their required tasks. If a process requires elevated access for any reason, we will request creating a second account for that explicit purpose. Any account with elevated permissions and/or rights will only have the access levels required to complete the task for a specified time frame.

SEC59 The Contractor shall ensure the confidentiality, privacy, and security of all state data passing through the Contractor and subcontractor networks.

Optum manages and supports a comprehensive Information Security Program through industry best practice, a blend of applicable regulatory obligations, and customer considerations. We support compliance to HIPAA, NIST 800-53, FIPS, CMS ARS, CMS MARS-E, IRS 1075, and other prevailing control authorities. The outcome is assurance of data and technology confidentiality, integrity, and availability.

Our Information Risk Management team develops, maintains, and communicates a comprehensive information security program to protect the confidentiality, integrity, and availability of Optum information assets. This policy applies to all Optum employees, third parties, and subcontractors.

SEC60 The Contractor shall establish and implement emergency access procedures for the Department to obtain secure access to module data during an emergency. Emergency access procedures shall be subject to the Department's approval.

Optum will comply with this requirement. Emergency access procedures for DPHHS to obtain secure access to module data during an emergency will be documented within the Disaster Recovery and Business Continuity Plan for DPHHS.

SEC61 The Contractor's solution must protect data from improper alteration or destruction including authentication mechanisms and to corroborate that the data has not been altered or destroyed in an unauthorized manner.

As your data custodian we protect data from improper alteration and destruction. Security is integrated into our solution by design through our SDLC enabling identification and verification of regulatory requirements and controls required to meet compliance. Our security model is based on a layered defense strategy which complements SOA. The Optum Provider Services solution incorporates security controls across the environment to prevent unauthorized opportunistic access, abuse, disruption, modification, or destruction of data. The security settings applied in both native and third-party applications are designed based on applicable regulations and standards along with your specific organizational requirements. A combination of advanced data protection, auditing and logging, encryption, identity and access management, infrastructure security, security incident management, threat and vulnerability manage, and physical security solutions protects DPHHS assets.

Changes to environments containing live data must be submitted using a formal change control ticket and must include a back-out plan, in the unlikely event that such changes need to be removed. Auditing logs and records are protected from unauthorized changes, and access is limited to only those user accounts that require access to the logs.

SEC62 The Contractor's solution shall display a security warning banner prior to allowing entry into the system. The solution shall have security warning banners and headers and footers that adhere to Federal, state, and other applicable standards that are prominently displayed introductory screens.

Our solution will display a security warning banner prior to user accessing the system. The interface can also be configured with appropriate security banners in page headers, footers, and in the alerts section. We will work with you during DDI to determine the appropriate banner text to convey on the introductory pages, wherever applicable.

SEC63 The Contractor shall utilize cloud-based technology wherever advantageous to maximize the efficient and effective utilization of technology.

[redacted]

[redacted]

SEC64 The Contractor shall ensure user account access is reviewed on a quarterly basis at a minimum. User accounts should be appropriately disabled as roles and responsibilities change.

Optum will conduct a quarterly review of user accounts to validate accuracy of entitlements and access levels. We will provide results of the review to DPHHS for final authority of change prior to any role or responsibility reassignment or revocation.

SEC66 The Contractor's solution shall meet the minimum password requirements below:

1. Must not contain the user's account name or parts of the user's full name that exceed two consecutive characters
2. Minimum password length: 8 characters
3. Contain characters from 3 of the following 4 categories
   a. English uppercase characters (A through Z)
   b. English lowercase characters (a through z)
   c. Base 10 digits (0 through 9)
   d. Non-alphabetic characters (for example, !, $, #, %) (these will not work when logging into ReRite from Toshiba printers ... not on the key pad)
4. History: Cannot reuse a password for 24 password changes, user cannot reset password again for 24 hours
5. Expiration time frame: 60 day
6. Lockouts for failed attempts – account locks after 3 failed attempts, will unlock after 15 minutes

[redacted]

SEC67 The Contractor's solution shall track disclosures of ePHI; provide authorized users access to and reports on the disclosures.

We will track disclosures of electronic Protected Health Information (ePHI). Authorized users will have access to disclosure reports as required. We will work with you to identify the communications channel for disclosure processes. As a health care services organization, Optum has privacy and security programs designed to support compliance with various federal and state privacy regulations. These include HIPAA, CMS MARS-E, CMS ARS, and state privacy requirements.

During implementation, we use encryption as required for accessing each environment and for testing solution functionality in the development, test and deployment environments. We have a proven record of developing solutions that employ data masking and encryption to store, transmit and process ePHI. In addition, we integrate our SDLC with compliance and security components throughout each phase of the implementation and corresponding environment.

SEC68 The Contractor shall support the State in developing a Privacy Impact Analysis for each module or module component that includes the following information:

- Use of personally identifiable information (PII) or personal health information (PHI) and a description of the types of data that will be collected
- Sources of PII/PHI, populations, and transfer and disclosure mechanisms
- Legal environment (legal authorities and state privacy laws)
- Details about the entities with which the collected information will be shared
- Privacy and security standards for its business partners and other third parties and the agreements that bind these entities
- Incident handling procedures
- Privacy and/or security awareness programs and materials for its workforce

Optum will assist you in developing a Privacy Impact Analysis. We will work with you to capture the following information:

- What information to collect, such as name, phone numbers, addresses, social security numbers, and medical data
- Data will classify and categorize as PHI or PII based on the information contained within the data and the intended use of the data
- Documenting that users with access to PHI or PII have a bona fide need to know and access to the data is restricted to the least possible level based on required job duties
- Documenting who the data will be shared with and how that transfer will occur
- Documenting where PHI and PII data originates and how that data is transferred to the system: PHI and PII will be used in accordance with HIPAA, CMS ARS, and NIST guidance
- Documenting details about the entities with which the collected information may be shared, including:
  - Who performed the extract?
  - When extract was done?
  - What was the extract?

  - Where was the extract taken from?
- Has the extract been deleted? If not deleted after 90 days, monitoring that it is still needed in 90-day intervals; documenting the privacy and security standards for our business partners and other third parties
- Incident handling procedures will be documented, including what will be done in the event of a breach, who will be notified, the required timeline for such disclosures, the auditing data collected, and the impact of any such incident to clients and customers
- Privacy and/or security awareness programs and materials for the workforce will include employees receiving annual training on and signing an Acceptable Use policy and Rules of Behavior for PHI and PII data

SEC70 The Contractor shall provide the ability to de-identify and/or redact data for entities not authorized to receive PII or PHI and utilize de-identification algorithms to allow for re-identification of data if required.

The flexible architecture of our solution enables us to implement a tailored approach to satisfy your de-identification requirements. Our SMEs will work with you to locate relevant data and de-identify or redact it as necessary. Data can be de-identified through several mechanisms, including stripping data elements, obfuscation, and masking. We will work with you to enforce an agreed-upon process for data de-identification and redaction. De-identified data can be re-identified, if required.

SEC71 The Contractor shall provide a process for masking, sanitizing, scrambling, or de-sensitizing sensitive data (e.g., PII/PHI) when extracting data from the production environment for use in non-production environments.

Our data transformation and extract tools support processes to extract data from the production servers, de-identify that data, and load it to non-production environments. Data can be de-identified through several mechanisms, including stripping data elements, obfuscation, and masking. Our database replication tools enable full synchronization of data from production to disaster recovery.

SEC72 The Contractor shall review and identify monthly, any unneeded hardware, software, and licenses, present recommendations to the State for review and ensure that any unneeded hardware, software, and licenses have been decommissioned upon approval from the State.

We will review hardware, software, and licensing needs monthly. A summary report, including any recommendations for decommission of resources, will be presented to DPHHS monthly.

SEC73 The Contractor will provide the completed reports with the results of the service organization control (SOC) 1 Type II audit annually on date identified by the State. The Contractor shall provide a mitigation plan for all areas of non-compliance. Issues found to be non-compliant shall be corrected within forty (40) calendar days of the report submission to the Department.

We will provide a completed SOC 1 Type II audit annually to the State as referenced in SEC22 and SEC73. Our hosting environment exceeds Statement on Standards for Attestation Engagements (SSAE) 16 by complying with SSAE 18 Type II certification standards. We will employ an external auditor to conduct an annual SSAE 18 Type II audit based on the security trust principle. Results and remediation plans, including plans of actions and milestones, will be available to DPHHS. Critical deficiencies will be corrected within the period agreed upon with the Department.

3.10.1.3 Hosting and Environments

This section addresses hosting and environment requirements. The Department prefers cloud based hosting for the proposed solution. The Department expects the delivery of the solution/services to be seamless with the hosting solution providing the flexibility to integrate other solutions for security and regulatory purposes in the future, and be

cost-effective and scalable. Also, the Contractor is expected to provide a hosting environment for all solution components that has a Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance, or has a documented NIST 800-53 rev 4 at a "moderate" system risk assessment designation. In addition, the Contractor is required to demonstrate that their hosting solution is Statement on Standards for Attestation Engagements (SSAE) 16) SOC 1 Type 2 and SOC 2 Type 2 compliant.

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

Optum will bring unique knowledge and experience to the implementation of the DPHHS Provider Services module. Our innovative capabilities in hosting are optimized for HHS enterprises. We will provide an efficient, highly secure hosting solution. Our solution provides the highest degree of performance with the lowest level of risk.

The State's Provider Services module is planned for hosting inside our FISMA environment. We built our solution to support collaboration with multiple vendors, and we will work with you and your contractors to integrate with the MPATH Integration Platform to verify full connectivity. All connections use secure and trusted networks.

Our CRM is hosted in a FedRAMP-certified government cloud infrastructure and will meet your SLAs. All back-end cloud connections will be transparent to DPHHS users and customers. Any components not hosted within the Optum FISMA environment or in a FedRAMP-certified government cloud infrastructure will be audited per requirements.

Our capability to manage data hosting is demonstrated in the resources and facilities we have created. We manage our own Tier III data hosting centers. Our primary data center operations organization has received a Gold Certification for Operational Sustainability by the Uptime Institute. Gold Certification demonstrates exceptional management, operations, and building characteristic behaviors, and low site location risks. Our on-staff Accredited Tier Designers have subsequently carried forward those certification compliance requirements for quality, reliability, redundancy, and strength into our secondary data center.

Our data centers are TIA 942-compliant, host 61,000 servers, and provide more than 63 petabytes of primary storage. They support more than 5,500 applications and maintain business processes for 844,000 contracted providers and 5,950 contracted health care facilities, performing more than 100 billion computing transactions annually. Our systems process more than two billon claims per year with more than 99 percent accuracy and hold over 131 million secured patient records. Our data centers are located in the continental United States.

Advantage

Our primary Data Center received its Tier Certification of Constructed Facility from the Uptime Institute as a Tier III rated facility.

Its operations organization has also received a Gold Certification for Operational Sustainability by the Uptime Institute.

We own and operate these data centers with a security-first mindset that follows security architecture guidelines to protect customer data. These guidelines include those issued by NIST, ISO 27018, and HIPAA.

Optum hosting uses high-quality industry standard components throughout our facilities. Our technical experts experiment in small-scale settings to continually evaluate the performance of new infrastructure components, tools, and techniques. The goal is to continuously take advantage of technological advances while maintaining proven reliability.

Servers: Optum uses data center quality servers, such as the DL380 G9, designed to support virtual and physical environments. These servers handle mission-critical applications, configured with up to 24 cores and 3Tb of memory.

Storage: Industry storage area network technology is designed for the performance requirements of SaaS processing. Hitachi Storage Area Network (SAN) provides enterprise-scale storage. We provision slices of storage in Logical Unit Numbers and present those to the virtual infrastructure for consumption. Our operations management tools promote the efficient and protected management of storage resources.

Encryption: All data is encrypted both at rest and in motion using multiple technologies. All Optum SANs support encryption, along with optional key encryption management.

The following table shows typical Optum-hosted components.

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Our TIA 942-compliant data centers are highly scalable for future needs and fully maintainable with the capability for zero scheduled downtime. Redundancy is a key design principle in our hosting facilities. Figure 3.5 shows the underlying design of our network and Optum hosting services.

[redacted]

Our solution has been designed with full redundancy. Components in this architecture are located in our three geographically diverse data centers, where any site can fully support the production application and recover if a disaster with minimal intervention occurs. Features of our data center facilities include:

- Tier III Gold Certified for Operational Sustainability
- 60,000+ square feet of raised floor space
- Full UPS and battery failover
- Nine megawatts of usable power
- 10–12 diesel generators installed in an N+2 configuration
- Independent raised floor isolating potential conditions in one area from other areas
- On-site fuel for 96 hours of run-time at full load, plus four-hour fuel delivery
- Multiple carrier rings for network connectivity
- Dedicated feeders from substations
- 12 computer room air-handing units, in N+2 configuration with dual power sources
- Six 1,550 ton chillers backed by a 500,000 gallon thermal storage tank

Optum maintains specific policies, which address physical security of critical processing facilities, hardware and work areas, and information systems. Critical areas, such as server, MDF, IDF, mechanical and electrical rooms, docks, labs and IT workrooms, are secured with proximity sensor card readers and monitored with cameras.

Data centers and critical facilities must be secure locations with controlled access and monitoring. Our security standards include the following:

- Entrances to data centers and critical facilities must be locked and access obtained using electronic card readers.
- Critical computing areas and critical infrastructure areas must not be obvious externally and must be located away from windows and workspaces.
- At least two security officers monitor the areas 24 hours a day, 365 days a year.
- Only approved individuals with a documented valid need to perform hands-on services are eligible for access to critical areas, with tiered levels of access that allow access only to specific areas required.
- Managers perform monthly entitlement reviews to determine if there is a legitimate business need for their employees or third-party service providers to continue physical access to the critical area.
- All non-employees must present government-issued photo identification to a security guard, and employees can present their company-issued photo identification.
- Third parties receive temporary access badges and must wear a visitor nametag.
- Data backups are encrypted using EMC appliances.

We can review and discuss additional details of the core clinical platform security posture upon contract execution.

In the following sections, we provide our responses to the RFP requirements applicable to Hosting and Environments as identified in Attachment F, Requirements Matrix.

ENV02 The Contractor shall provide hosting services that shall meet all state requirements.

Optum offers a complete solution that provides the highest degree of performance with the lowest level of risk. As a health care technology company, Optum has privacy and security programs that comply with various federal and state privacy and security regulations. These include HIPAA, CMS ARS, and state and local security and privacy requirements.

We have the experience required to meet HIPAA, MARS-E, IRS 1075, and NIST 800-53 compliance for hosted and developed solutions. CoBiT and FedRAMP's current security design is based on NIST's Cybersecurity Framework, which includes the NIST 800:53 standard. Optum is experienced with designing systems to meet NIST 800:53 requirements. Moderate controls from prevailing regulations and standards are used to baseline controls. Where state statutes are more stringent, they supersede Optum and regulatory requirements. Contractual agreements deemed more stringent supersede statutes. When organizational policy is more stringent, it will take final precedence.

ENV03 The Contractor's hosting solution shall provide the flexibility to integrate other solutions for security and regulatory purposes in the future and be cost-effective with burst capacity.

Our hosting solution will provide DPHHS with extensive flexibility to integrate other solutions for security and regulatory purposes in the future and be cost-effective with burst capacity.

The modular design of our solution incorporates best practices and lessons learned from our successful operation of commercial systems and Medicaid FFS systems. As an integrated, modular COTS-based solution with open systems architecture, our solution is scalable and extensible. When extensibility is required, we can add or remove service components to satisfy specific business requirements as they evolve over time.

As service volumes increase or decrease, our solution is scalable to meet processing demands. The Optum Provider Services solution also delivers extensive interoperable capabilities to share and exchange data with exchanges, public health departments, and other local, state, and federal HHS agencies.

The enterprise architecture of our solution is based on the MITA and Optum BA capability models. For our solution, we used COTS applications to the greatest extent possible. Our approach was to integrate the various applications using SOA components, built around SOA standards, to provide the loose coupling, and increased agility to change as the market changes. Our vendor-hosted, NIST-compliant approach is built on established infrastructure and security models to help us gain the performance and security needed to keep information safe.

The Optum Provider Services solution will enable DPHHS to scale horizontally and vertically, based on seasonal or projected demand. As an example, for one of our State Health Exchange customers, Optum provisions additional servers during open enrollment. After the open enrollment period, the servers are de-provisioned so the state customer pays only for the additional server infrastructure in use during open enrollment. Our solution will also enable us to provision and de-provision environments based on the DPHHS' business or project needs. For example, we can provision temporary testing environments during major development projects. Then, after testing is complete, we can de-provision these environments so you pay only for the environments when used.

ENV04 The Contractor's hosting environment for all module components shall be compliant with Statement on Standards for Attestation Engagements (SSAE 16) SOC 1 Type 2 and SOC 2 Type 2 and has Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance, or has a documented NIST 800-53 rev 4 at a "moderate" system risk assessment designation.

We take an aggressive approach to security assessment and audits based on risk tolerance that maintains clear visibility into assets and awareness of vulnerabilities, and we hold our subcontractors to the same rigorous standards. Our solution and associated hosting environments follow the continuous monitoring practices outlined in CMS ARS, based on a NIST 800-53 moderate baseline, as well as FedRAMP moderate.

The CRM for our solution is hosted through a FedRAMP-certified cloud services provider which conducts continuous monitoring to maintain compliance. This process includes ongoing technical vulnerability detection and remediation, remediation of open compliance related findings, and at least an annual independent assessment of a selection of security controls by a third-party assessment organization (3PAO).

We can provide the necessary SSAE 16 SOC reports created for this solution per this requirement.

ENV05 The Contractor's solution shall be available and accessible twenty-four (24) hours a day, seven (7) days a week, with the exception of planned downtime due to system upgrades or routine maintenance. All planned downtime and maintenance outages shall be coordinated and approved by the Department at least five (5) business days in advance.

We meet industry-leading SLAs because of our unique Enterprise Stability Program, mature processes, and innovative technology solutions. The solution will be available 99.5 percent of the time, 24 hours a day, seven days a week with the exception of planned downtime, according to SLA 32. Optum will work with you to plan maintenance windows at least five business days in advance, during a mutually agreeable time frame. We scheduled updates, releases, and maintenance windows at times with the lowest user activity, such as late evening or early hours on weekends.

ENV06 The Contractor shall provide the ability to run multiple sessions /environments/applications/areas/views simultaneously. This includes providing sufficient environments and configurations (e.g., multiple environments, multiple application layers, hub architecture) necessary to perform all required functions (e.g., testing, training, production operations, modeling, disaster recovery).

[redacted]

[redacted]

ENV07 The Contractor shall identify the physical location(s) where the Contractor's solution is installed and operating. The Department must have transparent access to this location(s).

Optum has three Tier III data centers located in Minnesota. We can provide specific locations that will house the DPHHS Provider Services module upon contract award.

Our data centers are located in areas that are not geographically prone to major disasters. The data centers are built with necessary environmental redundancies, including critical areas of the building having the capability to withstand more than 200 MPH winds. Our data centers require that the mechanical and electrical systems are concurrently maintainable, which allows any

component within these systems to be isolated and maintained on a planned basis with no impact to the critical IT load.

We offer a geographically dispersed cloud-based solution that optimizes costs, improves performance, and reduces risk using our facilities.

Customer access to data centers for audit or other purposes require a minimum of two weeks' notice for prescreening. Depending on the specific server room, this may require U.S. citizenship. The lead-time for vetting guests allows Optum to validate proper security to prevent unauthorized individuals from obtaining key information about our hosting facilities ultimately protecting your applications.

3.10.1.4 Integration

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

OIL supports the Optum Provider Services solution to provide the interoperability between the solution and the DPHHS environment. Built upon SOA principles, OIL promotes transforming and routing the transactions and messages within our solution.

Figure 3.7 shows how OIL supports our integration with the DPHHS environment.



OIL is one of the key functional elements of the Optum technology approach. It is built on SOA principles using a lightweight ESB and integration platform. Because of OIL's inherent flexibility, loose coupling, and SOA framework, it enables our solution to scale and provides easy integration of new services, vendors, and applications.

OIL acts as the service integration layer and can leverage and integrate with almost any existing solution, asset, or system. OIL supports multiple data file transfer protocols and data formats, including:

- Data file transfer protocols:
  - Legacy file transfer (FTP)
  - Secure file transfer (SFTP)
  - Message queuing (JMS, AMQP)
  - SOAP Web services
  - RESTful APIs
- Data formats supported:
  - JavaScript Object Notation (JSON)

- XML
- COBOL copybook
- ANSI X.12 Healthcare Standards
- HL7 Messages
- Proprietary formats

OIL has an HHS-specific design, including a canonical data model built on the X.12 and HL7 standards, and mirrors the data definition of the X.12 and HL7 transactions. For example, provider data is represented to reflect the information contained in the ANSI X.12 274x253 Provider Directory transaction standard. Adoption of industry standards for the canonical model data definitions eliminates the need to develop transaction-specific data dictionaries and transaction-specific data maps.

Data is transformed to the standards-based data model by a producer proxy service. Additional workflow and orchestration inside the service layer uses the canonical data model. At the consumer end of the integration, a service proxy is implemented to convert the data to any non-standard output format. Each service proxy exists between a modern or legacy enterprise system and a standard OIL service supporting an HHS-specific data format and transaction technology as referenced above. This approach supports modularity and interoperability, rather than a general-purpose ESB implementation. Thus, extensions to the platform just need to focus on proxy development, not core data formatting and changes.

In addition to the many types and data sets supported by OIL, it provides the following features:

- Service orchestration
- Federation
- Routing
- Protocol conversion
- Transaction queueing
- Transformation
- Syntax validation

Design flexibility: Through its library of core integration capabilities, canonical data model, and the use of proxy services, OIL leverages an integration library that enables rapid design, development, testing, and integration of new services. All modules and systems that attach to OIL only need to communicate with an OIL proxy adapter.

Scalability: The architecture is designed to scale both vertically (e.g., VM and JVM sizing and capacity) and horizontally (e.g., adding additional application servers with fail-over and load balancing). The architecture can also support multiple tenants, both discrete tenants within an enterprise and multiple enterprise tenants when governance requirements allow. Automated configuration and deployment tools help verify that we can add or remove middleware capacity, as needed, to support operational needs. Using operating system and application stack configuration automation verifies this as well. As enterprise modules are scaled or added, the OIL platform can scale to meet these needs.

Independent versioning: Using standard-based APIs and proxy adapters allows modules to be built using independent SDLCs and to be versioned as needed. The APIs can evolve and are versioned as needed to support the module and integration.

Independent development and testing: Versioned and standardized APIs, as well as proxy adapters in the OIL implementation, provide isolated system module development and testing, if required. Modules only need to implement the API, and corresponding testing can use a black box testing method from the API's perspective.

Distributed deployment: The adoption of sufficient infrastructure capacity, proper API construction, and choice of communication fabrics enables distributed module deployment. It also enables deploying the required middleware across data centers or cloud providers, as needed, to meet your platform needs and non-functional requirements. The scalability, configuration, and deployment automation of OIL promote this capability.

In the remainder of this section, we include our response to each of the Attachment F integration requirements.

INT02 The Contractor's solution shall support retrieval and presentation of data associated with geographic indicators such as by state, by county, by zip code, by peer group, or other geographical indicators specified by the Agency.

User access to our solution is through the Provider and State Medicaid Agency portals. Those portals allow the user to search for providers using various search parameters, including geographic and peer groups. We will work with DPHHS on further defining the most efficient and effective provider search parameters. Provider address and address geo-location information is also retained in our solution, which enables reporting based on geo-location.

Users can search, using the Provider or State Medicaid Agency portals, for providers within a user-defined radius of a specific address or geographic location. The combination of search parameters with geographic location data enhances search routines. For example, a user can search for providers of a specific specialty and primary language within a user-defined radius, returning a richer and more meaningful search results than simple geo-location packages can provide.

INT10 The Contractor shall develop operational procedures in coordination with other enterprise module vendors to restore system availability.

We will develop system availability recovery procedures in coordination with the State and any other enterprise vendors the State selects as a part of the overall MPATH solution. Our experience offering commercial and Medicaid systems in SaaS and BPaaS delivery models requires us to work collaboratively with our customers and their vendor partners. We develop smooth system availability and recovery operational procedures while conforming to the availability and recovery SLAs negotiated with our customers. We develop operational procedures to manage system recovery for both planned and unplanned system downtime.

INT15 The Contractor's solution shall use XML standard messaging format to ensure interoperability.

OIL enables interoperability and interconnectivity between disparate applications through its use of adapters that communicate with the core canonical HHS data model. The data model is based on an XML representation of the standard X.12 and HL7 transactions. The OIL adapters can then communicate with specific systems in the most efficient manner for that system. Where those systems communicate by queued message or API, XML is used as the payload format for transmitting data.

INT22 All service endpoints/APIs shall be exposed to the ESB and are able to receive and submit messages through the ESB.

OIL is designed to simplify application integration through a central core ESB and service adapters that are exposed to the ESB. OIL has implemented service adapters that communicate with the core canonical data model and then implementation-specific adapters communicate through the exposed service proxy adapters. The service adapters communicate across systems through the ESB to assure message delivery, orchestration, and error recovery.

INT35 The Contractor shall provide an architecture that has clearly defined service endpoints.

We designed OIL to use standard and clearly defined service endpoints. Optum uses standard and clearly defined endpoints to rapidly and seamlessly introduce new applications in response to new business requirements or to decommission applications no longer serving a business purpose, without disruption to the existing systems environment.

INT40 The Contractor shall provide technical, functional and performance documentation required by the IV&V Contractor for the solution in order to support IV&V reporting needs identified in the most current version of MECT.

Optum will work collaboratively with you to provide the technical, functional, and performance documentation as required by the IV&V contractor, Public Knowledge, LLC. We acknowledge that it is our responsibility to keep all of our documents current and available for review by the State, the IV&V Contractor, the SI, and CMS or its agents.

We will work with DPHHS to follow a coordinated approach that includes regular communication with your PMO, IV&V, and SI contractor, as well as other solution providers. We will establish both formal and informal channels for this to occur and document our approach in the Communication Management Plan developed during the planning phase of the project.

INT52 The Contractor shall collaborate with all State enterprise contractors and solutions to accurately collect, process, and distribute applicable HIPAA EDI transactions.

The Optum Provider Services solution includes our HIPAA gateway. Our HIPAA gateway will validate and verify all HIPAA EDI transactions received from or sent to DPHHS. Our integration layer ESB will receive, process, and route all inbound transactions conforming to HIPAA standards and the DPHHS specific companion guides. We will validate outbound HIPAA transactions for conformance to DPHHS companion guides, and route them to the DPHHS Integration Layer for further processing and routing. If a transaction does not pass validation, we will send a notification to the sending systems. We store all EDI transactions within our solution and they are retrievable in either the ANSI X.12 or human readable formats.

INT54 The Contractor's solution shall require (when appropriate), capture, and maintain the 10-digit NPI.

We capture and maintain the provider's National Provider Identifier (NPI) during the provider enrollment process. We use it, in conjunction with other national and state-issued identifiers and demographic data, to uniquely identify providers in the solution. Our solution checks the NPI entered by the provider to verify it meets the NPI format and passes the NPI check-digit algorithm. The NPI entered is also cross-referenced against other demographic information entered by the provider to make sure the NPI is the correct identifier for the provider.

INT55 The Contractor's solution, shall accept the NPI in all applicable standard electronic transactions mandated under HIPAA

We built the OIL core data model to support the common standard X.12 and HL7 transactions. As part of the data model, relative to provider information, the NPI is captured from all standard X.12 electronic transactions.

INT59 The Contractor shall ensure all hardware, software, and communication components installed for use by State staff are compatible with the State currently supported versions of the Microsoft Operating System, Microsoft Office Suite and Internet Explorer; and current technologies for data interchange.

Based on the State's technology utilization standards documented on your Enterprise Technology website, the Optum Provider Services solution will support the State's versions of the Microsoft Operating System, Microsoft Office Suite, and Internet Explorer; and the technologies used for data interchange.

INT60 Unless otherwise mutually agreed to in writing, the Contractor must maintain any and all hardware and software products required to support the Contractor's solution at their most current major version (patches, fixes, upgrades, and releases for all software, firmware and operating systems) or no more than one version back from the most current major version.

Optum uses a rigorous Agile product management and release management process that makes sure production applications are current on the latest releases, patches, and upgrades. By deploying our solution as part of our BPaaS environment, we can make sure those products supporting our solution are continuously updated and are at the most current release levels, or no more than one version back.

Redundant components and high availability architecture reduce the potential for system impact during maintenance. We do patching and similar changes server by server to prevent the entire application from being down at any one time.

Because changes to the applications or environment can affect availability, our change management process governs hardware maintenance and software releases. We evaluate changes for potential impact and risk where a higher level of risk requires additional approvals.

Major application changes and upgrades are bundled into specific planned releases. DPHHS and Optum will mutually agree upon lead-time notification for maintenance windows requiring downtime.

We may implement additional small releases outside of the normal release cycle, as required. In the most urgent situations, the emergency changes process can be used to implement high-priority changes, which cannot wait for the next release cycle. These changes require the approval of an executive and an Emergency Change Advisory Board (ECAB). Certain high-priority changes can use the normal change process still not waiting for the next release cycle.

Many routine modifications, such as a business rule change, may not require a change ticket or may use a pre-approved change process. We treat regulatory and legislative changes with the highest priority and can implement them using any of the change management approaches: standard, emergency, or pre-approved.

INT61 The Contractor's solution shall allow internal and external stakeholders to upload and view electronically submitted documents.

Internal and external users can upload documents through the solution to the Optum Federated Data Services component. Users can also pass the documents in electronic form through OIL to the MPATH Integration Layer for storage in the State's enterprise content management system.

Figure 3.8 illustrates the flow of document storage and retrieval through our solution.

[redacted]

OIL uses a set of standard APIs to upload documents to the Optum data services component and will interoperate with the MPATH Integration Layer through a mutually defined set of APIs. Document retrieval from the Optum FDS is managed through retrieval APIs in OIL and with mutually defined retrieval APIs with the MPATH Integration Layer. All electronic documents are virus-scanned upon upload. Documents failing the virus scan are rejected and notification is sent to the user.

INT62 The Contractor's solution shall ensure information and event notifications include aggregated and integrated information.

Our solution uses an ESB within our integration layer to route and orchestrate messages between applications and between the MPATH Integration Layer and us. Message notifications in the ESB are configurable to the message content and can be configured as information only, warning messages, or error messages. The specific message content can be configured for each application message. When application integration results in multiple messages, the message exchange and content can be configured so that messages can be aggregated. The message receiver (application or domain) can then respond to single message containing multiple events instead of responding to multiple individual messages.

INT63 The Contractor's solution shall have business process orchestration in an event-driven environment that maximizes process automation.

The Optum Provider Services solution is a highly automated process where the only manual intervention in support of specific provider credentialing activities and approval of provider applications by State Medicaid personnel. All other workflow is designed to be automated and flow seamlessly between our solution and you using our respective integration layers. The ESB that is part of our solution automates and orchestrates the exchange of data and messages within the solution. Workflow events and event notifications are automated through the ESB and support the automation of the business processes.

INT65 The system shall provide the ability to share and federate data with other data sharing partners.

The design imperative of OIL is to simplify application integration and share data with other partners, through a central core ESB and service adapters that are exposed to the ESB. OIL has implemented service adapters that communicate with the core canonical data model and then implementation-specific adapters communicate through the exposed service proxy adapters. The service adapters communicate across systems through the ESB to assure message delivery, orchestration, and error recovery. We will work collaboratively with you and the SI contractor to create and maintain the Interface Control Documents. The Interface Control Documents will describe the frequency and details regarding the exchange of information between solution components.

INT66 The Contractor's solution shall provide the ability to create/edit, send, receive and process X12, NIEM standardized transactions and NCPDP D.0 transactions relative to the Contractor's scope of work.

OIL uses standard X.12 service adapters and has a data model that is designed around the common X.12 transactions. In addition, OIL has embedded our HIPAA gateway for the validation and verification of X.12 transactions.

INT68 The Contractor shall collaborate with the Systems Integrator to automatically report system availability to the SI availability solution. The frequency of each module component verification will be defined by the Department.

We will collaborate with the SI contractor to automatically report system availability to the SI availability solution. We propose that our integration layer and the SI availability solution interact and exchange availability messages through mutually agreed upon ping messages and APIs. The frequency of the exchange of these messages will comply with the schedule defined by the State.

We designed our solution with high availability in mind, building in redundancy and stability. Our operational processes further support high availability by providing multiple levels of continuous monitoring, tightly managing change processes, and delivering best practice high-incident management services, in conjunction with our established ITIL Availability Management Processes. Our primary goal related to solution availability is to eliminate possible causes of unexpected downtime and mitigate any service disruptions as soon as possible.

In addition, we will calculate availability and response time metrics using our suite of system performance monitoring tools. Updated availability information and response times will be supplied to the availability dashboard website. We will work with the SI contractor to integrate our performance monitoring tools with the SI availability solution so that module availability is communicated timely and accurately to infrastructure management staff and users.

INT70 The Contractor shall identify and describe the licenses necessary for the scope of work to support the infrastructure that will provide sufficient bandwidth and redundancy to ensure accessibility, reliability/fault tolerance and acceptable performance.

We will provide our solution to you in a BPaaS delivery model. We will provide the necessary bandwidth, system reliability, and software licenses to support the performance SLAs we have with you.

INT73 The Contractor shall be responsible for understanding the business processes to automate and orchestrate appropriate workflows, business rules, data flow and metadata within the solution and work collaboratively with the SI.

We will work with you during the DDI phase of this project to document and implement workflows, business rules, and data flow to support this project. We have extensive experience in Medicaid provider enrollment and will use our experience in optimizing the data and workflows necessary to support this project. We will work collaboratively with the State and the SI contractor to discover and document functional and non-functional requirements and workflows. These requirements will be documented in the requirements traceability matrix document to make sure system and unit testing plans verify successful testing of all use cases and workflows. We will work collaboratively with the SI contractor documenting integrations and interfaces as part of the overall business process workflows, and will detail the interface specifications in the interface control documents. The system design document and solution architecture document will describe the overall component architecture and data flows that will be implemented in the solution.

INT74 The Contractor's solution shall have the ability to identify errors in transactions and immediately notify the source system of the specific errors including whether the errors have precluded loading and/or using the data.

Our integration layer, including our HIPAA gateway, validates all incoming data for compliance to industry standards and specific companion guides, data cleanliness and integrity, and conformance to reference standards (e.g., valid ICD-10 code). Transactions that do not pass data validation, integrity, and cleanliness edits will error, and our integration layer automatically and immediately notifies the sending system or user. Detailed error information is sent, along with the error notification, so that the transaction can be corrected and resubmitted.

INT78 The Contractor shall provide an environment where components can be added or replaced quickly.

OIL facilitates interoperability in the Optum Provider Services solution. The solution leverages OIL for loose coupling and abstracted integrations. This level of loose coupling and abstraction allows Optum to change components as technology innovations occur and business and regulatory requirements change. OIL sits between every internal and external solution component, supporting your MITA and interoperability goals for an interoperable platform and loosely coupled services.

Interoperable platform: The proposed solution is a distributed service architecture design that facilitates interconnection across disparate technologies, message protocol, and data types. The OIL solution is stateless and contains no business logic minimizing the need to keep like business logic managed in more than one place.

Loosely coupled services: This leverages a library of health care and human service-specific connectors and APIs. Connectors are combined from the library to interconnect technologies, in turn, reducing or preventing tightly coupled integrations. By leveraging industry-standard transaction types, such as HIPAA transactions, where we can, we reduce the dependency of specific component custom interfaces.

INT79 The Contractor's solution shall allow internal and external users to enter data using electronic forms and receive documents electronically from other systems.

The Optum Provider Services solution is designed to use electronic forms rendered as Web pages for providers to conduct enrollment and the self-service functions through the Provider Enrollment and Self Service portal, as Figure 3.9 shows.

State Medicaid users also will use electronic forms rendered as Web pages to access information from our solution in order to approve provider applications and review documentation. Our solution enables users to search for, retrieve, and view uploaded documents that are stored in our federated storage solution.

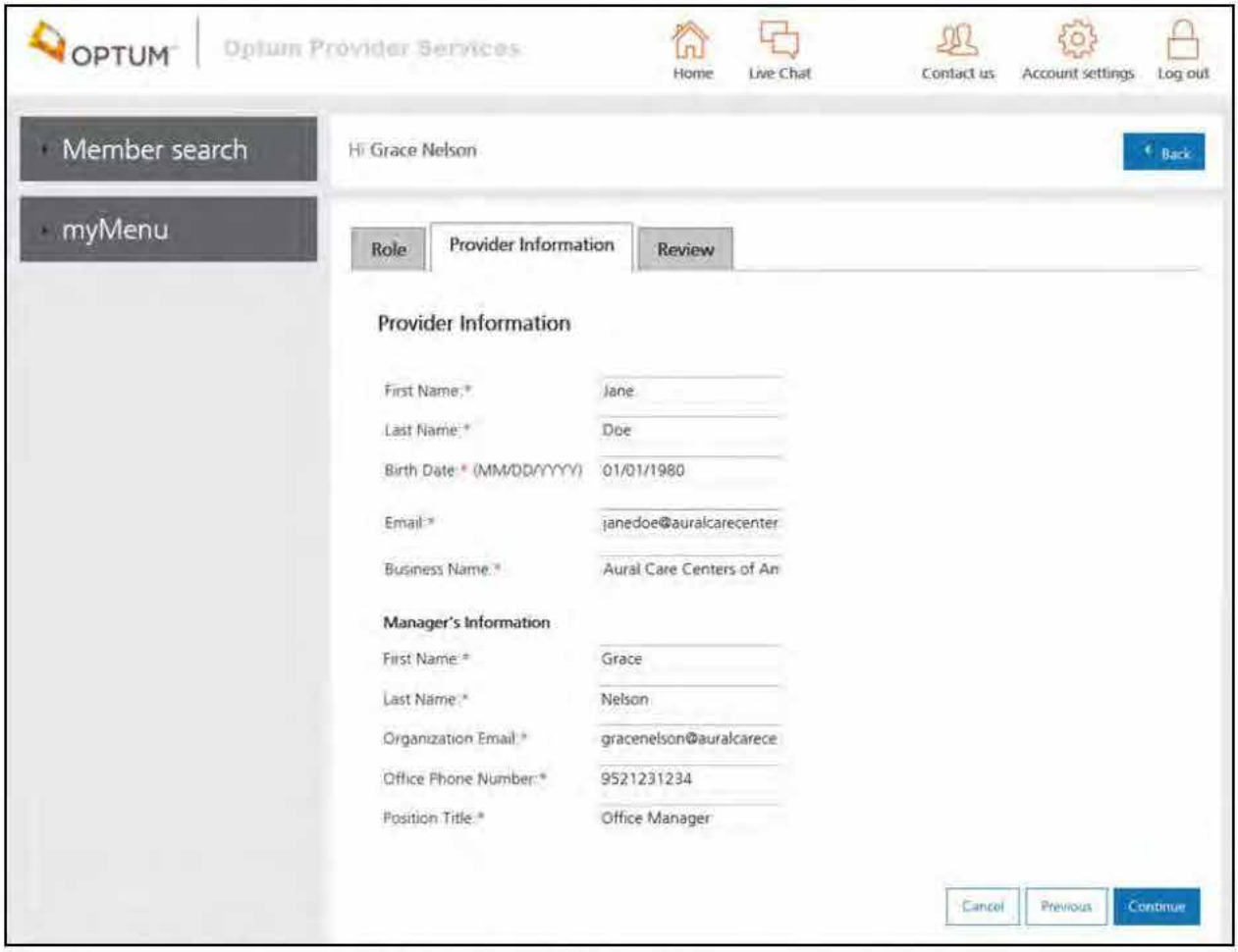


Figure 3.9: Provider Portal User Profile Tab for Provider Information.
Electronic forms simplify the data entry process by making sure required data is input and valid data is entered and updated.

INT80 The Contractor's solution will interface with the State's designated financial processing solution.

Our solution will enable the provider to securely submit their enrollment fees by credit card through our payment gateway. We will process the credit card payments and deposit the payments into a bank account established by the State for receiving those payments. Our secure payment processing gateway complies with all PCI regulations. The Optum Provider Services solution will send notification of the fee payment through your integration layer to your financial processing solution.

In addition, our call center staff will have access to the financial processing solution through a secure HTTPS link to update provider information and upload financial documents.

INT81 The Contractor's solution shall have the capability to receive and display data, messages, and alerts from other systems in real-time.

The Optum Provider Services solution is designed around a real-time system, enabled by the API integration in OIL. The solution minimizes the use of bulk data transfers and is designed around real-time entry, update, display, and retrieval of data, as well as messages and alerts across the solution.

INT85 The Contractor's solution shall support web services, specifications, and adapters: (e.g., ODBC, Web Service (WSDL, WS-*, SOAP, REST, UDDI, ODATA), JSON-WDP, MS SQL, SQL Server, Oracle, FTPS, SFTP, HTTPS, MSMQ).

The use of industry-standard technologies, such as description language-based Web services and transfer of XML messages through SOAP, are intrinsic capabilities of OIL that are central to the integration between you and us. The OIL capability that sets it apart from this basic capability is its internal use of a canonical HHS data model based on X.12 and HL7 standards and the adoption of the proxy service architecture pattern.

The interface technologies currently supported include the following:

- SFTP or FTPS
- File transfer using shared file system or pipe
- SOAP, WSDL, JSON, and HTTP through Web service
- RESTful services using XML, HTML, or JSON
- JMS and AMQP queueing not only for interface transactions, but also for workflow orchestration

The proxy service architecture of OIL enables Optum to deploy additional interface patterns and methods without disrupting existing data flows.

INT86 The Contractor's solution must be capable of receiving, translating, and processing data to and from the variety of protocols (e.g., FTP, FTPs, SFTP, HTTP, HTTPS, JMS, JDBC, ODBC, NET, AS2, AS3, POP3, SMTP, SSH, TCP, CICS). The Contractor shall include in their response a list of protocols supported.

OIL receives, translates, processes, and transmits data in various formats. OIL is built around a set of common service adapters to which consumer/producer proxy adapters communicate. The proxy adapters are implemented to transform the protocols and formats required by external applications to the formats necessary for the OIL service adapters. The formats that OIL already supports include SOAP, REST, FTP, FTPs, SFTP, HTTP, HTTPS, JMS, AMQP, ODBC, and JDBC. We can add other formats easily as business and technical requirements require.

INT87 The Contractor's solution shall provide context sensitive help (situational clarification and support associated with process specific steps), to support user activities (e.g., provider enrollment and maintenance activities).

The portal components of the solution provide context sensitive help to support user activities, provide guidance for workflow steps, and inform the user of critical and required data elements, as Figure 3.10 shows.



Figure 3.10: Provider Portal Context Sensitive Help.
Context sensitive help guides the user through data entry steps, explain search criteria, and describe required fields.

INT88 The Contractor shall implement a solution where module components are loosely coupled and can be added or replaced quickly.

OIL facilitates interoperability with the Optum Provider Services solution, including loose coupling and abstracted integrations. This enables Optum to change components as technology innovations occur and business and regulatory requirements change. OIL sits between every internal and external solution component, supporting your MITA and interoperability goals for an interoperable platform and loosely coupled services.

INT93 The Contractor shall provide electronic notification including detailed release notes for Major and Minor version , patches, updates and fixes deployed to the production environment.

We use a highly structured and rigorous Agile development methodology that governs the product management and development of our products, including applications, interfaces, and documentation. Part of that methodology is the development of detailed release notes for major and minor releases that we will share with you before deploying any changes to any environment. Electronic notification of release notes and electronic distribution of release notes are sent to specific users before any changes deploy to any environment.

INT94 The Contractor shall work collaboratively with module vendors to reconcile ODS data elements with the all data elements for each module component.

We will work with you to document the data elements in our module components that we will extract and pass to your ODS. We will provide you our conceptual data model that documents the data flows in conjunction with the end-to-end workflows and a data dictionary of the data elements in our system. In addition, we will use the data model and data dictionary to reconcile the data elements that are extracted and sent to your ODS.

3.10.1.5 Data Management

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

The Optum Provider Services solution can help DPHHS meet all federal and State privacy laws, including HIPAA, HITECH, and ARRA. We will install your system on the latest hardened infrastructure with encrypted drives and encrypt your data in transit.

Optum has privacy and security programs designed to support compliance with various federal and state privacy and security regulations, including HIPAA, CMS MARS-E, CMS ARS, IRS 1075 for FTI, and applicable state and local security and privacy requirements. We have the expertise required to design, implement, and maintain information systems that meet HIPAA, CMS, IRS, and NIST 800-53 compliance for hosted and developed solutions.

We meet security and compliance controls required by HIPAA, HITECH, ARRA, as well as other applicable federal and state privacy and security requirements. Our data management approach is based on industry best practices.

In the remainder of this section, we include our response to each of the Attachment F data management requirements.

DM04 The Contractor's solution shall maintain record/audit trail of errors during update processes, accounting for originating source and user.

The integration layer of our solution maintains a log of all error and warning messages arising in the processing of each update including the originating source and the user or application domain. The integration layer notifies the appropriate user or application of error or warning messages, for appropriate corrective action, including notifying the sender and identified stakeholders as needed.

DM09 The Contractor's solution shall provide audit trails to allow information on all transactions to be traced from receipt of the transaction through the completion of the transaction, capture at a minimum date/timestamp, data source, worker id, action taken and log any errors encountered for reporting.

The Optum Provider Services solution maintains audit trails of all updates made in the solution. Transaction updates can be traced from the receipt of the transaction (through batch file update or API) through to the completion of the update. The audit trails capture the transaction information, including date/time stamp of the update, source of the update, and user/application making the update. Applications that update data through bulk batch files generate error logs that are sent back through our integration layer to the appropriate user for resolution. Data updated through an API returns error statuses and error notification to the sending system for data correction and resubmittal.

DM10 The Contractor shall ensure that all narrative descriptions of codes and abbreviations are available for reporting.

Our solution uses industry-standard reference data (codes and descriptions) as well as reference data supplied by you in the processing of provider enrollment, re-validation, provider self-service activities, and customer service activities. These reference codes and their narrative descriptions are extracted and passed to the reporting and analytic component of the solution for inclusion in standard and ad hoc reporting.

DM108 The Contractor's solution shall provide a configurable workflow process for resolving near matches for providers that can link, void or end date extraneous records (i.e., duplicate provider records).

The workflow processes within our solution use an automated process for matching provider records. The models used for identity matching can be configured and tuned to the specific provider population to increase the rate of automated match. Provider records determined to not exactly match automatically route to our operations staff to manually determine provider matches. The provider matching logic and workflow enables the splitting and merging of provider records, as well as voiding extraneous records. Audit trails exist to document the matching (automated or manual) and the records that were matched, split, or merged.

DM11 The Contractor shall develop and maintain an electronic data dictionary using industry best practices to be approved by the Department. At a minimum, the data dictionary shall contain for each field: field name in human readable format, field description, database field name, database table, field type and length, valid values and their corresponding descriptions.

Our solution maintains an electronic data dictionary of our data model in a human readable (XML) format. We will share the data dictionary of our solution with you as we implement our solution. Our release management process also demands that any updates to our solution include updates to the data dictionary.

DM115 The Contractor's solution shall collect, store, and maintain the data necessary for T-MSIS reporting as required by CMS.

Our solution will capture, store, and maintain the provider data necessary populating the T-MSIS provider file. It will also capture, store, and maintain the provider demographic, location, licensing, identifier, taxonomy, enrollment records, bed types, and affiliated groups and program information necessary for T-MSIS reporting. Our solution will extract the information and provide it to you through your integration layer in a mutually defined format for you to format and report to CMS.

DM116 The Contractor's solution shall capture and maintain the provider related data items needed to support Payment Error Measurement (PERM) processing.

Our solution retains and maintains the provider demographic and identification information (name, address, phone number(s), NPI, specialty taxonomy) to support PERM processing and reporting.

DM117 The Contractor's solution shall retain in the module, after implementation, seven (7) years of electronically imaged documents and data. After seven (7) years, the data will be purged (deleted) from that module. All active records (active providers, active members, active cases, etc.) and 100% of all history for any entity or case that has been active within the last seven years will be retained. Any entity and/or case that has been continuously inactive for the last seven years will not be retained, will be purged, and will no longer be accessible by users in that module.

The Optum Provider Services solution will maintain electronically imaged documents and data within our system to comply with your requirements for active and inactive records. Our solution includes a dynamically expandable Enterprise Content Management (ECM) system for document and image storage and retrieval.

Our ECM is a dynamically expandable object storage solution with a simple Web service interface to store and retrieve large numbers of data and image files. It delivers high durability and scale, serving as our primary storage service. Our ECM solution includes a collection of technologies for storing, virus scanning, transforming, identifying, sharing, and retrieving files across multiple sources.

The ECM retains document metadata that includes information linking documents to the provider and enrollment records. We can remove entities from our system that are inactive, as determined by your policies, as well as purge their associated documents and images from our

storage solution. We will periodically examine the inactive provider records, along with a list of the linked documents, and will obtain approval from you to remove their linked information and documents.

DM13 The Contractor shall be able to demonstrate the ability to support requirements for backup and archiving consistent with Department SLAs and CMS, State, and industry standards. The Contractor shall also adhere to data retention requirements cited in 45 CFR 164.316 and the State's Administrative Rules.

Optum will demonstrate backup and archiving capabilities that will align with Department's SLAs, CMS, State, and industry standards. Our data backup and recovery retention standards guidelines govern how these capabilities apply. These standards dictate backup type, frequency, and longevity of retained data. Furthermore, our hosting environment is fundamentally designed and built to meet or exceed FISMA and MARS-E 2.0 data security and compliance regulations. These complementary controls will support the State's needs.

DM14 The Contractor's solution shall maintain an audit trail of all changes to data, including changes that were made in error and subsequently backed out of or suspended.

Our solution maintains audit trails of all changes or updates made in the solution. The audit trails capture the transaction information, including date and time stamp of the update, source of the update, and user/application making the update. Applications that update data through bulk batch files generate error logs that are sent back through our integration layer to the appropriate user for resolution. Data updated through an API returns error statuses and error notification to the sending system for data correction and resubmittal.

DM15 For audit and reporting purposes, the system shall provide and maintain the following data for all reference codes:

a. Effective date

b. End date

c. Date when last changed

d. Who made last change

e. Short description

f. Long description

Our solution uses reference codes from national sources (e.g., AMA) as well as from DPHHS. From our experience, you will have unique reference code requirements to support your existing legacy systems as you make the transition to the final integrated architecture. Reference codes maintained in our solution (both internally developed and COTS application) will maintain the date sensitivity of the code, who made the last change, and short and long descriptions. We assume that any reference code information passed to the Provider Services module will contain the information necessary to retain.

DM17 The Contractor's solution shall provide the ability to store and apply updates to all applicable codes upon new release at an interval appropriate for the data or when requested by the Department.

We routinely update the reference code information in our applications as the reference information becomes generally available from our sources. We will notify you of any reference code maintenance windows. Off-schedule reference code updates will occur at mutually defined intervals to minimize any production system impact.

DM18 The Contractor's solution shall perform batch control including logging and reporting.

The integration layer of our solution manages the sending and receipt of batch files into and out of our solution. Our integration layer performs all batch file control and logs the sending and receipt of batch files. It also manages the push/pull of data into/out of the secure file folders that

are part of our SFTP process and manages the archiving of files sent and received per your data retention policies. Reporting is available on the flow of data files through our integration layer.

DM19 The Contractor's solution shall archive all versions of reference information and update transactions.

Our solution maintains audit trails of all data changes within the applications. We will maintain and archive all versions of reference information provided to us by external national sources and by you.

DM20 The Contractor's solution shall have the ability to void or reverse recent changes by rolling back to prior configurations.

The solution supports the ability to roll back to prior configurations. Optum has adopted the Optum Structured Agile Method (OSAM) as a framework for all product development and release management. OSAM dictates that all product updates, including configuration changes are thoroughly tested, accepted, and signed off before promotion to production environments. Our process also dictates that we retain the ability to roll back to prior application configurations if defects or issues are discovered with the production deployment of new application releases, patches, fixes, or configuration changes.

DM21 The Contractor's data management strategy shall include the following concepts: Data Integrity (data cannot be modified undetectably), Data Availability (access is not inappropriately blocked or denied), Data Authenticity (validation of transactions), Data Security (encryption and Department approved security protocols and processes), Non-repudiation of Data (parties to a transaction cannot deny their participation in the transaction).

Our data management strategy supports the concepts of data integrity, data availability, data authenticity, data security, and non-repudiation of data through our integration layer. These concepts are inherent to the core capabilities of our integration layer and we take full advantage of these capabilities as part of our solution.

The integration layer of our solution enforces data integrity by managing and monitoring the routing of data between solution components; and the accompanying messaging informs the receiving application of the intent of the data (insert, update). Misrouting of data will result in an error condition within the integration layer and our operational staff will correct the error condition. Message routing within the integration also prevents data non-repudiation and enforces data availability in that refusal of a message or data instruction, or unavailability of a solution component will result in an error condition as well.

The file gateway and API/Web service gateways, ESB, and the data model within our integration layer work together to enforce data authenticity. They validate that transactions contain valid, standardized, and harmonized data, eliminating the need for point-specific validation routines with each solution component. The gateways assure that only authorized applications and users can access or update information as it transits our components. In addition, the gateways are responsible for data security through the encryption of information at rest with solution and in transit as the data enters and exits our solution.

DM22 The Contractor's solution shall provide entity search capability including the ability to search by entity type, entity name, entity address elements, entity phone number(s), unique identifier for entity type, any alternate identifiers including EIN, SSN, TIN and other demographic elements.

Our solution enables the user (provider or State Medicaid Agency user) to search for providers through the provider portal by various parameters, including provider unique identifier, name, type, and other demographic information. We will configure the search criteria requirements with you during the DDI phase of this project and adjust the search parameters to support your business requirements.

DM23 The Contractor shall provide real-time access to transactional data for all module components

Our solution makes extensive use of real-time APIs to update and retrieve data from the transactional systems. This provides the user with the most current data stored in each application. The Provider Portal and State Medicaid Agent Portal communicate with the balance of our solution through real-time APIs so that the user is always working with the most up-to-date information.

DM24 The Contractor shall ensure complete transparency of all data fields in reports generated by the system including: providing the Department with SQL, pseudo code, narrative description, analytic protocols and assumptions to document the logic and formulas used in all calculations.

We will provide report descriptions and a data dictionary as part of the implementation of our solution. Authorized State users can view report definitions that are part of our reporting component to validate how report data is retrieved, data calculations, and the report logic.

DM25 The Contractor shall create and maintain a suite of State/Contractor-defined on-line reports to allow users to choose from pre-built defined parameters (such as provider number, procedure code, date of service, etc.) to generate customized reports for monitoring the daily operations of the system and Fiscal Agent Operations.

The Optum Provider Services solution includes a comprehensive reporting and analytics module that provides you standard analytic and reporting requirements, as well as the flexibility to extract and provide data for State and federal reporting. The reporting component of our solution delivers a single-entry point, through the State Medicaid Agent Portal, for all of your analytic and reporting needs. Our solution harmonizes disparate data and enables a full range of analytic and presentation tools that deliver simple numerator/denominator calculations to complex statistical analysis capabilities. Users can use pre-built parameters to generate ad hoc and customized reports in addition to our standard report output. Our approach to reporting and analytics addresses the gaps caused by fragmented, inconsistent, and incomplete data. It will provide you the most complete, reliable, transparent, and integrated platform to support your reporting and analytical needs.

DM26 The Contractor shall certify that any and all unmasked or unscrambled Department data will reside in data centers located in the continental United States. Additionally, this data will only be accessible by resources within the continental United States that have completed the necessary HIPAA and PHI training. Any data that will be accessed by resources that are not physically located in the United States will be masked or scrambled (which would make it impossible to establish a connection between claims data and a specific member or provider associated with the claim) thereby removing the HIPAA and PHI connection between interested parties and the claim data.

The Optum hosting environments supporting the State's solution are physically located in the continental United States. Data relative to the solution as it is hosted will only be done so by personnel located within the continental United States. Optum personnel privileged to access the State's data will have confirmed completion of necessary data compliance and security training.

DM31 The Contractor's solution shall be configured and maintained to validate and standardize addresses according to United States Postal Service (USPS) verification, validation and standardization rules.

Our solution verifies, validates, and standardizes provider addresses in real time through direct integration with the USPS. Providers have the opportunity to correct addressing information to comply with USPS formats.

DM37 The Contractor's solution shall facilitate real-time data processing including data cleansing, data loading, data brokerage, integration, validation, reconciliation, and synchronization with the State's enterprise.

Our solution can communicate with the State's enterprise through OIL and the State's integration layer. OIL and your integration layer should communicate through mutually defined and supported APIs to facilitate real-time data exchange. The ESB and proxy service adapter

APIs within OIL and the coordinating APIs and ESB within your integration layer will make sure that data exchanged between our two platforms synchronize for data cleanliness, validation, governance, and reconciliation. Errors in data integration will route by the respective ESBs to the systems or users responsible for corrective action.

DM38 The Contractor's solution shall optimize and consolidate data management storage.

Our logical approach to data optimization and management inherently meets the State's requirement. Optum will demonstrate this capability by using technical controls that ingest, process, and store data efficiently, while employing business processes geared to the State's needs to govern accessibility in an effective manner.

DM39 The Contractor's solution shall maintain all data sets defined by the HIPAA Implementation Guides to support storage of all transactions required under HIPAA Administrative Simplification Rule (e.g., Gender, ReProject Namen Code) for seven (7) years.

Our solution enables us to monitor and report on activity within the solution components and includes a dynamically expandable ECM system for document and image storage and retrieval. The ECM retains document metadata that includes information linking documents to the provider and enrollment records. We can purge entities from our system that are inactive, as determined by your policies, as well as purge their associated documents and images from our storage solution.

DM40 The Contractor's solution shall maintain a normalized RDBMS with referential integrity and is optimized to meet performance requirements.

Our solution is delivered as SaaS. Our solution uses a combination of industry-leading RDBMS technologies and NoSQL technologies. Our relational databases maintain referential integrity and the data models are normalized for best database performance. The technologies behind the solution we are proposing will, at minimum, meet the performance requirements defined by the State. Our operations personnel constantly monitor and optimize database performance to meet the solution SLAs demanded by our clients.

DM41 The Contractor's solution shall provide a method to access, query, and report against archived data external to the Operational Data Store (ODS).

Our solution will provide online access to data stored in the component applications until the records are inactivated or purged according to your business requirements and retention policies.

DM43 The Contractor shall demonstrate through data analysis that the implementation outcomes have been validated and are accurate.

We will work with you in the requirements phase to identify targeted implementation outcomes and the data and algorithms to accurately validate them. We will collect that data and execute those algorithms accurately to report on implementation outcomes.

DM45 The Contractor's solution shall maintain a history of provider information (i.e., full audit history or equivalent capabilities). All transactions, including the execution of database scripts, need to be recorded in the full audit history.

Our solution maintains a complete history of the provider enrollment and re-validation records and activity. The records are exportable as part of reporting a complete audit history of changes to the records.

DM46 The Contractor shall develop and maintain a process to archive and access archived data (including legacy MMIS component data).

Our implementation plan includes the conversion of legacy MMIS component data into our solution. As data in our solution ages, and records become inactivated and are archived, we will provide a mechanism to retrieve and access those archived records.

DM47 The Contractor shall participate in ongoing data governance meetings as required by the Department.

We agree to participate in ongoing data governance meetings with you as required.

DM51 The Contractor's solution shall provide the ability to modify transactions in real-time.

Our solution portals communicate to the applications using APIs through our integration layer to the applications that are part of our solution. The APIs provide real-time access to the data stored in our applications. Where possible, our solution design will communicate with your integration layer through mutually agreed upon APIs. Through these APIs, data in our overall solution updates in real time.

DM52 The Contractor's solution must have the flexibility to quickly accept new and incremental data items from module components required by the ongoing component, product or service integration.

Our solution components accept both new and incremental data. New or incremental data can be loaded into our solution components through either API or bulk loaded through a batch file interface.

DM53 The Contractor's solution shall provide an address type, effective dates, and the ability to select the type of address for provider mailings.

The Optum Provider Services solution can maintain multiple addresses per provider with effective dates and address type. All addresses can be sent to the Correspondence Management modules for letter generation and the letter template can be designed to determine the most appropriate address to use in the composition and delivery of correspondence.

DM54 While the Department prefers real-time/event driven process, the Contractor shall provide a tool to easily administer and execute scheduled events (e.g. reports, file transfers, processes, notifications) to be performed on a regular basis (e.g. daily. weekly, monthly).

Our solution supports real-time and event-driven processes. We schedule some processes, such as bulk data loads or data extracts, at times to minimize the impact or disruption to the production system. The solution can process those scheduled transactions and our operations staff will work with your staff to implement processes that have to be scheduled.

DM55 The Contractor shall provide a conceptual data model (CDM) that identifies the data elements required for an end-to-end business process execution including the identification of data standards that will reduce future rework to achieve successful data sharing across the enterprise and for intrastate/interstate exchanges. The CDM is required to be used as a reference to provide high-level overview of the data and relationships used by the enterprise and to provide a tool for ensuring the completeness of the business model.

We will provide you a conceptual data model as part of the DDI phase that details the flow of data between the application components in our solution and between our solution and your integration layer. The conceptual data model will follow closely with the documented business workflows and the solution architecture and solution design documents.

DM57 The Contractor shall standardize the structure and visibility of data and applications to support automated electronic data exchanges within the State's enterprise to promote interoperability.

The integration layer of our solution provides a standardized method to promote interoperability with automated electronic data exchanges within the State's enterprise. OIL can leverage and

integrate with almost any existing solution, asset, or system. OIL supports integration using legacy FTP, for batch methods, message queuing (JMS), modern transactional Web services, or representational state transfer (RESTful) APIs. It can also support a broad range of data formats from the originating or receiving applications (data transformation), including JSON, XML, flat file, COBOL copybook, and other proprietary formats. OIL has an HHS-specific design, including a canonical data model and interface library built on the X.12, HL7, and Federal Data Services Hub (FDSH) API connectors. Originally designed to integrate legacy platforms with modern systems in these domains, OIL is well suited for an enterprise like DPHHS as it transitions between both types of systems.

OIL is a differentiator in this regard because it will enable DPHHS to incrementally implement the MPATH integration layer. OIL isolates the Provider Services solution from changes in the DPHHS infrastructure, thereby eliminating costly integration re-work due to changes in application integration patterns.

This broad integration ability uses implementation-specific adapters or service proxies that communicate with the OIL core. Each service proxy exists between a modern or legacy enterprise system and a standard OIL service supporting an HHS-specific data format and transaction technology as referenced above. This approach supports modularity and interoperability, rather than just a general-purpose ESB implementation.

OIL further extends this design pattern by implementing canonical models for each of the supported data sets in its core. When the data is transformed to a standard model by the producer proxy service, then additional workflow and orchestration inside the service layer uses the standard model. At the consumer end of the integration, a service proxy is implemented to convert the data to any non-standard output format. Thus, extensions to the platform need to focus on proxy development, not core changes.

DM58 The Contractor's solution shall maintain online access to at least four (4) years of selected management reports and five (5) years of annual reports.

The reporting and analysis component of our solution will enable authorized State users to generate standard and ad hoc reports for specific periods. Once generated, we will save the reports to our ECM component for future access. We will maintain online access for at least four years of selected management reports and five years of annual reports, as required.

DM60 The Contractor shall be responsible for data management including ensuring the architecture addresses data semantics, data harmonization, and shared-data ownership.

We agree that we are responsible for data management of our own data model. We will cooperate with your data governance operation and the SI contractor to resolve issues of data semantics, data harmonization, and shared ownership for data issues that involve multi-module business processes.

The OIL data model enables us to harmonize the data into common values and formats. Data mapping through the OIL data model enables us to insert and replace solution components over time without disrupting existing data flows or data sharing capabilities. The OIL ESB codifies data sharing ownership and data sharing agreements between applications. Data transformations and data flow are mapped and managed through the ESB and conditions are set to verify the completeness of data updates and data retrieval.

The integration of OIL with your integration layer, through a set of mutually defined APIs extends the data management of OIL to your integration layer. Our respective integration layer then manages the semantics, harmonization and shared ownership, and management of data in our joint overall solution.

DM62 The Contractor's solution will ensure current and historical provider IDs are linked back to one universal/common identifier.

The Optum Provider Services solution uses an internal identifier crosswalk capability to link multiple provider identifiers (e.g., NPI, TIN, UPIN, DEA number) to a single internal identifier. Historical identifiers are maintained so that current and historical identifiers can link to the single common record/entity.

DM63 The Contractor's solution shall assign standardized unique internal identifiers for entities and prevent the creation of duplicate records.

Our solution assigns a standardized and unique internal identifier to each unique provider and maintains a crosswalk capability to link multiple provider identifiers (e.g., NPI, TIN, UPIN, DEA number) to the single internal identifier.

DM64 The Contractor shall be responsible for backup and retention of data to include:

1. Daily incremental backups with retention of sixty-one (61) days.
2. Weekly incremental backups with retention of twelve (12) weeks.
3. Monthly full backups with retention of eighteen (18) months.
4. Annual full backups with retention of seven (7) years.

The Optum hosting environment supports adherence to FISMA and MARS-E 2.0 data retention and disposal regulations. This governs the retention length of daily, weekly, monthly, and annual backups, which exceeds the State's requirements.

DM69 The Contractor's solution shall maintain online access to all reference tables with an option to search and display by reference data type and code.

Our solution provides online access to reference tables and codes with the ability to search and display the reference data by type and code. Our solution only allows authorized users access to these reference tables.

DM70 The Contractor's solution shall maintain user controlled parameters for all standards and messages.

The Optum Provider Services solution is deployed in a SaaS model. In collaboration with DPHHS and the SI contractor, our operations staff will manage configuration of standards and messages.

DM71 The Contractor's solution shall verify that all dates are valid and reasonable.

Our solution will validate that dates are valid and in the formats necessary for use by our applications, as well as conform to formats documented in the interface specifications.

DM72 The Contractor's solution shall provide proper data validation rules (e.g., all fields defined as alphabetic contain only alphabetic data, fields defined as numeric contain only numeric data, items with definitive upper and/or lower bounds are within the proper range).

Our solution will apply data validation checking on data that is exchanged between the components of our solution and data is exchanged with you through your integration layer. The portals will also perform data validation checking on data entered through the portal to make sure properly formatted data passes to the integration layers for use by other components of the solution.

DM73 The Contractor's solution shall capture and maintain the data items needed for State or Federal reporting requirements.

Optum will work with the State during the course of the DDI phase of the project to capture and maintain the data necessary for currently required State and federal reporting and make it reportable in our solution.

DM74 The Contractor's solution shall validate calculated data items.

Our solution will validate calculated data items for data items that are an intrinsic part of our application or our reporting system.

DM75 The Contractor's solution shall validate, and/or verify that all data items that contain self-checking digits (e.g., National Provider Identifier) passes a specified check-digit test.

The solution performs data validation, including check-digit testing on all identifiers that include a check-digit algorithm. It also performs data type and format validation at data entry so that only valid data is entered into the solution.

DM79 The Contractor's solution shall support the Extract, Transform and Load (ETL) processes from real-time web services or batch processes.

The ETL processes necessary to load bulk data into our solution, or to extract data to send to your integration layer will use a combination of real-time APIs and batch processes. Data export ETL processes typically use batch processes, while bulk data loads into our customer service application (for Option B Services) will use an API.

3.10.1.6 Interfaces

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

Industry-standard technologies, such as description language-based Web services and transfer of XML messages through SOAP, are intrinsic capabilities of the Optum Provider Services solution. The OIL component of the solution supports industry-standard communications with the external data sources, and different components of the overall solution. These standards include NIEM, NIST, and HIPAA compliance standards. A key differentiator of the OIL component is its internal use of a canonical HHS data model based on X.12 and HL7 standards and the adoption of the proxy service architecture pattern.

The interface technologies currently supported include:

- SFTP or FTPS
- File transfer using shared file system or pipe
- SOAP, WSDL, JSON, and HTTP through Web service
- RESTful services using XML, HTML, or JSON

OIL also supports JMS and AMQP queueing not only for interface transactions, but also for workflow orchestration and flow control.

In the remainder of this section, we include our response to each of the Attachment F interface requirements.

INR01 The Contractor's solution must ensure that all data exchanges including inbound and outbound interfaces shall comply with industry standards (e.g., National Information Exchange Model (NIEM), National Institute of Standards and Technology (NIST), HIPAA-compliance standards, Health level 7 (HL7), Fast Healthcare Interoperability Resources (FHIR)).

Data exchange in our solution is managed through our integration layer. The integration layer supports industry-standard communications with external data sources, and different components of the overall solution. These standards include NIEM, NIST, HL7, and HIPAA compliance standards.

INR02 The Contractor shall support the exchange of data between the System and the systems with which it interfaces (including external entities) to facilitate business functions that meet the requirements of Department policy, and federal and State rules and regulations.

The integration layer component of the Optum Provider Services solution provides the ability for the solution to interface with external entities, and facilitate business functions to meet DPHHS' policy requirements and federal and State regulations. OIL acts as the service integration layer and can leverage and integrate with almost any existing solution, asset, or system. OIL supports integration using legacy FTP, for batch methods, message queuing, modern transactional Web services, or RESTful APIs. It can also support a broad range of data formats from the originating or receiving applications (data transformation), including JSON, XML, flat file, COBOL copybook, and other proprietary formats.

OIL has an HHS-specific design including a canonical data model and interface library built on the X.12 and HL7 connectors. Originally designed to integrate legacy platforms with modern systems in these domains, OIL is well suited for an enterprise like DPHHS as it transitions between both types of systems.

OIL is a differentiator in this regard because it will enable DPHHS to incrementally implement the MPATH integration layer. OIL isolates the solution from changes in the DPHHS infrastructure, thereby eliminating costly integration re-work due to changes in application integration patterns.

INR04 The system shall send and receive real-time discrete transactions between modules and the State's integration platform to reduce the need for bulk data transfers.

Our solution is designed using a library of standard service adapters/APIs. This differentiating design principle makes extensive use of real-time transactions through services, as opposed to bulk data transfers. Our solution accepts and processes bulk data transfers efficiently; however, it is optimized to support SOAP and RESTful services with JSON and XML payloads. The integration layer ESB orchestrates the service transformation and routing between applications (internal and external to the solution). We expect that our integration layer will communicate primarily with your integration layer through real-time services.

INR05 The Contractor's solution shall provide the ability to view raw daily interface files for up to sixty (60) calendar days. Archive raw daily interface files after sixty (60) calendar days and maintain for up to six (6) months.

The solution will retain and archive raw daily data files sent to Optum by the State for up to 60 calendar days and will archive the raw daily data files for up to six months. Files retained by our solution are encrypted at rest, and authorized users with the appropriate security credentials can access and view retained data files.

INR06 The Contractor's solution shall provide the ability to view raw monthly and quarterly interface files for up to one year (365) calendar days. Archive raw monthly and quarterly interface files for two years (730) calendar days and maintain for up to two (2) years.

The solution will retain monthly and quarterly raw data files for up to 365 calendar days and will archive monthly and quarterly raw data files sent to Optum by the State for up to two years. Files retained by our solution are encrypted at rest, and authorized users with the appropriate security credentials can access and view retained data files.

INR07 The Contractor shall document all interfaces in an Interface Control Document (ICD) which will include data layout documentation, data mapping crosswalk, inbound/outbound capability and frequency of all interfaces.

We will work with you to develop Interface Control Documents (ICD) that fully document the operation, data mapping, and data routing for all interfaces between our solution and your integration layer.

INR08 The Contractor's solution shall include a process and toolset to maintain interfaces, code, and data models.

We use a highly prescribed and rigorous Agile development methodology to govern our product development. OSAM makes sure that all products (e.g., applications, interfaces, documentation) adhere to a formal development, testing, and release process.

INR11 The Contractor shall design, develop and maintain interfaces. Each Application Program Interface (API) and components that will interface with the Systems Integration Services Integration Platform will be documented using a mutually agreed upon ICD template. This effort is performed in collaboration with other stakeholders in the State's healthcare programs enterprise.

We will cooperate with the SI Contractor, your governance operation, and other stakeholders in developing a template for ICDs. When we create new interfaces, we will document them according to that template.

INR12 The Contractor shall ensure proprietary interfaces and protocols between modules are not used.

The solution does not use any proprietary interfaces between its modules. We will only connect with MPATH modules using industry-standard protocols and interfaces.

3.10.1.7 Business Rule

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

Our solution is a commercially available, cloud-based solution built on an industry-leading CRM platform. The solution provides powerful pre-defined workflow and reporting tools that enable us to configure our operations to support State-specific provider enrollment requirements. We provide our solution in a BPaaS delivery model. As part of the BPaaS delivery, the workflow to enroll, validate, and credential providers is internal to our solution. The workflow rules and business rules relative to the provider enrollment are pre-configured and optimized to support our solution.

Our BPaaS model:

- Enables faster time to market in a cloud-based solution with a flexible API architecture
- Features an extensible and scalable platform to meet the DPHHS' needs

- Provides end-to-end visibility and greater transparency
- Enables compliance with evolving regulatory mandates
- Provides integrated validation of licensing, sanctions, and exclusions

The provider enrollment, credentialing process, and workflow can differ slightly from state to state. Our solution has sophisticated tools embedded that our operational users use to rapidly configure and deploy workflow and business rules to support your specific requirements. The advantage of offering our solution as BPaaS is that we manage the entire provider enrollment, credentialing, and re-validation. This will help your resources focus their efforts on other strategic initiatives.

In the remainder of this section, we include our response to each of the Attachment F business rules requirements.

BR01 The Contractor shall configure, support and maintain a business rules engine (e.g., add, modify, or remove/retire rules) based on the Service Architecture (SOA).

Our operational staff will configure the business rules engine internal to our solution in collaboration with you to meet your business requirements. Our solution integrates with our integration layer using pre-defined APIs.

BR02 The Business Rules Engine (BRE) shall allow authorized system users including Department resources, the ability to create, configure and maintain rules for business functions in a user-friendly graphical user interface (GUI) that facilitates rules maintenance without coding changes.

Our solution includes sophisticated rules engines for the processing and routing of provider enrollments and revalidation. Our operational staff is responsible for configuring the rules engines in collaboration with you to meet your business requirements.

BR03 The Contractor shall provide real time access to a Business Rules Catalog, in an electronic format approved by the State, that documents all business rule logic used by the solution.

The Optum Provider Services solution uses pre-built business rules and workflow rules optimized to support provider enrollment and revalidation activities. We will work with you to modify rules to support your specific business requirements. Electronic documentation of all rule configurations is maintained and can be made available to DPHHS.

BR04 The Contractor shall update the Business Rules Catalog with all additions or changes.

We will provide you with documentation on the processes we use to enroll, validate, and credential providers so that you thoroughly understand the business processes and workflows internal to our solution.

BR05 The Contractor's Business Rules Engine shall be integrated into a testing environment that contains production data to allow users to perform "what if testing" and compare the before and after outcomes. The Contractor will provide Department staff and designated project resources, support and access to reports or reporting tools to evaluate the impact analysis.

The rules engines that drive our solution are embedded as part of our solution. The rules engines will be present in all of the environments we manage for you. We do not recommend using production data within a testing environment because of the increased possibility of exposing protected health information. From our experience, we can perform “what if’ testing” of automated processes using de-identified data that functions similarly to production data and does not incur additional risks of exposing sensitive data.

BR06 The Contractor's Business Rules Catalog shall include granular check-out and check-in rules and an audit trail of business rules changes.

In conjunction with our standard change control procedures, we will document and coordinate with DPHHS any changes to business rules or transaction routing rules internal to our solution.

BR08 The Business Rules Engine shall allow changes to be made to valid values without impacting production rules engine availability and operations.

We employ rigorous and proven application change control procedures. We thoroughly document and test any changes made to business rules or transaction routing rules to comply with the testing procedures we develop with you. Changes to production systems are scheduled and communicated in advance to eliminate disruption to existing operations and system availability.

BR09 The Business Rules Engine shall include the ability to debug business rules at rule execution.

We thoroughly debug and test business rules and transaction routing rules according to our established change control procedures and to comply with the testing procedures we develop with you. Workflow rules and transaction routing rules are built-in components of the applications we deploy as part of our solution.

BR10 The Contractor shall provide the ability to allow multiple users to work concurrently on different parts of the same rule base.

The ability to create and edit workflow rules and transaction rules are built-in functions of the applications we use as part of our solution. The individual applications enable multiple users to create/edit different rules simultaneously; however, the applications do not allow multiple users to simultaneously create/edit the same rule.

BR11 The Business Rules Engine shall have the ability to rollback to prior versions of rules without impacting production rules engine availability and operations.

We employ rigorous and proven application change control procedures. We thoroughly document and test any changes made to business rules or transaction routing rules to comply with the testing procedures we develop with you. Changes to production systems are scheduled and communicated in advance to eliminate disruption to existing operations and system availability. Our change control procedures enable us to roll back to prior versions of application changes if rollback is necessary to recover production environments from an unintended defect in a business rule or transaction routing rule.

BR12 The Contractor shall provide and maintain a graphical representation of business rule flow(s) and orchestration for all business rules.

We will provide and maintain complete documentation of the business workflows and transaction routing rules as part of the delivery of our solution to you.

BR13 The Business Rules Engine shall have mechanisms to identify which rules are executed for each specific business process.

We will provide and maintain complete documentation of the business workflows and transaction routing rules as part of the delivery of our solution to you. This documentation will detail the workflow processes and transaction routing that support each business function provided as part of our solution to you.

BR14 The Business Rules Engine shall be able to produce a report on rules passed or failed for all transactions.

The applications we use as part of our solution employ fully integrated capabilities to assure completion of all workflows and transactions. Workflow processes and transactions that do not

complete successfully will not update the production data and users are notified of the failed process or transactions.

BR15 The Business Rules Engine shall send alerts to the appropriate resource for issues identified in the rules engine. The Contractor will take appropriate action to address any alerts or rule failures.

The applications we use as part of our solution employ fully integrated capabilities to assure completion of all workflows and transactions. Workflow processes and transactions that do not complete successfully will not update the production data and users are notified of the failed process or transactions.

BR16 The Business Rules Engine rules editor shall allow subject matter experts or technical resources to write natural language business rules (i.e. human readable).

The applications we use for our solution have inherent functionality to create and edit rules. Since our solution is provided in a BPaaS method, our team maintains the business rules logic across all components of the application. One of the benefits of the BPaaS approach is the delivery of the services required by DPHHS, without the Department having to rely on your own staff to maintain the functionality of the system. Our team makes certain that the overall solution performs business processes in accordance with your requirements. When modifications are required, we manage that change process for you. You can then focus on more critical program management activities rather than making modifications to the technology solution that we provide for you.

BR17 The Business Rules Engine shall provide the ability to prioritize, sequence, and allow administrators to control processing.

In coordination with your resources, we will manage configuration of the workflow processes and transaction routing rules within our solution.

BR20 Where applicable, the business rules engine shall use standardized business rules definitions.

The applications we use for our solution have inherent functionality to create and edit rules. Because we provide our solution in a BPaaS method, we configure and maintain the business rules across the entire solution to meet your specific business processing requirements.

BR21 The Contractor's business rules shall execute in a runtime environment.

The applications we use for our solution execute workflow and transaction routing rules in real time.

3.10.1.8 Enterprise Content Management

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

Our solution includes a federated solution for ECM hosted in our private cloud. Our ECM is a dynamically expandable object storage solution with a simple Web service interface to store and retrieve large numbers of data and image files. It delivers high durability and scale, serving as our primary storage service. Our ECM solution includes a collection of technologies for storing, virus scanning, transforming, identifying, sharing, and retrieving files across multiple sources.

Key features of our ECM solution include the following:

- Synchronous and asynchronous RESTful APIs to store and retrieve documents and images
- A comprehensive security framework managed by Optum
- Automatic virus scanning
- Any-to-any file format conversion with digital image processing capability
- Arbitrary metadata storage and search capability with JSON path query
- Storage capability for large size files through RESTful API with adapters to multiple S3-compliant storage systems
- Support for calls to external APIs, email, MQ, other workflow

APIs enable the permissioned creation and retrieval of files stored in the ECM environment.

In the remainder of this section, we include our response to each of the Attachment F Enterprise Content Management requirements.

ECM02 The Contractor's ECM solution must be able to support all common document types (i.e., Word, PDF, Visio, Excel, PowerPoint, TIFF, and JPEG) and must integrate seamlessly with the most common document viewing and editing tools used by the Department.

The Optum ECM solution supports the upload and storage of common document types, including Word, PDF, Visio, Excel, PowerPoint, TIFF, JPG, and GIF. Retrieval of those documents will enable the user to view and edit them in their native toolsets.

ECM03 The Contractor's ECM solution must allow users to access documents from any platform with all core features available across platforms (desktop, web, mobile). The ECM must allow users to view all documents and images without the use of plug-ins.

The Optum Provider Services solution allows users to access documents through the portal components of the solution. Documents are uploaded and retrieved from the system through APIs between the portals and the ECM solution. The portals support a responsive design philosophy; therefore, the portals can be accessed across platforms and devices.

ECM04 The Contractor's ECM solution must support role-based control and access of documents, as well as including the following:

a. Granular authorizations for access, preview, editing and sharing.

b. Automatic access expirations for documents deemed sensitive by the Department.

c. Content security policy enforcement, such as unusual document access activity and sharing of documents with sensitive information of uploads/downloads of prohibitive data.

The solution is governed by role-based access where you will establish the roles and data access as part of the solution's security implementation. Users are assigned role profiles when the user is established and those role profiles govern the access to information, including documents within the solution. Based on our experience, we will provide you guidance for role profiles and work with you to determine the granularity of application and document access when the role profiles are defined.

ECM05 The Contractor's ECM solution must include a flexible search engine, including document and content search capabilities.

Our solution includes a flexible search engine that uses the document metadata. Document searches are initiated through the portal APIs, which construct the JSON search parameters.

ECM06	The Contractor's ECM solution must allow users to associate metadata with documents.

The ECM associates metadata with each document. Our solution enables searching of the document metadata through a JSON-based search path. Document searches are initiated through the Provider Portal or State Medicaid Agency Portal APIs that construct the JSON search parameters.

ECM07	The Contractor's ECM solution must support simple integration with scanning solutions (support for bulk-scanning).

The solution supports simple integration with scanning solutions and supports bulk scanning. Bulk scanners create files of document images that are placed in an SFTP location. Our solution will then upload those images with the attached metadata and place them in cloud storage. The location of the document and the associated metadata are written to an internal database for use by the document retrieval APIs.

ECM08	The Contractor's ECM solution must support version control.

Our solution supports document version control through the metadata associated with the document. As new versions of documents are uploaded, the version metadata is updated and the location of the latest version is persisted in the storage solution database.

ECM09	The Contractor's ECM solution must be configurable to comply with the Department's document retention policies.

Our solution supports configuration of document retention to comply with the DPHHS' policies.

ECM10	The Contractor's ECM solution must support document workflows with review/approval ability with digital signature support (e.g., scan notifications).

The Optum Provider Services solution manages the creation of documents through the integrated correspondence management functions. Document templates are created in the correspondence management application and use its integrated review and approval workflow for document review/approval. Digital signatures can integrate with those documents at template creation. Document templates that have been fully approved are promoted into the production environment. Documents are then generated from the provider enrollment activities and can be digitally signed at document generation.

ECM11	The Contractor's ECM solution must scan all uploaded documents for viruses prior to storage.

Our solution uses a commercial virus scanner to scan all documents prior to storage. The virus signatures are routinely updated in the virus scanner to keep current with the latest virus signatures identified. Documents failing the virus scan are rejected and the application attempting the upload receives notification of the document rejection.

ECM12	The Contractor's solution shall be able to index, link and display incoming correspondence or uploaded documentation with the entity record.

The access to documents and correspondence stored in our ECM solution is provided through the portal interfaces. These portals communicate with the ECM solution through pre-defined APIs to link documents and correspondence with specific provider records.

ECM13	The Contractor's solution shall send all documentation to the Systems Integration Services module for storage in the centralized ECM.

The solution will integrate with the System Integration Services module so that all documents and correspondence uploaded to our ECM solution are sent to the centralized ECM. The OIL component of the solution will use the mutually defined APIs to send documents and correspondence to the centralized ECM.

ECM14	The Contractor's solution shall have an integrated electronic document management solution to meet the business needs of the State's enterprise.

The Optum Provider Services solution includes a complete electronic document management solution to address the provider management needs of the State. We provide a complete description of the document management solution in our response to Requirement ECM16 on this page.

ECM15	The Contractor's solution shall accept, record, store, and retrieve freeform or HIPAA attachment documents submitted with or in reference to claim submission activity (e.g. operative reports, occupational, physical, and speech therapy reports, durable medical equipment and warranty data, manufacture's tracking data for implants, waivers and demonstration specific requirements).

The solution can accept, record, store, and retrieve freeform or HIPAA attachment documents. Providers can upload documents through the portal in support of claims submission activities. Documents uploaded through the portal will be stored in our ECM through existing APIs. The OIL component of the solution will use mutually defined APIs to send the same documents to the centralized ECM.

ECM16	The Contractor will configure, support and maintain Enterprise Content Management (ECM) functionality (including Document Management and Workflow) to meet the business needs of the State's enterprise.

The ECM component of the Optum Provider Services solution provides federated content management services. ECM is an object storage solution with a simple Web service interface to store and retrieve large numbers of data and image files. ECM includes a collection of technologies for storing, virus scanning, transforming, identifying, sharing, and retrieving files across multiple sources.

In Figure 3.11, we present a high-level view of the ECM architecture.

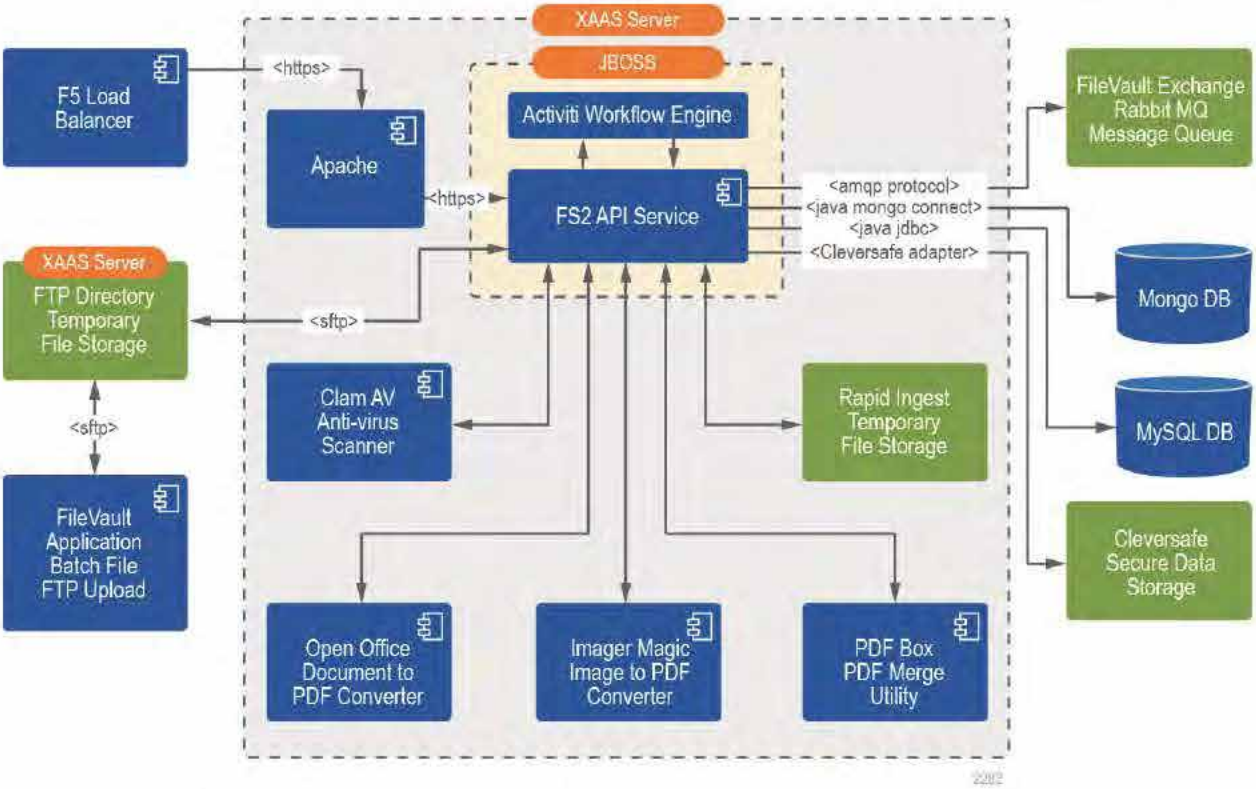


Figure 3.11: ECM Architecture.
The ECM solution delivers simple, scalable, and highly resilient storage services to the Optum Provider Services solution.

Our ECM solution enables the system to upload documents through the API interface or through batch file uploads. The solution uses the APIs to upload documents directly from the portals. Documents added to the ECM are automatically virus-scanned and then stored in our secure data storage. Document upload is done in the background so that the user's portal session is released to perform other work. Document metadata and storage location are updated upon storage of the document. Image documents can convert to PDF for compression purposes.

The user performs document retrieval in the portal through the ECM APIs. The user can retrieve documents linked, through the metadata, to specific providers or enrollment records. After selection for retrieval, the document is retrieved from the storage solution and streamed to the user.

3.10.1.9 Workflow

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

Our solution uses our commercially available, cloud-based BPaaS application for provider network teams to gain visibility to provider activity across all communication channels. This provides transparency of the behaviors, preferences, and key issues of each provider account.

As Figure 3.12 shows, our solution provides a single view of the provider across the organization and drives transparency and alignment across provider touch points.

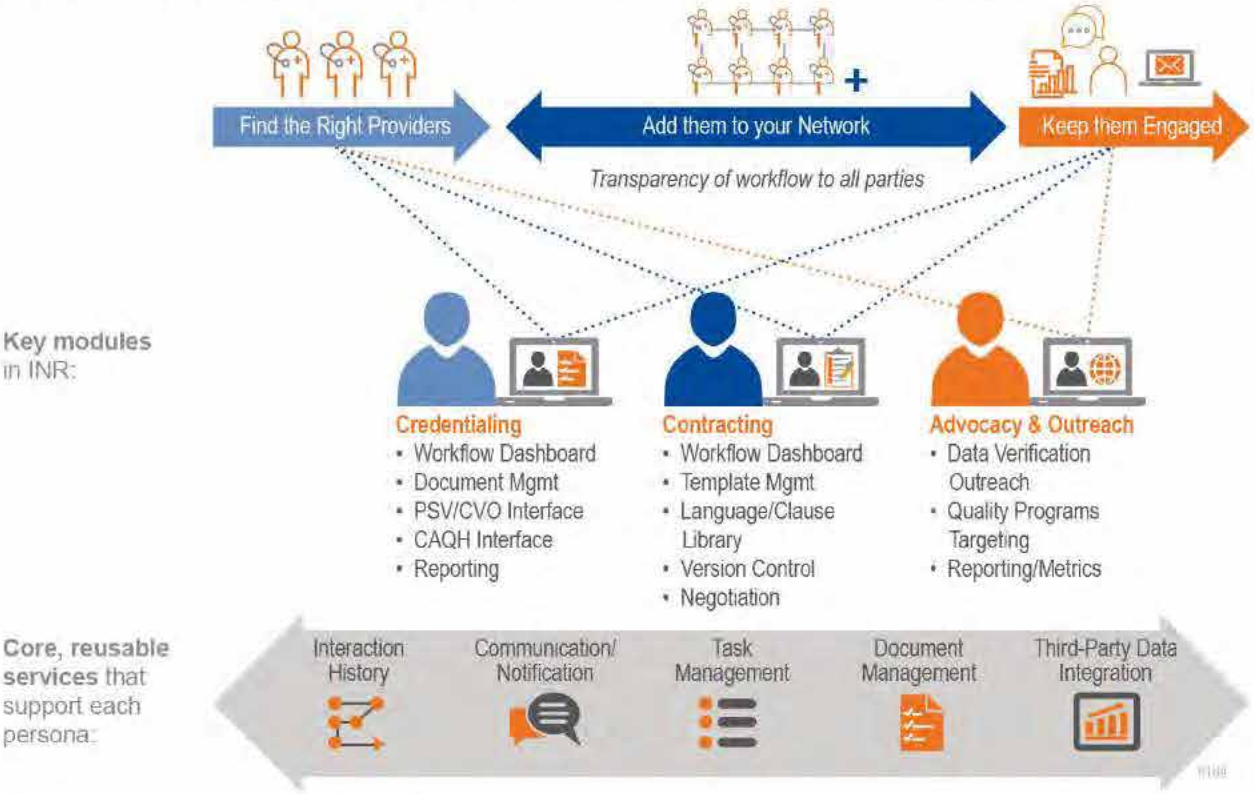


Figure 3.12: Optum Provider Services solution.
Our solution is our workflow tool used to manage, review, validate, enroll, and communicate to the provider community and all submitted provider enrollment applications.

Establishing and maintaining a strong provider network to serve the Medicaid enrollee population in the State is key to achieving the best outcomes and to help members live healthier lives. We can meet this goal by leveraging our provider enrollment solution already proven in commercial engagements. It uses automated workflows and data collection mechanisms to validate the accurate and timely processing of provider enrollment applications. Equally important, our approach offers multiple tiers of support, enabling the provider community to complete this important and mandated function with ease.

Our solution is built on an industry-leading CRM platform. The solution provides powerful pre-defined workflow and reporting tools that enable us to configure our operations to support State-specific provider enrollment requirements. This system will perform mass emails, and we can track outreach campaigns and provider enrollment status and statistics. The system will track provider touch points for historical reporting to meet CMS compliance needs for ongoing provider network outreach. The solution:

- Enables faster time to market in a cloud-based solution with a flexible API architecture
- Features an extensible and scalable platform to meet the DPHHS' needs
- Provides end-to-end visibility and greater transparency
- Enables compliance with evolving regulatory mandates

- Provides integrated validation of licensing, sanctions, and exclusions

In the remainder of this section, we include our response to each of the Attachment F workflow requirements.

WKF01	The Contractor's workflow solution shall provide a runtime engine that facilitates process events throughout the work type lifecycle.

Our solution uses an industry-leading, cloud-based CRM application as the core engine that powers the provider enrollment and re-validation workflow process. The engine processes workflow rules in real-time as data is entered or updated throughout the system. Pre-configured workflows assure that the enrollment process flows seamlessly in response to new provider information, and that appropriate users are alerted to events that can affect the completion of the enrollment and approval process. Final approval of provider enrollments is communicated through the State Medicaid Agency Portal. The solution also automates the creation and distribution of all provider communications necessary as part of the enrollment and re-validation process.

WKF02	The Contractor's workflow solution shall provide configurable work distribution and redistribution based on work type, worker skill, priority, and age of work which can be configured by the State.

The solution includes pre-defined workflows that are configured to optimize the efficient processing of provider enrollment and re-validation activities. The business and workflow rules embedded in our solution automatically route and distribute work to our operational personnel based on the status of the provider application and any missing data.

Provider approvals will route to your agents through the State Medicaid Agency portal for final review and approval/denial. We will work with you to redefine any internal solution workflows to meet your specific business requirements.

WKF03	The Contractor's workflow solution shall provide a user-friendly Graphical User Interface (GUI) for process definition, execution, monitoring, and management. Support a role-based interface for process definition that leads the user through the steps of defining the workflow associated with a business process including processes that are managed by Department staff only, and that captures all the information needed by the workflow engine to execute that process.

We provide our solution as a BPaaS-based delivery model, which automates the provider enrollment and re-validation process. As mentioned previously, a benefit of the BPaaS approach is the delivery of the services required by DPHHS, without the Department having to design and maintain the functionality of the system. Our team makes certain that the overall solution performs business processes in accordance with your requirements. This includes making certain that the business process workflows are configured correctly, and in accordance with your specific requirements. This includes the business processes that are completed by Department staff.

WKF04	The Contractor shall support and assist the Department in mapping all business processes and subprocesses to the workflow application and in transitioning from manual to automated process execution.

We provide our solution as a BPaaS-based delivery model, which automates the provider enrollment and re-validation process. We will work with you to map the business processes and sub-processes into the workflow component of the application. This activity supports the transition of business processes from manual to automated processes.

WKF05	The Contractor's workflow solution shall support work-type processing that includes internal and external dependencies.

We provide our solution as a BPaaS-based delivery model, which automates the provider enrollment and re-validation process. We will work with you to determine if our internal

processes need to incorporate any external dependencies and will modify the internal workflows (under your guidance and with your testing approval) to support those dependencies.

WKF06 The Contractor's workflow solution shall provide the ability to view alerts and/or reminders by user, by work-type.

Our solution communicates the status of the provider application as well as any alerts to your staff through the State Medicaid Agency Portal. Your staff will make the final determination if a provider is approved or denied as a valid provider in the State's Medicaid network. Communication of final status is automated to the provider through our solution.

WKF07 The Contractor's workflow solution shall provide the ability to set alerts and or reminders by user, by work-type.

Our solution communicates the status of the provider application as well as any alerts to your staff through the State Medicaid Agency Portal. Your staff will make the final determination if a provider is approved or denied as a valid provider in the State's Medicaid network. Communication of final status is automated to the provider through our solution.

WKF08 The Contractor's workflow solution shall automatically set the state of the work item, based on the processing steps when completed to provide transparent, accurate status of the work at all times.

Our solution sets the status of all applications as pending until final approval or denial is received from your staff through the State Medicaid Agency Portal. Your users can use the portal to inquire as to the status of applications on any provider. Likewise, a provider can inquire on the status of the application through the Provider Enrollment Portal.

WKF09 The Contractor's workflow solution shall provide supervisors access and control of work by type and by user.

The workflow dashboard that is internal to our solution enables our internal users and supervisors to monitor and control the flow of work within the solution. Supervisors can reassign work to meet specific business requirements or processing deadlines, as needed.

WKF11 The workflow engine shall be configured to support capturing business processes using Business Process Model and Notation (BPMN) 2.0 or later, even if the engine uses a separate coding of the rules for execution.

Our solution uses an industry-leading, cloud-based CRM application as the core workflow engine of the provider enrollment and re-validation process. The workflow in the COTS application we use is pre-configured to optimize the provider enrollment and re-application process. The workflow engine uses a graphically oriented guided rule builder to document and deploy workflow rules and business processes.

WKF12 The workflow engine shall be configured to support the establishment of work queues allowing in-process knowledge, data, and documentation to flow from one-solution to another solution.

Our solution uses an industry-leading, cloud-based CRM application as the core workflow engine of the provider enrollment and re-validation process. The workflow in the COTS application is pre-configured to optimize the provider enrollment and re-application process. Our solution has pre-configured work queues that our staff uses to manage and monitor work. Data within our solution is seamlessly passed within our solution. Application status is communicated to the State Medicaid Agency Portal through a set of pre-defined APIs.

WKF13 The workflow engine shall be configured to support workflow access, assignments, and execution for all essential aspects of the business processes (e.g., provider enrollment, provider screening, client communications).

We provide our solution as a BPaaS-based delivery model, which automates the provider enrollment and re-validation process. We configure the workflow engine components to support workflow activities that support all critical business processes. This includes provider enrollment,

provider screening and communications. Our approach is to deliver the specific provider services required by DPHHS in a services model, where our experienced team configures the technology solution to meet your needs.

WKF16 The Contractor's solution shall deliver automated business process/workflow management to support the establishment of work queues via an assigned worker portal allowing in-process knowledge, data, and documentation to route from one worker's queue to another as well as across solutions. The Contractor's solution shall ensure compliance with defined processes.

Our solution uses an industry-leading, cloud-based CRM application as the core workflow engine of the provider enrollment and re-validation process. The workflow in the COTS application we use is pre-configured to optimize the provider enrollment and re-application process. Our solution has pre-configured work queues that our staff uses to manage and monitor work. Data within our solution is seamlessly passed within our solution. Application status is communicated to the State Medicaid Agency portal through a set of pre-defined APIs.

WKF17 The Contractor shall configure, support and maintain a configurable document management and workflow solution that meets the State's requirements.

Our solution is configured to manage and automate the communications to providers through our solution and the accompanying Correspondence Management and ECM solutions. The combination of these applications enables our solution to generate, track, monitor, and support the distribution and retention of correspondence and documentation associated with the provider enrollment and re-validation functions.

WKF18 The Contractor shall have configurable workflow processes to support auto notifications to providers for specific events (e.g., license expiration, revalidation).

Providers will access our solution through the Provider Portal. Providers can inquire on the current status of their application. They will also be alerted to any additional information or documentation required to complete the application and re-validation process. In addition, providers can receive notification of upcoming re-validation events so that they can provide the required documentation before the event deadlines.

WKF19 The Contractor shall provide links to screening and monitoring databases in the workflow tool if the data isn't available via an automated interface.

Our solution automates the interface between the workflow engine and the commercial and governmental screening and monitoring databases.

WKF20 The Contractor's solution shall have configurable workflow to present for validation, updates submitted online/electronically by specific criteria (e.g., program type, data type, risk level).

Our solution uses a pre-defined workflow for the provider enrollment and re-validation process. Regardless of how the provider application is submitted, all applications and re-validations follow the same workflows to make sure no steps are skipped during the application and re-validation process.

3.10.1.10 Correspondence Management

This section addresses Correspondence Management requirements for the Contractor's solution(s) and operations. The Contractor's correspondence engine shall be configured to generate enterprise correspondence and coordinate the print and distribution through a State approved print and mail service. The Contractor must describe the proposed solution's capacity to configure, support and maintain correspondence management functionality (i.e., add, modify, or remove correspondence) and the type of resource and necessary skill set(s) required for correspondence management functions. Describe the change management processes associated with correspondence management. In addition, the Offeror must describe their approach to meet each of the Correspondence Management requirements detailed in Attachment F, Requirements Matrix.

The Optum Provider Services solution includes an integrated correspondence generation solution that provides industry-leading capabilities to create, manage, deliver, and track correspondence to your stakeholders. The correspondence solution consists of three core components: the authoring environment, the user interface, and the delivery engine. These core components allow us to configure, test, and rapidly deploy letters to our solution, and to make updates to letter templates in support of changing business requirements.

Authoring Environment

The correspondence authoring tool enables the author to create correspondence templates. Templates are generic formats to support one-to-many letters. The template defines the variations of the letter and defines the placement of fixed text, as well as variables inserted from the source systems. For example, a template could be created to describe the provider application status and variations of the master template defined to support multiple languages. Data variables can be queried and inserted from the source system or can be defined as graphic content, or as common text elements (e.g., logos). Variables support date sensitivity so that future text changes can be pre-defined and pulled into letters at the appropriate time according to the active date of the variable.

Templates can be defined to create collections of letters, that is, a single template can generate multiple letters. Collections are typically used to communicate status of applications to many different recipients in different formats. For example, the application approval notice may need to be sent to the provider and other State agencies, and these letters have different content. A user or system needs to only request generation of the template for the entire collection of letters to produce automatically.

The authoring environment also defines the queries so that data can be extracted from the various source systems. Queries are saved and re-used across multiple templates so that as queries are updated, they are automatically updated in each template. Queries support either direct database access through ODBC or JDBC, or can be based on an extracted XML document.

The authoring environment supports a structured testing, review, and approval process. Templates proceed through the testing, review, and approval process and authorized administrators promote the templates into the production environment.

End User Interface

The end user interface is a Web-based interface where the end user can request generation of a letter. If letters require the end user to enter additional text (e.g., explanations of a provider's application denial), the end user interface supports an integrated approval workflow so that supervisory or other management personnel can approve the letter and text prior to letter delivery. The Web-based interface allows end users to create on-demand letters. The interface parameters can also be called from an API so that applications can automatically generate letters for delivery.

Delivery Engine

The correspondence generator composition and delivery engine combines the template data and the letter data at composition and run-time. Delivery methods include paper (mail), fax, email (HTML) and text (SMS). The template defines the delivery methods. In the case of a collection, each template can have a separate delivery method. The delivery engine can also automatically generate a PDF copy of any correspondence, as well as an XML file of the data extracted and used for each letter produced. The solution will generate the PDF of each letter and will deliver the PDF to the ECM component, as well as deliver a copy to the DPHHS Integration Layer for storage in the centralized ECM.

Letters can be batched, ZIP code barcoded, and sorted by ZIP code for fulfillment. This saves on postage costs. Letter batches can be released for print at frequencies mutually defined between you and us.

In the following content, we provide our responses to the RFP requirements applicable to Correspondence Management as identified in Attachment F, Requirements Matrix.

COR01 The Correspondence Management Solution must be able to generate correspondence (e.g., scheduled and ad-hoc correspondence and bulletins) using standard letters or forms, letter templates, and free-form letters.

The Correspondence Management solution will generate both scheduled and ad hoc correspondence using standard templates and free-form letters, as described above. Users and applications can both generate scheduled and ad hoc letters. The Correspondence Management solution maximizes the automation of letter generation and minimizes manual intervention. This leads to fewer inaccuracies, misdirected letters, and reduced labor usage.

COR02 The Contractor shall configure, support and maintain a correspondence engine to generate correspondence and coordinate the print and distribution through a State approved print and mail service.

The correspondence generated through the solution will send PDF files of the correspondence to the DPHHS Integration Layer. The DPHHS integration layer will send the PDF files to the State-approved print and mail service.

COR03 The Contractor's solution shall utilize industry standard barcode technology that is approved by the Department.

The correspondence solution supports multiple industry-standard barcodes as standard output elements, including the following:

- Aztec, Codabar, Code11, Code128, Code39, Code39ext, Code93 Code93ext, Databarextended, Databarlimited, EAN8, EAN13, EAN14, IATA2of5, Interleaved25, ISBN, ISMN, Matrix2of5, Maxicode, MSI, Onecode, OPC, PDF417, Pharmacode, Postnet, QRCode, SSCC18, Standard2of5, UCC128, UPCA, UPCE, VIN
- United States, Canadian, Australian, German, Italian, Singaporean, Swiss postal barcodes

COR04 The Contractor shall utilize letter, notification and other templates for correspondence that are approved by the Department.

The authoring environment of the correspondence generator is expressly designed to create correspondence templates that we will route for review and approval by DPHHS before final testing and deployment. New letter templates and changes to letter templates are prohibited from deployment to production until we obtain approval from DPHHS.

COR06 The Contractor's solution shall send documents and the necessary indexing metadata to the modular integration platform for storage of documents in the enterprise content management solution (ECM).

The solution will send the PDF files for generated correspondence, as well as the associated metadata to the modular integration platform for ingestion by the State's enterprise content management system.

COR07 The Contractor's solution shall store all sent or received documents in the ECM.

The solution will send all sent or received documents to both our enterprise content management system and the State's centralized content management system. The OIL component of the solution will communicate with the State's Integration Service to transmit or stream documents to the State's enterprise content management system. Metadata will be sent, along with the documents, to the respective enterprise content management systems.

COR08 The Contractor's Correspondence Management Solution must be able to integrate variable data to maximize efficiency.

A key differentiator of the correspondence management component of our solution is the ability to incorporate variable data as part of letter templates and template collections. Variable data can be extracted directly from source systems using an ODBC or JDBC driver or through an XML document. Variable data can be extracted from source systems, or variable data can be defined as specific content as logos, pre-defined text and paragraphs, and graphics.

COR10 The Contractor shall generate applicable notices to members, providers, and other entities (e.g., enrollment/disenrollment notices, requests for information, and program information).

The solution will support the creation of templates and the generation of the applicable notices to providers and other entities. The notification templates will be subject to approval by DPHHS.

COR12 The Contractor's solution shall produce notices to applicants of the approval, rejection, and pending status of their provider enrollment.

The solution will support the creation of notices to providers and other entities of the approval, rejection, and pending status of their enrollment. The notification templates will be subject to approval by DPHHS.

COR13 The Contractor's solution shall provide the ability to create materials at between a sixth and eighth grade reading level and for a culturally diverse population.

The letter and notification templates created in the solution will support the culture, language, and reading level requirements as defined by DPHHS. All letter and notification templates will be subject to approval by DPHHS.

COR15 The Contractor's solution shall support official approval and denial notifications to the provider. The notification will support consolidated communication for multiple taxonomies in the case of split approval and denial of provider enrollment service determinations.

The official approval and denial letter and notification templates created in the solution will support consolidated communication for multiple taxonomies in the case of split approval and denial of provider enrollment service determinations. All letter and notification templates will be subject to approval by DPHHS.

3.10.2 Project Management and System Development Requirements

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

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

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

Our proposed systematic, mature, and measureable project management methodology is based on industry standard methodology—the Project Management Institute (PMI) PMBOK Guide and the Carnegie Mellon SEI principles described in the CMMI framework. Optum also adheres to ANSI and ITIL standards, where applicable. We will use our Optum Delivery Model and our SDLC to govern each stage of the project beginning with DDI.

Best Practices

- Follows proven industry standards (i.e., PMBOK)
- Incorporates and ins itutionalizes these standards throughout the other project processes
- Provides situational awareness of schedule, performance and cost status for project reporting and decision-making
- Includes tools and processes hat provide transparent views into relevant schedule, performance, and cost data
- Allows enterprise visibility for consistent control of project performance

We will jointly establish a unified governance structure with you and apply our integrated project management framework to your program. As your trusted partner, we will focus on the components that make up your program and develop milestones that meet the objectives and established deadlines. Optum has extensive experience in effective program and project management using PMI-aligned methodologies and processes in engagements with 47 state clients and the District of Columbia. Our program and project management framework features a comprehensive approach to strategy alignment, process optimization, quality assurance and managing contract performance. We use formal procedures modeled after internationally recognized standards. Our on-site management team will develop approved performance management measures to maintain visibility into the status and health of the project. We structured our overall program and project management approach and methodology to best meet the needs of the Provider Services module as defined by the RFP.

Project Management Methodology

Our project management for the project will be a joint effort between the following parties:

- DPHHS
- MPATH Stakeholder Committee
- MPATH Program Management Office
- The awarded MPATH System Integrator vendor
- Current MMIS vendor
- IV&V contractor

Together, these parties will agree upon in-scope deliverables and deliver services that meet or exceed contract requirements. We understand consistency and organization in the migration of your platform is a key business driver. We will use proven project management principles, including all activities required for appropriate management, monitoring, documentation, traceability, and communication. This methodology promotes the best use of your resources and reduces redundancy as the teams work toward a common goal and milestones.

This section describes how we will partner with you to apply our methodology to complete all the project phases within the Communication Plan and Delivery Model sub-sections.

Optum PMO for the Optum Provider Services Solution

Our PMO will integrate with the MPATH PMO for governance, managing the implementation effort, finance and contract management, change management and the overall project management methodology, policies, and procedures as applied to the Provider Services module. Our PMO is not an additional layer of management, but part of the operational team that promotes better overall communication within the project. Dedicated resources include our:

- Project manager
- Contract manager
- Testing lead
- Integration lead
- Certification lead
- Business operations manager
- Technical manager

This team will support the technical and functional teams as they execute their responsibilities. We will make sure the project team adheres to the established project standards, policies, and procedures. The team will also serve as a central collection point for project status, metrics, and for overall project status reporting. Figure 3.13 shows the planning, tracking, and administrative activities of the Optum PMO team.

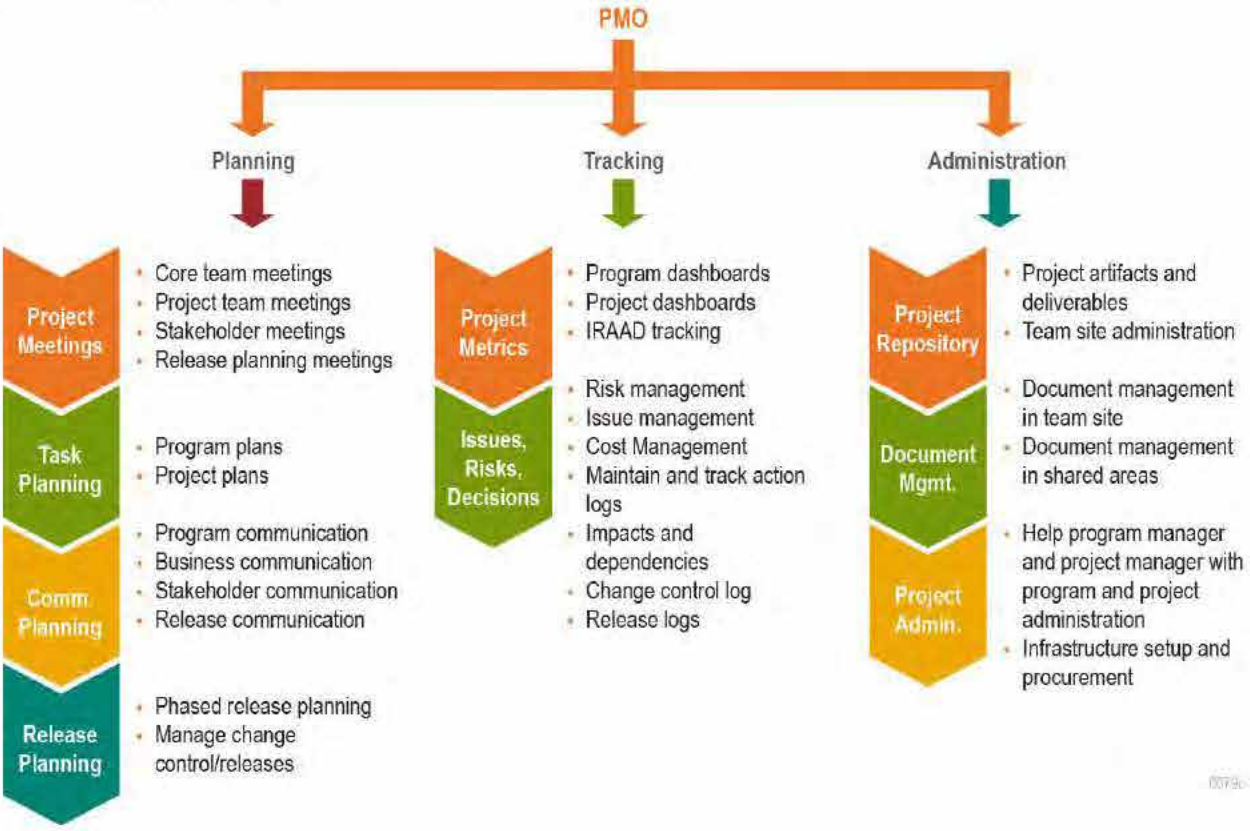


Figure 3.13: Optum PMO Team and Administrative Activities.
The Optum PMO team will support, monitor, and manage the Provider Services module.

An awareness of your business objectives, business pain points, and your project goals will improve team efficiency. All staff members on the PMO team will receive training on the processes and procedures established for the Provider Services module. During all project phases, we will work collaboratively with DPHHS. We will align existing processes and procedures to achieve successful delivery.

Integrated Project Management and Governance for the Provider Services module

Our methodology and approach interacts effectively with the overarching project plan, developed to align with industry project management standards, to work cooperatively and integrate with the Provider Services module management team. We use the same methodology with our partners to align the entire Provider Services module portfolio. We will partner with you to mutually agree on and adhere to the integrated project management framework for the Provider Services module.

Communication Plan

Optum will develop a Communication Plan that will guide project communications. Early in the project, we will meet with you to determine project communications requirements and incorporate your feedback in the Communication Plan. This will include project status reporting, monitoring activities and the processes required to support appropriate planning, collection, creation, distribution, storage, retrieval, management, control, and monitoring of all project activities. Figure 3.14 shows a sample Communication Plan table of contents.

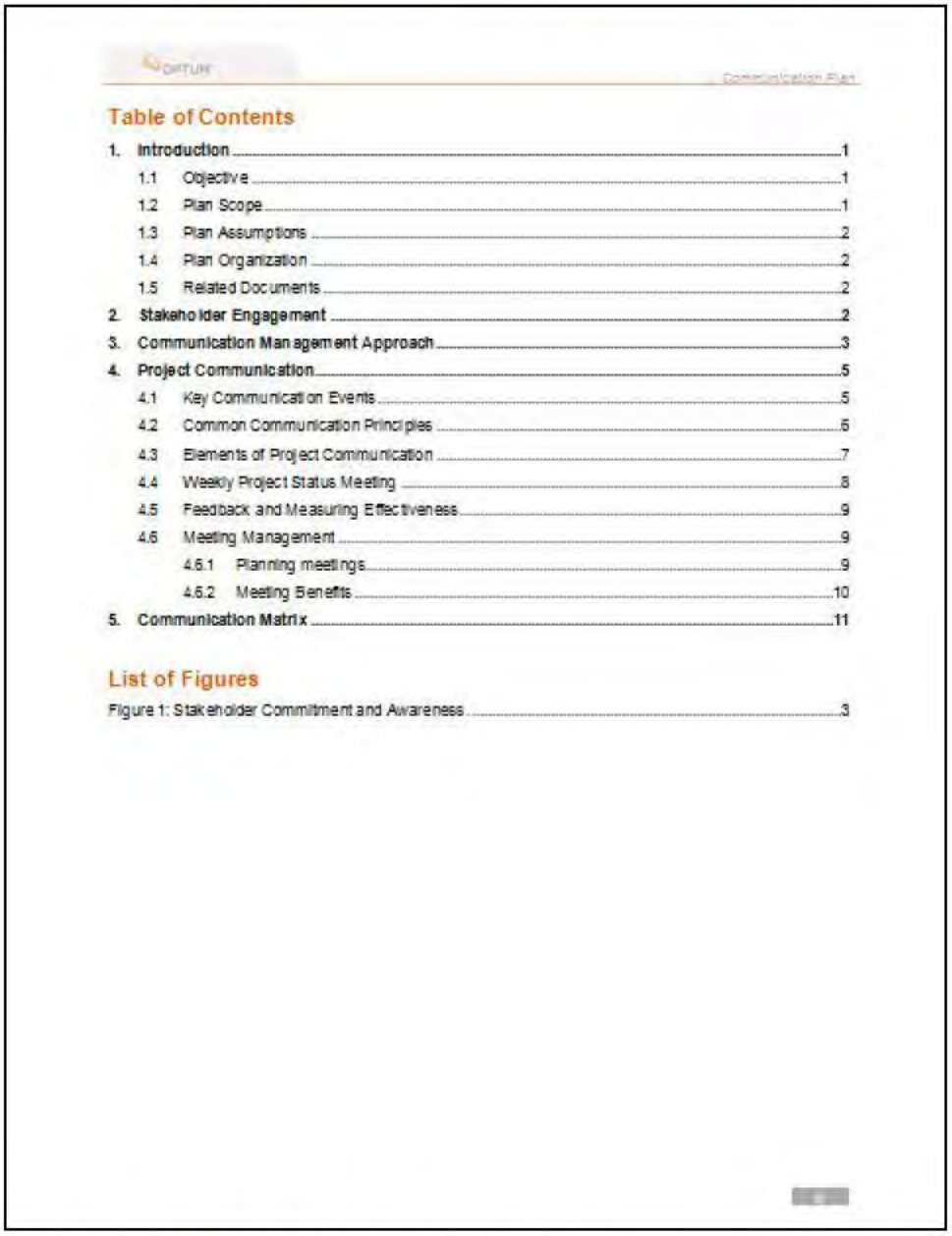


Table of Contents

1. Introduction 1
1.1 Objective 1
1.2 Plan Scope 1
1.3 Plan Assumptions 2
1.4 Plan Organization 2
1.5 Related Documents 2
2. Stakeholder Engagement 2
3. Communication Management Approach 3
4. Project Communication 5
4.1 Key Communication Events 5
4.2 Common Communication Principles 6
4.3 Elements of Project Communication 7
4.4 Weekly Project Status Meeting 8
4.5 Feedback and Measuring Effectiveness 9
4.6 Meeting Management 9
4.6.1 Planning meetings 9
4.6.2 Meeting Benefits 10
5. Communication Matrix 11

List of Figures

Figure 1: Stakeholder Commitment and Awareness 3

Figure 3.14: Sample Communication Plan Table of Contents Activities.

The Communication Plan will guide our communications with DPHHS, the IV&V vendor, and other vendors and stakeholders for the Provider Services module.

As you have stated in your RFP, your team seeks a collaboration that aligns all stakeholders supporting your program and that communication is an area where you would like to see improvement. Our organized, open, and transparent approach will enable our teams to quickly grasp, mitigate, and respond to potential issues. In the rapidly evolving HHS environment, systems and organizations must align closely to provide quick and reliable support. The Communication Plan will align with DPHHS requirements and address those requirements during DDI, maintenance and operations, and enhancement and modernization. We are flexible and can suggest various approaches that have proven successful with other clients.

For example, the Commonwealth of Massachusetts required an approach that supports their client's broad set of stakeholders and decision-makers. In this case, Optum employed a model that included committees to engage different levels of leadership to prioritize strategic and tactical communications so all stakeholders received timely, clear, and appropriate information. We provided weekly status reports, daily status meetings, release-specific status meetings, and facilitated weekly executive steering committee meetings.

In another example, the State of Vermont required a more flexible model for a consolidated set of leaders with broad accountability like the State of Montana. This model employed weekly status reports, weekly status and prioritization meetings, as well as on-demand reporting and real-time dialogue to support the State's time-sensitive business needs.

We propose a streamlined and flexible governance model that enables us to coordinate and adjust to changes in an organized manner, and respond effectively and transparently. Figure 3.15 shows our proposed Integrated Project Management and Governance Model, which enables effective collaboration with DPHHS, the Optum Provider Services team, the management team, vendors, and other stakeholders.

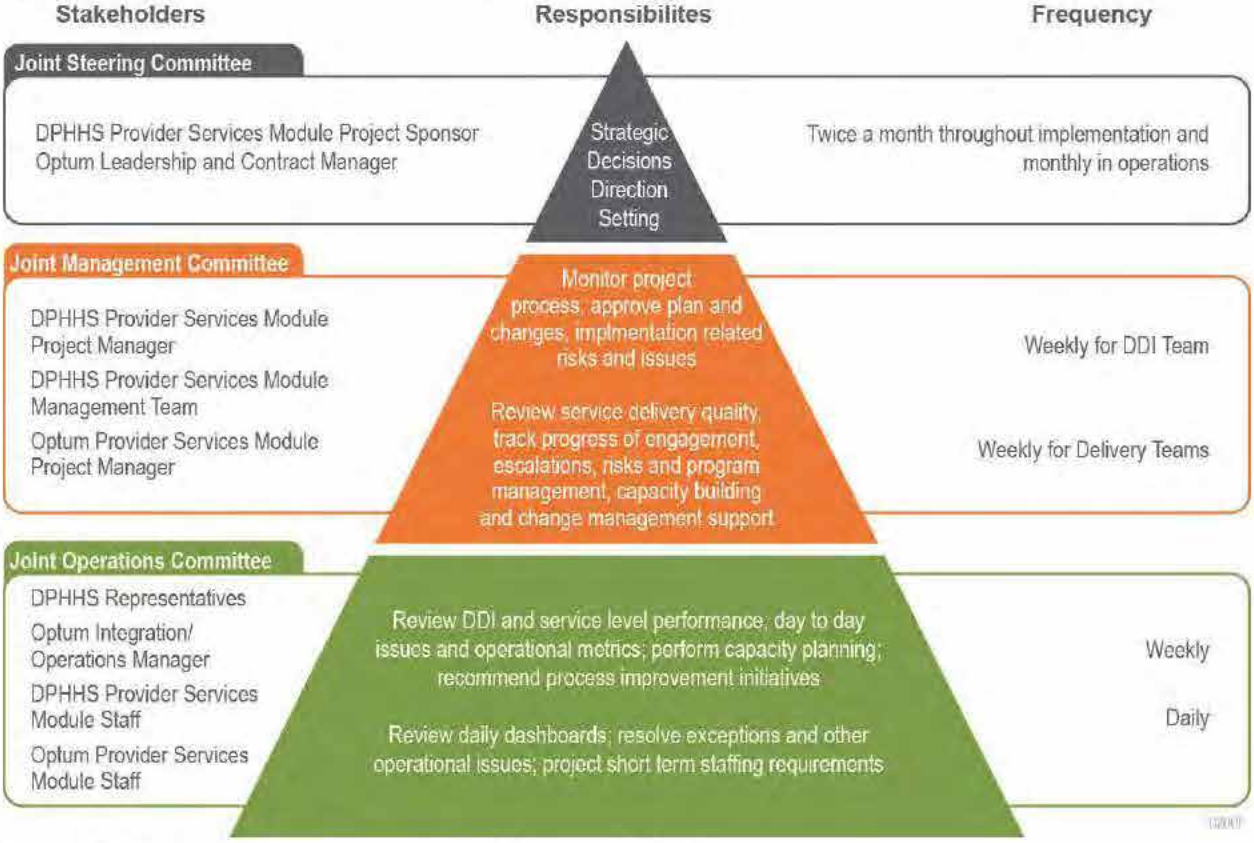


Figure 3.15: Integrated Project Management and Governance Model.
Our proposed governance model enables us to coordinate and adjust to changes in an organized and thoughtful manner, and to respond effectively and transparently.

Our three-tier communication model includes a Joint Steering Committee, a Joint Management Committee and a Joint Operations Committee. These committees will function as follows:

- The **Joint Steering Committee** will include representatives from DPHHS and Optum executive leadership and provide strategic guidance and decisions.

- The **Joint Management Committee** will include senior delivery leaders, such as the DPHHS project manager, Optum on-site project manager, and the Provider Services module Management team. This committee will review the overall health of the engagement.
- The **Joint Operations Committee** will include operating teams from the DPHHS, the Optum, Provider Services team, the management team, vendors, and other stakeholders. This committee will manage day-to-day operations.

Using our proven successful approach, your communication model will facilitate joint opportunities for periodic review of the production status of all work areas; setting priorities and goals; transparency, control, and visibility into operations; and review of plans for issue resolution. We can easily modify this model to meet your needs for the Provider Services module. We will work as partners to manage the relationship and expectations by accomplishing the following:

- Enabling strategic alignment to your business goals
- Allocating resources to meet business requirements
- Reviewing our approach to new tasks and establishing clear roles and responsibilities for decision-making, issue resolution, and service delivery
- Meeting schedules and contractual obligations through SLAs
- Continuously evaluating performance, user satisfaction, and effectiveness
- Providing regular and frequent communication across all DPHHS stakeholders

We will work with you to define a communication approach that provides regular and frequent communication with DPHHS and is flexible to make changes as we seek to continuously improve and adjust to changing needs and requirements. Weekly meetings will provide a status update and plan of the week's activities. DPHHS and Optum will collaborate in regularly scheduled, formal status meetings that will provide a status of activities.

Appropriate DPHHS leadership and our Optum project manager will hold scheduled meetings to discuss overall project activities and the status of tasks in progress. Our project team will enable transparent governance and flexible partnership. The Optum account manager will facilitate ongoing communications between DPHHS contacts and the Optum team.

We will use the project health criteria and definitions detailed in the RFP (i.e., red, yellow, green), as well as DPHHS-standard health measures, to manage the project through closeout, as Figure 3.16 illustrates.



Figure 3.16: Project Health Status.
Our weekly and monthly project status reports will include a dashboard of project health at various levels.

Our issue escalation process includes defined lines of communication, roles, and responsibilities, and span-of-control parameters. Our issue escalation procedures defined in the Issue Management Plan will define when and how to escalate the issue to the next level. When necessary, we will involve DPHHS and our executive management to expedite the resolution of mission-critical issues. Optum will partner with the DPHHS to develop the escalation process. We will invoke this process when conditions and severity of the issue warrant escalation. Figure 3.17 shows our proposed issue escalation process.

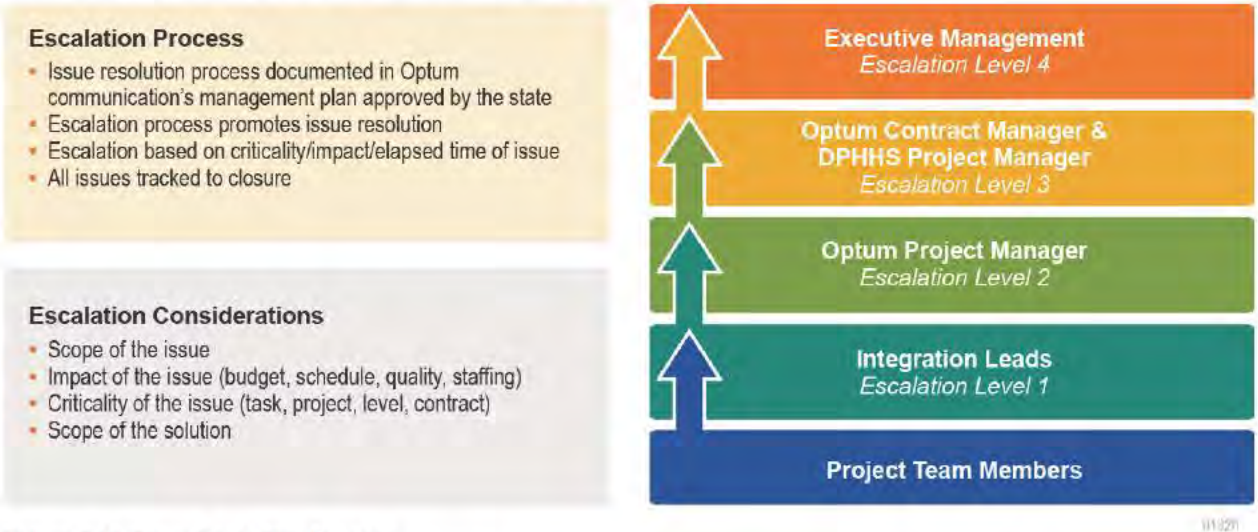


Figure 3.17: Issue Escalation Process.
Our issue management approach mandates timely communication and proactive monitoring until each issue is resolved.

Optum Delivery Model

Our strategy for achieving effective project management and completing your scope of work is to drive our work using a model that we have proven successful over more than 20 years of large-scale commercial and HHS projects. We will implement our best practices-based Optum Delivery Model, which we developed by integrating the PMBOK and Scaled Agile Framework (SAFe) principles. Our project management methodology adheres to the PMI project management standards and is applicable throughout the contract term. The Optum Delivery Model combines our innovative SDLC with a standards-based project management methodology.

Our delivery model provides a disciplined system development methodology, the OSAM, and structure for managing project activities and assessing status. It will facilitate communications for managing project activities, assessing status, and communicating with other contractors, DPHHS management and staff.

The Optum Delivery Model:

- Follows the strategy of early delivery of high quality services while gradually building the features and value provided to users. DPHHS users will gain access to the information and features they need as they become available, rather than waiting for an all-or-nothing delivery in a single release.
- Uses an iterative development model to shorten development cycles and provide opportunities for early stakeholder feedback, in this manner delivering value quickly and frequently to users.
- Uses Agile practices that reduce waste by following a continuous improvement cycle for development. We implement discrete, collaborative gate reviews for each release with specific criteria required before the release is promoted or moves into the next phase.
- Is based on collaboration to reduce and eliminate communication barriers.

The Optum Delivery Model includes an integrated set of project management disciplines adapted to meet your project requirements during DDI and ongoing operations, as Figure 3.18 shows.

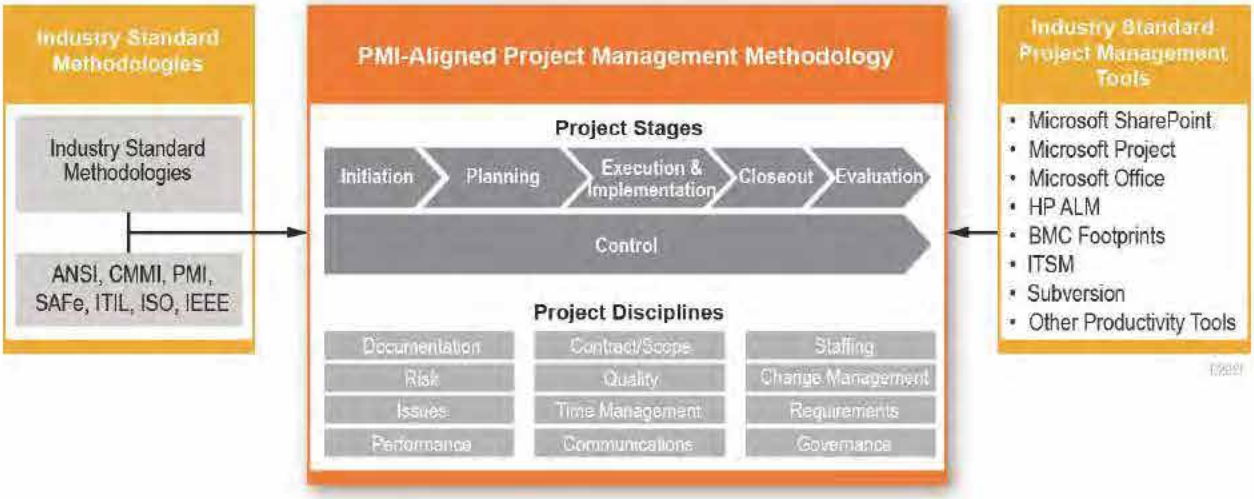


Figure 3.18: Optum Delivery Model.
Our delivery model aligns with PMI, SAFe, and other DPHHS and industry standards to provide integrated management across all project phases.

Our delivery model includes an integrated set of project management disciplines that we adapted to meet or exceed your contract requirements. Our management team will coordinate with the DPHHS project manager to adapt our program and project management processes and procedures to align with yours. We will work with you to develop approved performance management measures that will give you visibility into the status and health of the project throughout the project lifecycle. Industry standard methodologies and tools are also important inputs into the Optum Delivery Model.

A central tenet of our project management strategy is to use industry standard methodologies and tools to drive quality, speed of delivery, and provide transparency for DPHHS. We use a suite of industry-leading tools to support our delivery model. At the same time, our COTS-based, SaaS solution enables quicker configuration and streamlined integration. Our solution, combined with our experienced, talented team, and our proven delivery model, will reduce project risk and facilitate project control for DPHHS.

Our Optum Delivery Model will govern each stage of the project, beginning with DDI. We describe each stage of our PMI-aligned project management methodology (shown in the center section of Figure 3.18) in more detail in the following narrative.

Initiation

As we begin the project, we will work with you and identified stakeholders to clarify the objectives; understand deliverables; set milestones and schedules for project deliverables and phases; confirm roles and responsibilities; establish clear lines of accountability; and implement a framework for effective project management and control. We will schedule a kick-off meeting and initial working session with you, other appropriate project stakeholders, and members of our team. The goal of the kick-off is to introduce the solution and give you and other project stakeholders an understanding of our approach to implementing it. We will review the scope of work that we will undertake for the project and confirm project goals and objectives. In addition, we will highlight participant roles and responsibilities so that attendees will know what to expect during the project.

Likewise, our team will spend time confirming our understanding of what role the solution will play in the overall Medicaid enterprise environment. Additionally, we will work with you to review and help you refine your enterprise IT strategy to drive the implementation (and later operations) of the solution. We will demonstrate our approach to meeting the CMS Seven Conditions and Standards so that you can receive enhanced Federal Financial Participation (FFP) for our proposed solution.

Planning

To guide the project, we will create a comprehensive project management plan (PMP) and project work plan (PWP). We discuss the PMP and the PWP in the project management section that follows.

Execution and Implementation

During this phase, we will deploy new capabilities to production, validate completion of required activities, and confirm your acceptance of deliverables.

Our SDLC is integrated with compliance and security components throughout each phase of the system development starting with validation of functional and non-functional requirements. We have matured these processes over the last 20 years while successfully delivering large-scale HHS solutions and provider services. Our approach is based on the well-established and adaptable system development methodology that you seek. It leverages the best practices that we have field tested in our previous implementations to deliver a best value solution for you.

We will design, develop, test, and implement each release according to your requirements, using our Optum Delivery Model. The Optum Delivery Model is an iterative methodology that provides users frequent touch points with our developers during design preview sessions and other collaborative forums. We incorporate these sessions throughout the design, build, and test process as often as necessary for components that benefit from frequent client input, such as metadata model design and report design.

Through design previews, your stakeholders will view a live, working version of the portal and user interface. We will work with you to preview the solution, gather your feedback, update configurations tailored to your needs and then review the updates with you. We will continue this iterative process until we reach agreement that the solution meets your requirements. Figure 3.19 illustrates the design preview process.



Figure 3.19: Design Preview Process.
The design preview process allows iterative design and development based on your feedback.

Design preview meetings help acquaint future users to the system they will use. The meetings also help confirm that we deliver the solution that meets your requirements because you have seen it updated with your specific configurations.

For example, if we are working on the Provider Portal supporting applications and screening, we will have sessions with the business analyst groups after we provide the initial workflows and business rules. We will then adjust the workflows and rules based on the input from the sessions.

These sessions can iterate a number of times depending on the complexity of the subject area. They help confirm that everyone is on the same page regarding workflows, business rules, data models, or reports. We do not use design preview sessions for all components of the solution. Some components, such as programming ETL interfaces, do not typically lend themselves to this technique.

We find that our iterative methodology reduces surprises and increases client satisfaction. We operate these iterative development sessions in the context of stage gate approvals by you. This method provides you with confirmation that the software is working to specifications and the project has been planned appropriately. It also provides confirmation that the software delivered actually meets users' needs, which is difficult to gather under a pure waterfall methodology. This approach enables rapid deployment and flexible Agile processes embedded into the stages where they provide the greatest advantage—Design, Build and Test. Figure 3.20 illustrates this iterative development and delivery process.



Figure 3.20: Iterative Development and Delivery.
The Optum implementation methodology incorporates Agile principles into the waterfall SDLC framework to deliver high quality software quickly.

Control

We continuously monitor and control the progress of all project phases and releases. Our delivery model and tools will enable us to produce metrics, schedules, and deliverables to show that we continuously perform to SLA expectations. We incorporate quality control and auditing into our successful, verifiable approach to monitoring and controlling performance. Our risk, issue, and quality management plans result in generating quality artifacts to demonstrate project performance. The Optum PMO will update the project plan and work plan schedules weekly to reflect current project status.

As part of project control activities, the Optum Provider Services solution team will prepare and provide weekly and monthly status reports and briefings to you. Both the weekly and monthly status reports will include a dashboard of project health at various levels.

Closeout and Evaluation

After the implementation of our solution successfully completes, we close out implementation activities and progress into ongoing operations and maintenance. Additionally, we conduct an after-action review with you to evaluate what we did well and where our challenges lay. The results of this review are documented and added to our repository of lessons learned, enabling us to address any identified issues for the next project.

Successful Approach to SDLC Management

Optum has a documented record of success delivering and remediating large, high-visibility, HHS technology projects like the Provider Services module.

Our iterative development and delivery approach has provided previous clients with the following advantages:

- Shorter development cycles
- Early stakeholder feedback opportunities
- Exposing flaws faster and reducing re-work by following a continuous improvement cycle for development

Proven Success

- Recognized leader in enterprise data integration, enabling states to achieve integrated HHS service delivery
- Served as CMS's general contractor to remediate challenges experienced with initial roll-out of HealthCare.gov
- Performed stabilization, development, and maintenance for five state eligibility systems

A good example is the support we provided to the federal government and CMS in overseeing the stabilization and implementation of HealthCare.gov. We led a collaborative, badge-less team across multiple IT vendors to bring the site back up to performance, enabling millions of people to enroll in health coverage by the end of that first enrollment period.

Before contracting with Optum, the HealthCare.gov project lacked strict software development and quality assurance processes, resulting in defective code and missed timelines. CMS also needed a reporting system to monitor and manage all business requirement alignment with CMS policies, which we provided.

Our success supporting CMS led to multiple states requesting our help to fix their challenged exchange, eligibility, and enrollment projects. We ultimately performed stabilization, development and maintenance for eligibility systems in Massachusetts, Vermont, Maryland, West Virginia, and the District of Columbia.

- For Massachusetts, Vermont, Maryland, and West Virginia, we completed a smooth takeover of the eligibility system from the prior vendor in less than two months.
- In Massachusetts, we completely replaced the Commonwealth's failed eligibility solution in a six-month period, which was an unprecedented accomplishment.
- In Michigan, we provide an enterprise data warehouse with supporting data from 40 state agencies, requiring detailed coordination.

Our Approach to Multi-Vendor Collaboration

In a multi-vendor, multi-contract environment like MPATH, a close partnership with DPHHS and your other contractors will be crucial for meeting program objectives for delivery of the Optum Provider Services solution and other replacement MMIS modules. Active collaboration and communication will enable us to meet the challenges of the project within the context of the overall multi-vendor enterprise environment. MPATH represents a large, complex initiative with multiple components, each with its own set of goals and objectives. In addition to the unique requirements and objectives of this project, in your RFP, you outline a clear, unified vision for the overall modernization project. Using this vision as our guide, we will collaborate with your Systems Integration Services contractor and your other vendors to incrementally build the MPATH modules and components to achieve your common objectives for the Medicaid enterprise.

Collaboration with the IV&V Team

As an organization with years of experience working on large-scale government engagements, Optum frequently interacts with IV&V vendors. We view your IV&V vendor as a key partner who will promote quality and contribute to overall project success. We will cooperate with IV&V team with the same professionalism we provide to DPHHS or any other project stakeholder.

Experience

Optum has extensive experience successfully delivering solutions and services in multi-vendor health care projects, including:

- CMS for healthcare.gov
- Massachusetts exchange
- Vermont exchange
- West Virginia Medicaid
- Wyoming Medicaid

To achieve these objectives, we will establish a close partnership with you and your vendors through coordinated communication, planning, and execution. Our goal for the project is to foster open communications, shared goals, a spirit of cooperation, and a positive working environment. We will work with you to implement a coordinated approach that includes regular communication with the SI contractor and your other vendors and stakeholders. We will adjust our project management approach and project schedule, as needed, to collaborate with them and meet our responsibilities for this scope of work.

3.10.2.1 Project Management

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

To guide the Provider Services module, we will work with DPHHS and the MPATH PMO, the SI vendor, and the IV&V vendor to develop a comprehensive PMP during the Planning Phase. The PMP will define the processes, methods, tools, and resources we will use to manage project activities. These include project management, quality management, and our SDLC. We base our PMP on our experience, lessons learned, and industry-based project and quality management methodologies.

The PMP includes various component plans that combine to form a holistic approach. This approach provides the framework to control the DPHHS project activities and assess their status through a transparent view to the project schedule, performance, and cost. This is important for accurate project reporting and appropriate decision-making. It will provide full project visibility for consistent command and control of project activities. In addition, it will guide the overall project execution, the way we report project progress, and the way we communicate with project stakeholders. Figure 3.21 shows the PMP component plans.

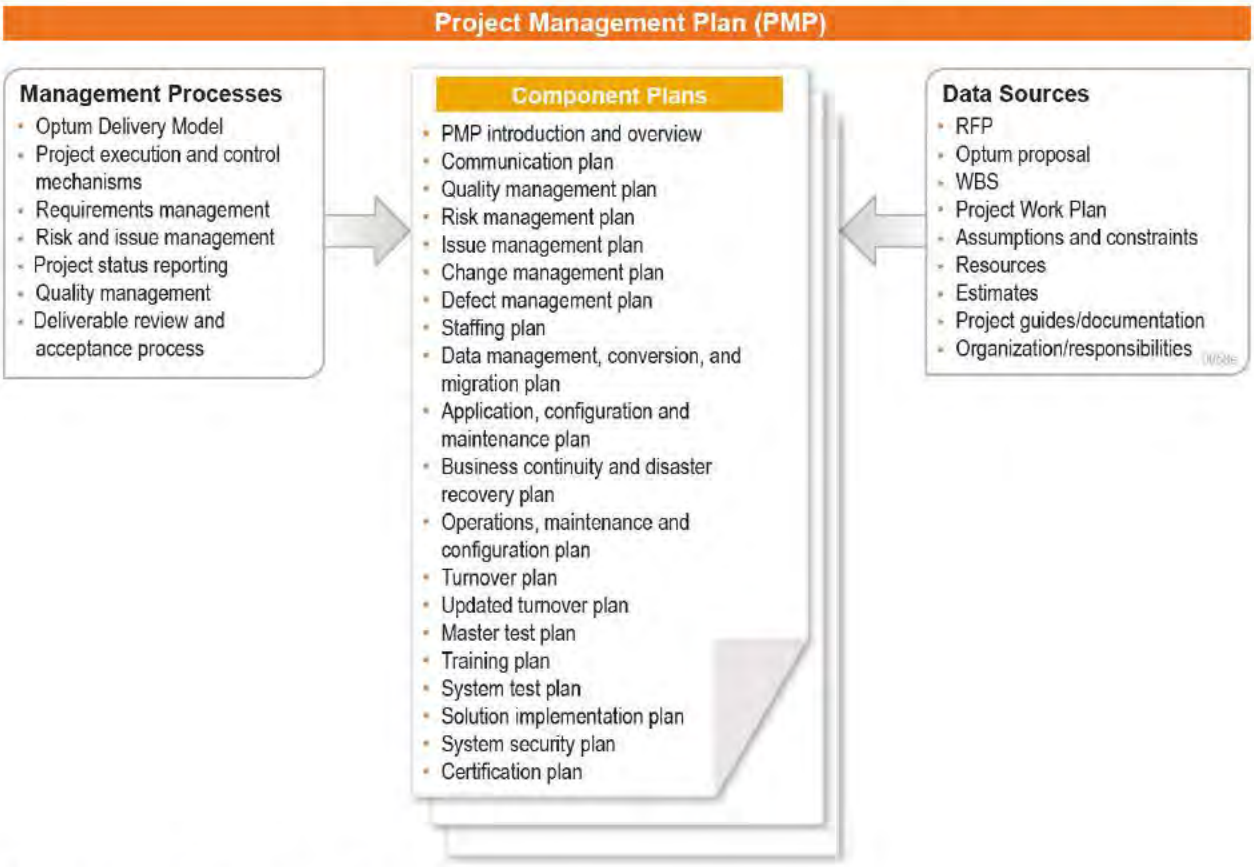


Figure 3.21: Project Management Plan.
Our PMP integrates project management processes and data sources into a holistic approach for delivering the Optum Provider Services solution.

We manage an existing library of project planning documents and templates that can be tailored. We will work with you to confirm the content of the PMP and related planning deliverables meet your project requirements. The PMP, PWP (project schedule), and other planning deliverables will serve as the roadmap to coordinate project activities for timely implementation. They will reflect our Optum Delivery Model and include the tasks, milestones, and deliverables necessary to fulfill requirements and deliver the Optum Provider Services solution successfully.

Commitment to Quality

We will deliver high-quality services and solutions to help you meet your project and business objectives. Our quality management approach is integrated into our PMP and centers on five guiding principles:

1. **Client satisfaction:** We work to understand your expectations and manage accordingly. This requires a combination of conformance to requirements (e.g., configuration according to approved specifications per RFP and contract requirements) and usability (e.g., your staff members can achieve business objectives).
2. **Prevention over inspection:** The cost of preventing mistakes is always much less than the cost of correcting them, as revealed by inspection. In this usage, cost can be a loss of time, confidence, efficacy, opportunity, or other tangible or intangible value.

3. **Management responsibility:** Success requires the participation of all members of the team, but it remains the responsibility of our project management team to plan and lead the quality approach. Our quality practices integrate with our project management approach, so we include quality into every phase of the project.
4. **Transparency:** We want you to feel as confident as we do in the quality of the work we provide, and the solutions we deliver. Through status meetings, quality reviews, dashboards, and reports, we will provide visibility into the status of quality initiatives, results of quality verification and testing activities, and compliance with quality and performance standards.
5. **Continuous improvement:** Quality improvement initiatives will improve the quality of both the project and the Optum Provider Services solution delivered and operated by Optum.

Project Management Tools

Our comprehensive suite of project management tools supports our delivery model and makes sure our staff delivers the Optum Provider Services solution in compliance with all of your requirements. During project initiation and planning, we will establish the tools in the Provider Services module environment. These tools will include the following.

Microsoft SharePoint: We will establish and maintain a Provider Services module document repository dedicated to project documentation and artifacts. The document repository will be available at the beginning of the project and throughout the life of the project. Optum will organize documents and artifacts in the repository supporting the CMS certification milestone reviews. We will work with you to establish a process for routing project documents, deliverables, and other Optum work products to and from the document repository to your Medicaid Enterprise document repository described in your RFP.

Microsoft Project Web Access: Using Microsoft Project Web Access (PWA), we will develop and maintain the Integrated Master Schedule (IMS). It will help us identify logically sequenced tasks, milestones, and deliverables and then trace them to your RFP requirements.

Microsoft Office: Optum uses the Microsoft Office suite of products to produce documentation for the project, including Microsoft Word, Visio, and Excel.

HP Application Lifecycle Management: We will use the HP Application Lifecycle Management (ALM) COTS tool for requirements traceability throughout the project. In addition, we will use it as a complete test case creation, planning, team management, and execution tool. HP ALM is fully customizable to the specific demands of the Optum Provider Services solution. Features include:

- End-to-end requirements traceability
- Comprehensive test coverage management
- Wizard-driven test scheduling and assignment
- Automated testing tool integration
- Defect submission that enables defects submitted in HP ALM to be linked to test cases and tested
- Built-in reporting and analysis that provides testing trend analysis, team performance, and other metrics

- Reporting that provides an accurate window into testing progress so that project stakeholders have an accurate, up-to-the-minute perspective on the progress of testing tasks

Using the HP ALM features, we will track product defects and development issues. It provides the following benefits:

- A flexible graphical user interface (GUI)-based workflow engine that enables Optum staff to configure escalations, email notifications, and team inboxes easily
- Streamlined integration with version control tools that makes it easy to track defects across solution components and configuration items
- Visibility into the development process through pre-defined reports and graphs providing transparency to DPHHS

ServiceNow*:* Optum will use ServiceNow for change control, help desk ticketing, and incident reporting. When a person calls the help desk, we will log a ticket in the tool and update the ticket as we address the incident. Using the tool's automated workflow and reporting capabilities, we will route, monitor, and track tickets. For changes to project scope, schedule, or cost, we follow a rigorous change control process where we log change requests and route the workflow according to a defined process.

SharePoint deliverable tracking tool: For deliverable management, we will use a SharePoint tool integrated with our document repository. The tool will house our baseline deliverable matrix with due dates and owners. We will update it regularly to show progress toward deliverable milestones. When a deliverable is ready for formal submission to you, we will coordinate with you to route the documents from our document repository to your Medicaid Enterprise document repository.

PMT01 The Contractor shall provide licenses as required by the Agency to allow users access to perform all necessary business functions.

Optum will provide licenses as required by DPHHS to give users access to perform all necessary business functions. Our configurable, COTS-based solution uses commercially available products whose vendors continually upgrade and improve those products to keep current with evolving market requirements.

PMT02 The Contractor shall support the Department in all program governance activities as necessary.

Our project management structure, together with your established governance structures, will help you advance your governance model. We will support your governance model, adapting as requirements evolve. To accomplish this, we will leverage our guiding project management principles of sustainability, consistency, transparency, accountability, and objectivity. A strong alignment will enable our project manager to set appropriate priorities, make informed decisions, and resolve issues quickly.

Our approach to project management establishes repeatable processes. These processes establish expectations, key checkpoints, team interactions, well-organized and effective meetings, efficient decision-making, scope management, and sound detailed planning. Within our project management framework, our project governance plan will capture mechanisms to achieve your defined project governance essentials and yield high results for desired project results and expected outcomes.

Our customized project governance approach will clearly articulate a strong sponsor buy-in and project governance planning that will be essential for overall success. Project governance will

support transparency by keeping all project activities visible to our mutual leadership. As your governance requirements change, we will update our project management model to reflect new guidance and direction. Our project governance model includes:

- **Setting project governance expectations:** Our project team will recommend different project governance possibilities that align with your governance model, along with the strengths and weaknesses of each approach. We will review these recommendations with you, establishing the option that best fits your model and expectations.
- **Customizing project governance:** Because our project management processes are adaptable to support your changing needs, change management and control for project governance implementation is important. We will develop an approach to establish our new project governance model along with recognizing and mitigating any potential negative consequences. In addition, we will leverage value-added tools, proven processes, and strong accountability procedures. We will align the correct people with the required skills to the right roles.
- **Executing project governance:** Upon agreement, we will work with you to execute your governance model and facilitate communication to set expectations for all project team members.
- **Monitoring project governance:** We will continuously monitor our alignment to critical success factors for our project management and governance processes. As appropriate, we will recommend changes to optimize governance efforts. We will adjust our project governance model, along with guidance from executive stakeholders, when there is significant executive turnover or acknowledgement that a current process has encountered new challenges.

The following guiding principles of our project management framework help us maintain an adaptable governance model:

- **Sustainability:** We will commit leadership, effective project governance, and critical skilled resources for the life of the project.
- **Consistency:** Our project governance processes will provide a unified approach for controls and minimize duplicative risks.
- **Transparency:** Our project governance will foster open communication, create a spirit of cooperation, and create a positive work environment by keeping project activities visible to leadership.
- **Accountability:** We will clearly define and delineate project governance roles and responsibilities for ownership, controls, approvals, decision makers, and inputs for other key processes.
- **Objectiveness:** Working with you, we will:
  - Achieve a solution that accomplishes your mission and vision
  - Verify our solution satisfies your needs
- **Facilitation:** Project governance will facilitate key meetings with executive stakeholders.
- **Participation:** Our project governance representatives will include stakeholders from affected units, state offices, or partners.

Key to project governance facilitation is a well-defined communications framework, as Figure 3.22 shows. Using this framework, team members can consistently make key decisions aligning with discussions stemming from key meetings with you and your stakeholders.

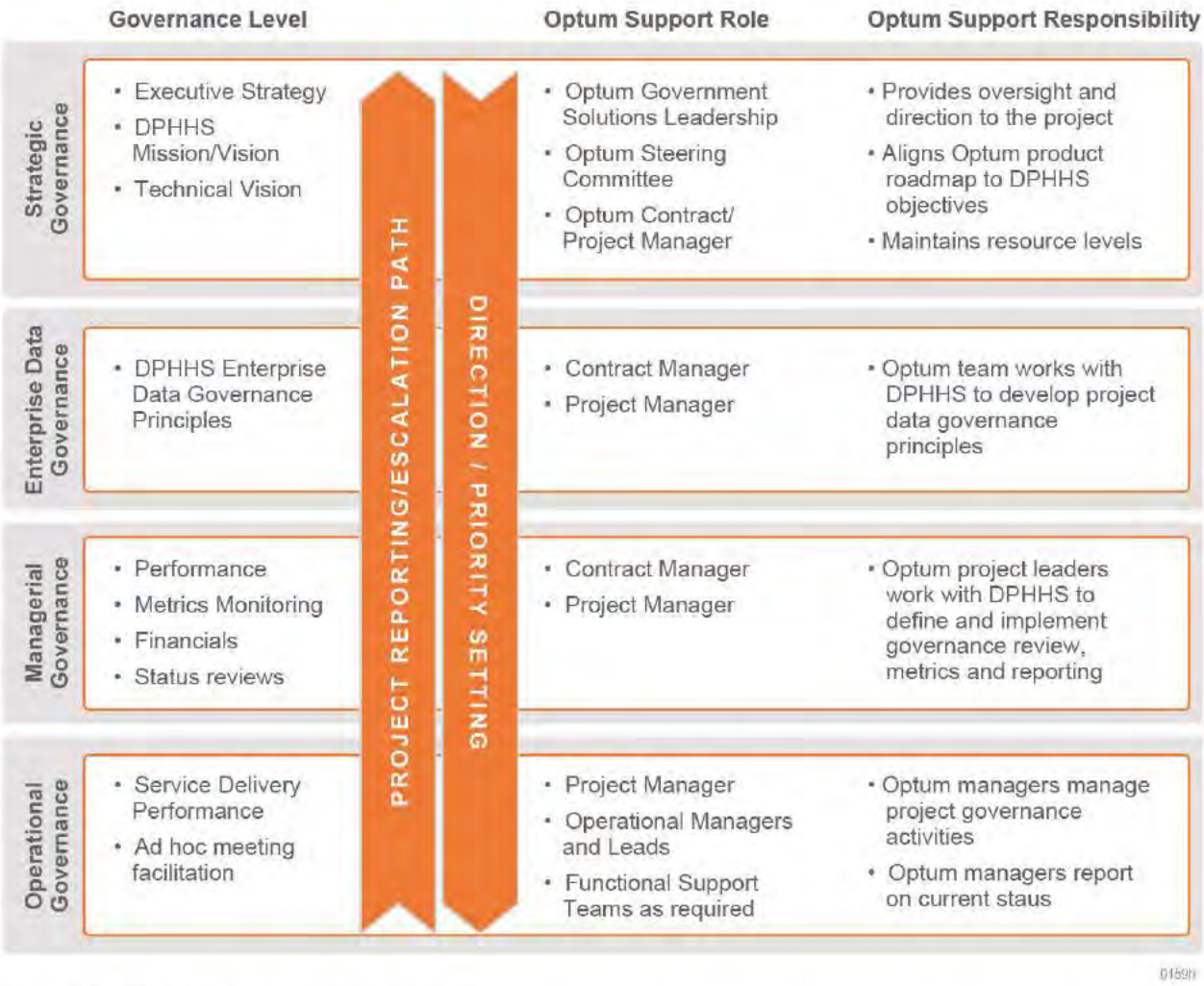


Figure 3.22: Project Governance Framework.
Our proposed project governance model for the State will promote close cooperation, communications, and active management participation.

Our project governance model will serve as a project roadmap for frequent and candid communication, early risk identification, a clear escalation path, and timely issue resolution.

PMT03 The Contractor shall be responsible for the capture and dissemination to the Department of agendas, meeting minutes and documentation necessary for successful execution of the project.

We will be responsible for the capture and dissemination of agendas, meeting minutes, and documentation necessary for successful execution of the project. We prepare meeting agendas and necessary meeting materials in advance of regularly scheduled meetings. Depending on the circumstances, we will distribute the agenda and meeting materials in advance of the meeting (such as for regularly scheduled status meetings), and in some cases the agenda and meeting materials will be distributed in the meeting (such as in an ad hoc meeting). During the

meeting, one of the Optum attendees will be designated as a scribe for the meeting, capturing the meeting minutes as the meeting progresses. At the end of the meeting, the scribe will prepare and draft version of the meeting minutes, which is then distributed to all meeting attendees for review and comment. The meeting minutes are updated as needed to address any comments or concerns expressed by the meeting attendees, and a final version of the meeting minutes is prepared and distributed. A copy of the final meeting minutes and any appropriate materials or items presented in the meeting will be uploaded to the SharePoint shared portal for easy access by authorized personnel. The approved meeting minutes are converted to PDF prior to uploading to the SharePoint portal so the minutes cannot be changed after approval.

PMT04 The Contractor shall participate in necessary meetings with the stakeholders and/or other Contractors.

We will participate in necessary meetings with DPHHS designated stakeholders and other contractors. Our contract manager or project manager, or their designee, will attend all meetings approved by you. Our goal is to have open and honest communication between all parties so we can meet your project objectives. Our Stakeholder Management Plan will enable our project manager to effectively engage stakeholders, manage their expectations, nurture relationships between the stakeholders and the project team, and ultimately achieve project objectives by satisfying stakeholder needs. Understanding the interests and expectations of project stakeholders will help our project manager develop a clear, concise, and actionable plan to communicate and interact with stakeholders at the appropriate times throughout the project.

By building trust, resolving conflict, and overcoming stakeholder resistance to change, we will accomplish effective stakeholder management. The Optum project manager will collaborate with the DPHHS project manager, as needed, to facilitate consensus on project objectives, exert influence over stakeholders to support the project, negotiate agreements that satisfy project needs, and modify organizational behavior to accept project outcomes.

Activities that will help us manage stakeholder engagement for our solution include the following:

- Engaging stakeholders during appropriate project phases to obtain or confirm their continued commitment to the success of the project, in particular during the initial phases of the project when stakeholder interest and influence is the greatest
- Managing expectations through effective communication or negotiation to help make certain we achieve project goals
- Addressing potential concerns and anticipating future problems raised by to prevent project risks and issues
- Clarifying and resolving issues stakeholders have identified

To facilitate project success, we will establish structured lines of communication with stakeholders and stakeholder groups. Collaborating with them will help us understand their expectations, address issues as they occur, foster stakeholder engagement, and provide an update mechanism to keep them involved and aware of the project's progress.

PMT05 The Contractor shall provide deliverables or documentation as defined in the Project Work Plan (PWP) and approved by the Department.

Optum will provide deliverables or documentation as defined in the PWP and approved by DPHHS. The deliverables we provide will include the deliverables specified in the RFP and illustrated in the following table.

Deliverable	Delivery and Update Frequency
Project Management Plan	As scheduled in approved PWP, updates as necessary
Project Work Plan	Project initiation, updates as approved
Communication Plan	As scheduled in approved PWP, updates as necessary
Quality Management Plan	As scheduled in approved PWP, updates as necessary
Risk Management Plan	As scheduled in approved PWP, updates as necessary
Issue Management Plan	As scheduled in approved PWP, updates as necessary
Change Management Plan	As scheduled in approved PWP, updates as necessary
Defect Management Plan	As scheduled in approved PWP, updates as necessary
Staffing Plan	As scheduled in approved PWP, updates as necessary
Data Management, Conversion, and Migration Plan	As scheduled in approved PWP, updates as necessary
Application, Configuration, and Maintenance Plan	As scheduled in approved PWP, updates as necessary
User Interface Style Guide	As scheduled in approved PWP, updates as necessary
User Documentation	Project initiation, updates as necessary
Operations Procedure Manual	As scheduled in approved PWP, updates as necessary
Business Continuity and Disaster Recovery Plan	As scheduled in approved PWP, updates annually
Operations, Maintenance and Configuration Plan	As scheduled in approved PWP, updates as necessary
Turnover Plan	12 months prior to final Contract year
Updated Turnover Plan	6 months prior to final Contract year
Technical Documentation	Project initiation, updates as necessary
System Design Documentation	As scheduled in approved PWP, updates as necessary
System Documentation	Project initiation, updates as necessary
Master Test Plan	As scheduled in approved PWP, updates as necessary
Training Plan	As scheduled in approved PWP, updates as necessary
System Test Plan	As scheduled in approved PWP, updates as necessary
Module Implementation Plan	As scheduled in approved PWP, updates as necessary
Solution Architecture Document	As scheduled in approved PWP, updates as necessary
Attachment L – Technology Matrix	Upon initial proposal, updates annually
Turnover Results Report	Upon completion of turnover activities
Monthly Status Report	Monthly
System Security Plan	As scheduled in approved PWP, updates as necessary
CMS Information Security Program Plan of Action and Milestones (POAMS)	Conditional upon security risk assessment findings
Risk Assessments	Annually and as needed

Deliverable	Delivery and Update Frequency
Requirements Traceability Matrix (RTM)	As scheduled in approved PWP, updates as necessary
CMS Certification Checklists	As scheduled in approved PWP, updates as necessary
Certification Plan	As scheduled in approved PWP, updates as necessary
Operational Readiness Review Checklist	As scheduled in approved PWP date
Operation Readiness Test Results	As scheduled in approved PWP date
Penetration Test Report	Annually and 6 months prior to implementation
Performance Test Results	As scheduled in approved PWP, updates as necessary
System Test Results	As scheduled in approved PWP, updates as necessary
Parallel Test Results	As scheduled in approved PWP, updates as necessary
Regression Test Results	As scheduled in approved PWP, updates as necessary
Integration Test Results	As scheduled in approved PWP, updates as necessary
Disaster Recovery/Business Continuity Test Report	Annually
Monthly Turnover Report	Monthly, during Turnover Period
Subcontractor Usage Report	Annually
System Enhancement Pool Report	Monthly
Business Rules Catalog	Project initiation, procurement of each MPATH module and updates as necessary
Certification Crosswalk	As scheduled in approved PWP, updates as necessary
Personnel Background Check Attestation	As necessary
Interface Control Documents (ICD)	As scheduled in approved PWP, updates as necessary
Deliverable Review and Acceptance Process	Project initiation, updates as necessary
Data Dictionary	As scheduled in approved PWP, updates as necessary
Conceptual Data Model	As scheduled in approved PWP, updates as necessary
Security Audit Report	Annually on September 30
Service Organizational Control (SOC) 1 Type II Reports	Annually
Implementation Letter	As scheduled in approved PWP

We will work closely with DPHHS in developing and reviewing Deliverable Expectation Documents (DEDs) for all deliverables where this is required. The DED enables both parties to agree on the format and content of each deliverable so the deliverables we provide will align with your expectations.

We include tasks in our preliminary PWP to develop each deliverable for submission to DPHHS. You will then have the opportunity to review and comment on each deliverable. Then, we will update the deliverables as needed to address your comments and resubmit the deliverable for final review and approval.

PMT08 The Contractor shall support the State and its Contractor(s) in Independent Verification and Validation (IV&V) activities associated with the contract including CMS Certification(s).

Certification

Optum has successfully achieved CMS certification on time, the first time, in every implementation where certification was required.

Optum will support the State and the State's Contractors in IV&V activities associated with the contract including CMS Certifications. For certification, we will provide the necessary documentation to verify our solution performs according to the module's certification requirements. Throughout implementation, we will provide transparent reporting and ongoing dialogue with you to verify DDI and certification documentation are complete and in place, activities are on schedule, and meet the predefined milestones. Solution documentation and project artifacts will be readily accessible for review by you and the CMS certifying officials on our SharePoint document repository.

Our team has a thorough working understanding of the Medicaid Enterprise Certification Toolkit (MECT) and the way effective documentation helps drive the certification process. In fact, all of key areas in which we provide support to our state customers during certification revolve around retrieving or generating effective project documentation. These include the following:

- Compiling reports and data required for the preliminary letter submission to CMS
- Preparing required certification manuals, reports, forms, and documentation
- Providing staff to assist State personnel in certification procedures, data warehouse/business intelligence operations, and supplying information needed for the State to make certification presentations
- Participating in CMS site visits including vendor's operational facilities
- Providing the expertise to answer questions, locate, and provide additional materials needed by the CMS review team

In one experience, our team tried to work with a vendor whose documentation we needed to finalize our solution requirements in preparation for certification activities. The submitted documentation was inadequate, and we worked collaboratively with our customer and our customer's IV&V Contractor to obtain adequate documentation. Our customer's IV&V contractor was especially helpful in making sure the project documentation acquired was complete, comprehensive, standardized, and in place in time to support the CMS-approved plans and milestones.

PMT09 The Contractor shall conduct a monthly status meeting to discuss project tasks and activities (e.g., deliverables, milestones, issues, risks, and SLAs).

Optum will conduct a monthly status meeting to discuss project tasks and activities. The monthly status report items for review and discussion will include:

- **A complete set of updated and current output from the PWP along with a copy of the corresponding project schedule files in electronic version:** Optum will maintain the current updated version of the PWP on SharePoint repository where authorized DPHHS personnel can review and download it at any time.
- **A description of the overall completion status of the project including schedule variations that report the earned value of the work completed, the planned value of the work completed, and the variance:** Schedule variations include tasks not completed on time, tasks behind schedule, tasks not started on time, and tasks that were underestimated that require additional resources be assigned.

- **Planned tasks and activities for the next month:** These planned tasks and activities for the next month will derive directly from the PWP.
- **Deliverable status, with percentage of completion and time ahead or behind schedule for particular tasks:** We include tasks for developing and submitting all deliverables required by the RFP in our preliminary PWP, including the start and completion dates for all tasks. This will enable us to constantly monitor the status of each deliverable and determine if a deliverable is on schedule for submission.
- **Identification of any staffing issues or changes in the Resource Allocation Matrix:** Our project manager is responsible for maintaining resources for the project at the proper level. If any staffing issues or changes arise during the course of the project, the monthly status report will include those issues or changes.
- **Status updates on all issues being monitored:** We will document and manage all project risks, issues, decisions, and action items assigned to us. We will use our IRAAD (Issues, Risks, Actions, Assumptions, and Decisions) tool as the primary means to track project action items, decisions, issues, risks, and defects. Updated at least weekly, and we will use the SharePoint-based IRAAD tool to report on the updated status of all project issues being monitored.
- **Provision of metrics necessary to support the State CIO's Legislative Finance Committee (LFC) reporting requirements:** During the early stages of the contract, we will meet with DPHHS to review the monthly status report requirements and agree on the format and content for the monthly status report, including LFC reporting requirements.
- **Testing status and metrics:** Optum uses automated tools to the extent possible in testing. This enables us to generate ongoing reports detailing the status of testing activities. It also enables us to report, by functional area, on the total number of test cases, test cases completed, test cases passed, test cases failed, and test cases in progress.
- **System enhancement hourly pool total hours used and total hours remaining:** Optum will submit a monthly System Enhancement Pool report that details tickets invoiced to the hourly pool. This includes hours used and hours remaining for the DPHHS's approval. Please see our response to Requirement PMT29.
- **Status updates on all SLAs being monitored:** We will maintain a project scorecard that tracks and reports on our approach to achieving performance standards. It is an established management infrastructure that:
  - Tightly manages the core processes that matter most to the DPHHS and may affect the provider community
  - Measures and reports on aspects of operations beyond DPHHS's stated SLAs
  - Builds quality into our processes to maintain attention on effective operations rather than corrective actions

We have successfully implemented this approach into many other state accounts. We will tailor these procedures and strategies to meet your requirements. Our proven processes, tools, and best practices are built based on our comprehensive focus on quality and lessons learned from previous projects. Our Performance Management Framework is illustrated in Figure 3.23.

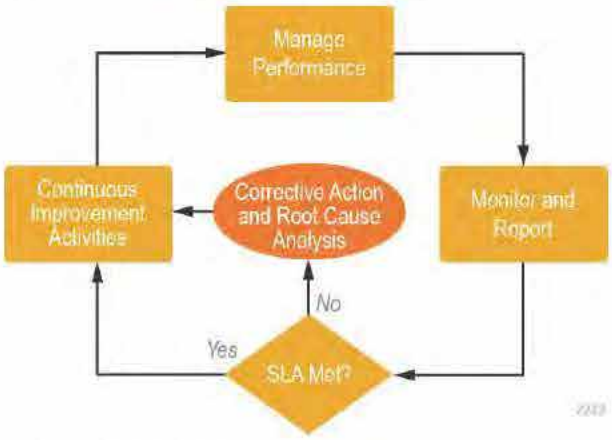


Figure 3.23: Performance Management Framework.
Our proven Performance Management Framework has proven integral to delivering quality solutions to our state clients.

Our Performance Management Framework focuses on three key activities:

1. **Manage performance:** Optum uses a layered approach to managing performance that starts and ends with our leadership. Our leaders are accountable for achieving performance goals so they work diligently with our quality management team and operational executives to monitor performance, identify opportunities, and develop improvement strategies.
2. **Monitor and report results:** Our approach to monitoring and reporting performance starts with developing systems and procedures that proactively measure performance, adhere to controls, and identify potential issues. A validated issue that affects a performance standard then follows a corrective action process managed by the quality management team and responsible supervisor and leadership.
3. **Continuously improve:** Our operational leadership team continually meets with our quality management team to identify potential risks and issues requiring root-cause analysis efforts. All potential risks are vetted for new, preventive controls, while identified issues are examined for root cause and performance improvement projects.

We will also address any other items deemed appropriate by the State. During the early stages of the contract, we will meet with DPHHS to review the monthly status report requirements and agree on the format and content for the monthly status report.

PMT10 The Contractor shall conduct weekly meetings to discuss issues, risks, progress of current projects, solution changes, resource changes, and other areas specific to the scope of work.

We will conduct weekly meetings to discuss issues, risks, progress of current projects, solution changes, resource changes, and other areas specific to the scope of work. An effective reporting model is needed to provide you and other key stakeholders with continuous transparency into the project delivery progress. Early in the project, we will meet with you to determine project performance reporting requirements. This will include project status reporting and project activity tracking objectives. The weekly status briefings will include, at a minimum, an assessment of progress against the plan; any slipped or slipping tasks, risks, and issues; mitigation plans and changes needed to the PWP or project approach.

Typical information we will provide in our project status reports includes the following:

- List of tasks/milestones completed this reporting period

- List of tasks/milestones scheduled to start during the coming reporting period
- List of tasks/milestones not completed as scheduled
- List of tasks not started as scheduled
- Planned corrective actions for tasks not on schedule, status of assigned action items
- Issues/risks that have to be addressed/mitigated
- Issues/risks mitigation plans
- Issues/risks that have been resolved
- Project metrics

Advantage

We implement a no-surprises approach to project delivery by reporting status and progress in detail and often to multiple layers of key project stakeholders.

Status reports will help us track progress against project plans and report status in a form and format you approve. They provide a mechanism for us to document and manage project plan risks, issues, and action items.

PMT11 The Contractor must employ a project management approach that will satisfy the scope of work and incorporate all activities described in the RFP. The Contractor shall adjust the project management approach or project schedules, as necessary, to collaborate with the module vendors in order to incrementally build the enterprise platform.

To manage the project, we will implement our best practices-based Optum Delivery Model, which we developed by integrating the PMBOK and SAFe principles. Our delivery model provides a disciplined system development methodology, the OSAM, and structure for managing project activities, governance, communications, and assessing project status. It will facilitate and assess communications with the project team.

Our Optum Delivery Model will govern each stage of our solution within the broader overarching project plan. It includes an integrated set of project management disciplines adapted to meet the State's project requirements during DDI as well as ongoing operations. The Optum Delivery Model enables us to employ a project management approach that will satisfy the scope of work and incorporate all activities described in the RFP.

The Optum Delivery Model allows great flexibility in adjusting the project management approach or project schedules, as necessary, to collaborate with third-party entities, such as other module vendors, to incrementally build the State's enterprise platform. DPHHS will review and approve the Optum PMP and the PWP at the beginning of the project. These documents then become the baseline, placed under configuration management control. All subsequent updates to the PMP or the PWP must move through approved change control processes and receive appropriate DPHHS and Optum management approval before being implemented.

PMT12 The Contractor shall conduct a project initiation kick-off meeting with key stakeholders and the State's project team.

Optum will conduct a project initiation kick-off meeting with key stakeholders and the State's project team. As we begin the project, we will work with you and identified stakeholders on the following:

- Clarify the objectives
- Understand deliverables
- Set milestones and schedules for project deliverables and phases

- Confirm roles and responsibilities
- Establish clear lines of accountability
- Implement a framework for effective project management and control

We will schedule a kick-off meeting and initial working session with you and other appropriate project stakeholders and members of our team. The goal of the kick-off meeting is to introduce the Optum Provider Services solution and give you and other project stakeholders an understanding of our approach to implementing our solution. We will review the scope of work that we will undertake for the project and confirm goals and objectives for the project. We will also highlight participant roles and responsibilities, so attendees understand expectations of them during the project.

Likewise, our team will confirm our understanding of the role our solution will play in your overall enterprise environment. We will also work with you to review and help you refine the State's enterprise IT strategy to drive the implementation (and later operations) of the solution. We will demonstrate our approach to meeting CMS' Seven Conditions and Standards so that you can receive enhanced FFP for the solution.

PMT13 The Contractor shall implement procedures and tools for tracking project action items, decisions, issues, risks and defects.

Projects of the size and scope of the Provider Services module normally experience risks or issues that we must understand and evaluate to determine their effect on project objectives. We expect the project to experience a certain level of risk that we must identify, manage, and mitigate. We will document and address risks identified during the course of the project and resolve or mitigate them without compromising the success of the project. Figure 3.24 shows our risk management approach.

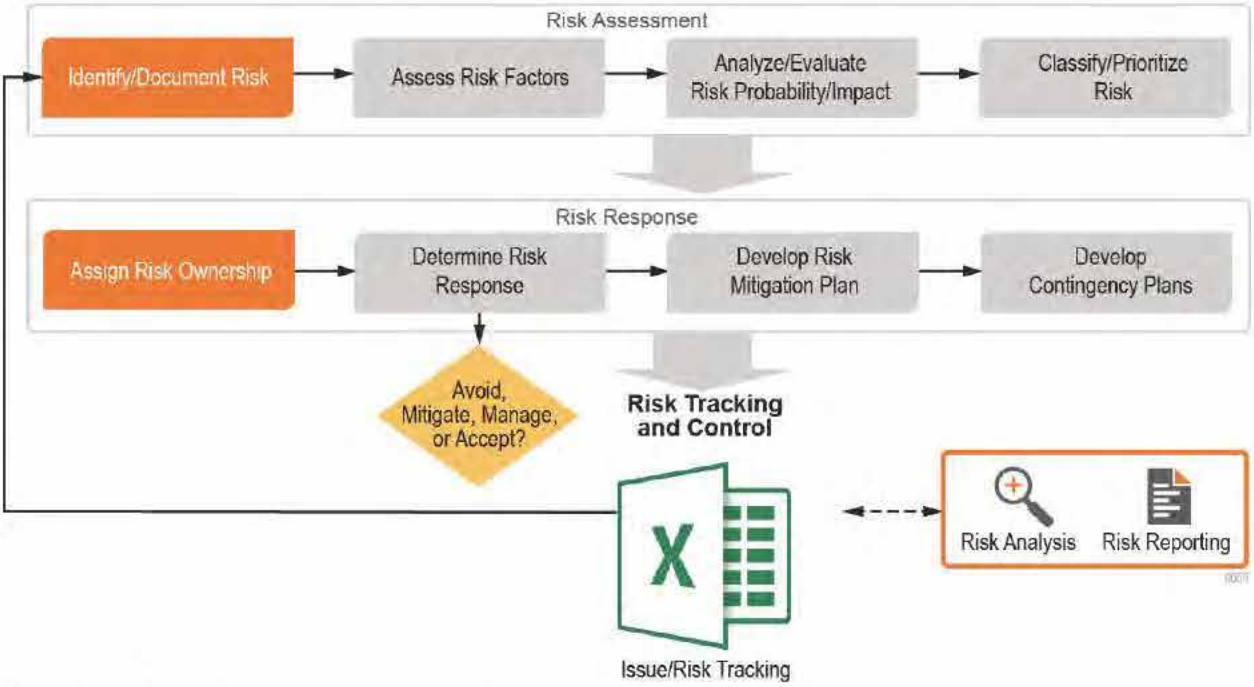


Figure 3.24: Optum Risk Management Approach.
Our risk management approach includes identifying and assessing risks, assigning them to a responsible owner, and resolving risks or developing and implementing a mitigation approach.

Using sound risk management techniques, the Optum Provider Services solution team can identify potential problems and issues and provide contingencies. Risk management addresses the following:

- **Risk:** A threat to project success
- **Risk probability:** Percent chance that a risk will materialize as a real problem
- **Risk impact:** The potential effects of a risk on the project, characterized in terms of cost, schedule, and performance
- **Risk avoidance:** Actions to remove a risk (probability = 0)
- **Risk mitigation:** Actions to reduce the risk probability or the risk impact
- **Risk exposure:** The probability times the cost impact
- **Risk contingency:** Actions to resolve the problems when a risk materializes

We will develop, deliver, and maintain a Risk Management Plan for your review and approval. It will define the risk assessment and risk management process for the Provider Services module. We will use it to identify and manage project risk. Figure 3.25 depicts the sequence of tasks included in our risk management process.



Figure 3.25: Risk Management Process.
Our risk management process contains clearly defined steps to classify, track, and manage identified risks effectively through to resolution.

Risk management control starts with the implementation of any risk avoidance, mitigation, or contingency activities. Risk management control generally does not occur until risk

management planning is completed. The tasks accomplished during risk management control include:

- **Implementation of risk avoidance/mitigation approaches:** The purpose of this task is to implement risk mitigation and avoidance actions as needed.
- **Project reviews, risk reporting, review, and corrective action:** The purpose of this task is to review risk status periodically and update risk plans.
- **Implementation of risk contingency plans:** The purpose of this task is to implement risk contingency actions as appropriate.

A well-documented, step-by-step approach to risk management will help us identify, manage, and control risks. When we have identified a set of non-redundant risks, we will assess each one for its likelihood and consequence:

- Likelihood is ranked as Very High, High, Nominal, Low, or Very Low
- Consequences are ranked as Very Severe, Severe, Nominal, Low, or Very Low

This combination of likelihood and consequence positions each risk into one of three categories:

- Most Important Risks
- Very Important Risks
- Important Risks

Figure 3.26 shows the risk assessment matrix.

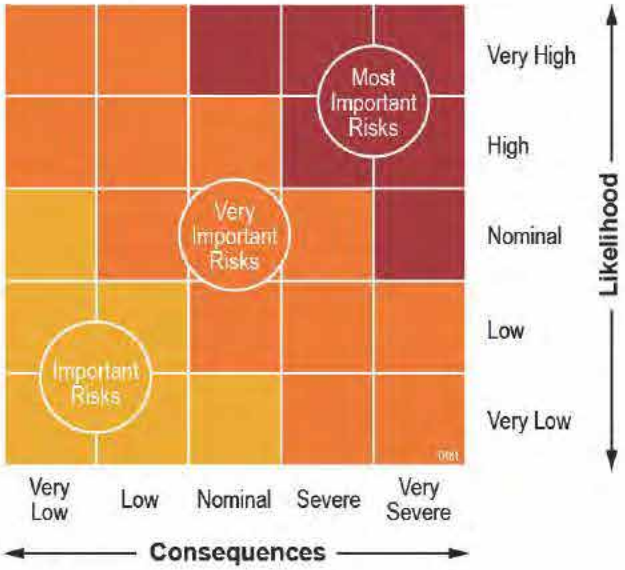


Figure 3.26: Risk Assessment Matrix.
We will assess each risk for its likelihood and consequence.

We will document identified risks and resolve or mitigate them so the project is not compromised. The owner of each risk will track the status of that risk, update the risk status weekly, and inform the manager or team lead of a change in status as it occurs. The DPHHS project manager and Optum project manager will review the status of each risk at the weekly IRAAD review meeting with key stakeholders and take necessary action. The risk tracking and reporting process begins by identifying and producing a list of potential project risks. Risk

assessment identifies risk probability and impact. Risk assessment may be hierarchical, depending on the size of the project and total system solution. Low-level risks feed upward and must be monitored in parallel with the total solution. Management experience and lessons learned from other projects commonly serve to effectively assess risk probability. Impact estimates generally require in-depth analysis because specific quantification is required.

After risk assessment, we will filter the candidate risks to include only those that have a moderate to high likelihood and consequence. We will assign risk management responsibility for identified risks and create a risk management strategy. For each significant accepted risk, we will develop appropriate risk mitigation strategies to limit the project impact.

We use an IRAAD tracking log maintained in an Excel spreadsheet to track risks and resolutions. We will store a copy of the log on the secure DPHHS SharePoint repository where authorized DPHHS or Optum personnel can access it.

In addition to the IRAAD log, we will use an industry standard Risk Priority Number (RPN)-based risk model used for assessment and mitigation of all major identified risks. This model will provide objective evaluation and classification of all risks, with a numerical score assigned to each risk based on the project impact and probability of occurrence. We will measure each risk against its influence on project timelines and costs. In addition, we will provide timely updates on key risks to stakeholders through comprehensive reporting. Figure 3.27 shows the risk management process using the RPN model.

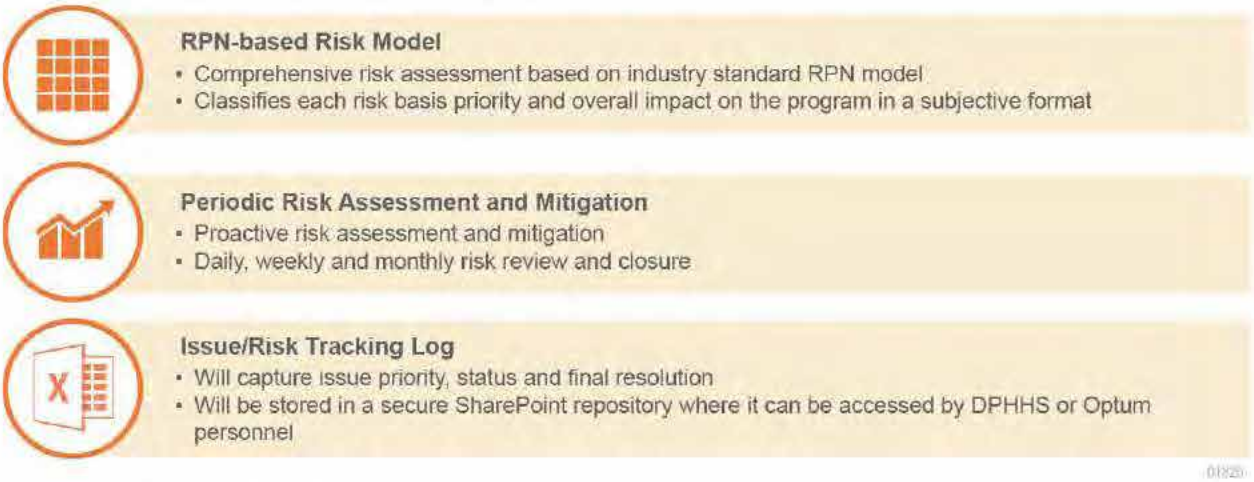


Figure 3.27: Risk Priority Number Model.
We use a proven risk model to identify risk, which we will manage and communicate through the IRAAD tool.

We will document and manage all project risks, issues, decisions, and action items assigned to us. We will use our IRAAD tool as the primary means to track project action items, decisions, issues, risks, defects and their status. It will help teams and project managers drive more predictable outcomes by identifying key risk areas across a product or project development initiative. It will enable the DPHHS and Optum leadership to have a common understanding of project activities that may affect the project schedule.

We will review and discuss open issues during the weekly IRAAD review meeting. Team members will be notified of any impact analysis assignments. Updates will be made to the issue log as appropriate, and decisions may include closing an issue or creating a new issue. During the meeting, we will review issues according to their priority: 1 – Urgent; 2 – High; 3 – Medium; and 4 – Low.

During the IRAAD review meeting, project team members assigned to an issue will provide status updates on actions taken to resolve the issue. The updates will follow the agreed upon frequency based on priority. Team members will be responsible for identifying the various documentation assets that are affected by the issue noted in the IRAAD log. They will also document the actions taken to update those related documents.

To verify transparency and communication, we will summarize and report on risks and issues at a high level in the Weekly and Monthly Project Status Reports.

PMT14 The Contractor shall provide an electronic document repository for project documents and deliverables. The Contractor, Department staff and other contractors with the appropriate security level must have the ability to upload/attach new or revised versions of documents. The repository must perform version control and allow users to view all prior versions.

We will establish a SharePoint project repository to store and manage deliverables and other Optum work products, as well as house our risk management tool. The repository will maintain version control and provide our team and the State with secure access to key project documents. We will work with DPHHS to identify all users who will require access to the SharePoint repository, and establish secure access for those users. Authorized DPHHS, IV&V, and Optum staff will access the repository easily to view the latest version of key project artifacts, as well as prior versions. Because our solution is built on SharePoint, it provides a full suite of documentation management capabilities. These capabilities include tagging, version control, collaborative edit, familiar user interface, and search.

Many of the key artifacts placed in the SharePoint repository are deliverables DPHHS has reviewed and approved. These documents are placed under configuration management control and can only be updated through an approved change control process, with appropriate DPHHS and Optum management sign-off before becoming effective. We will work with DPHHS to identify the DPHHS or Optum personnel who will have the ability to upload/attach new or revised versions of documents. Our SharePoint repository provides role-based access control so only authorized users can view and edit documents, provide comments and approvals, and participate in deliverable workflows according to defined routing rules.

Features of our SharePoint document repository include the following:

- **Web-based access to documents and operational artifacts stored to our SharePoint repository:** The repository will store project information, deliverables, documents, and operational artifacts based on your requirements.
- **Tagging of documents and artifacts:** SharePoint supports using metadata, such as date/time stamp, user last modified, unique document identifier, and other data points to classify content. These metadata, in turn, make it easier for documentation users to search and locate the exact information they are seeking.
- **Collaborative editing and version control governed by role-based access:** Each user accesses content appropriate for his or her user permissions. Users with edit permissions can check documents out for editing. Multiple users can co-author a single file using this check in/out feature. SharePoint supports full version control and the ability to roll back to a prior version of a document.
- **Automated notifications of new and changed documents:** SharePoint includes the ability to configure and set up rules for automating notifications to users. Document routing and approval workflows can easily be configured based on State requirements.
- **Ability to interface with common desktop productivity software:** SharePoint natively integrates with most common desktop productivity software.

- **Search capability:** SharePoint provides a robust search capability. Users will be able to search within individual documents or among documents in the repository. Both basic and advanced search features are available.
- **Ability to annotate documents:** Documents can be annotated in several ways. Many desktop productivity tools already include functionality for making notes and comments. For example, Microsoft Office documents, such as Word and Excel, the comments feature can be used to make notations within the documents themselves. When stored to the SharePoint repository, we maintain a full version history including any notes or comments made within the document. In addition, our SharePoint site will enable users to append information to documents using metadata and by making notations in document description and properties fields.

PMT15 The Contractor shall establish and utilize a deliverable review and acceptance process agreed upon by the Department that incorporates the following:

a. Review cycles, which will be conducted and scaled to the size and complexity of the deliverables.

b. Deliverables will need to reflect coordination with the overall modular program and will follow agreed upon change control processes.

c. Informal reviews and walkthroughs of draft and final deliverables are encouraged.

d. Queuing up excessive deliverables for simultaneous review is unacceptable to the Department.

We will develop and submit required deliverables as defined in our PWP. Upon contract award, we will work with your team to review and confirm the list of required deliverables. Optum will establish and maintain a project knowledge repository for the Provider Services module. The project repository will facilitate the deliverable review and approval process. We will develop and submit all required deliverables. We will publish draft and final deliverables to our project repository. Our SharePoint repository provides RBAC so only authorized users can view and edit documents, provide comments and approvals, and participate in deliverable workflows according to defined routing rules.

Optum has a no-surprises approach to managing deliverables. This means that we will work with you during joint reviews to confirm, in advance, that every deliverable we submit will meet your expectations.

We start by developing a DED for each deliverable to confirm that the planned format and content meets your needs. Rather than just creating the DED and submitting it, we will conduct a joint walk-through meeting to review the DED and make real-time updates based on your feedback. Our experience shows this to be the most efficient way to achieve approval of the DED, so we can move quickly into developing the draft deliverable.

Optum will follow a disciplined approach to developing deliverables and documentation. We will begin by creating a template or tailoring an existing template. To verify quality, we customize deliverable content to specific project requirements and peer review the document. User, technical, and system documentation, as well as project plans, status reports, correspondence and other deliverables and documents will be maintained in file formats according to your requirements.

Our deliverables will conform to the standards and quality processes defined in our PMP as well as the PWP we develop. During deliverable development, we will perform quality reviews to confirm we are meeting our high quality standards. These include comparing each deliverable against quality checklists and subjecting content to peer review, where appropriate.

We provide transparency throughout the deliverable development process. We will work with you during joint reviews to confirm, in advance, that every deliverable we submit will meet your expectations. We use the DED to help everyone understand the deliverable. We also schedule a walk-through of the DED with you before we start the deliverable. When a draft deliverable is ready, we will publish it to the project repository along with a meeting agenda and schedule a joint walk-through meeting. During the meeting, we will walk through the draft in its entirety and gather your comments. The objective is to identify any issues during the walkthrough, so we can address them before finalizing the document. This way, we can be sure that you are familiar and comfortable with the content of the deliverable prior to its formal submission.

The review cycle for deliverables may vary based on size and complexity. Each review cycle includes these steps:

- Develop the DED
- Walk through the DED with you
- Develop the deliverable (this varies depending on the complexity)
- Walk through the deliverable with you
- Revise the deliverable based on your feedback in the walkthrough
- Submit the deliverable to you
- A seven-day first review period (may vary depending on the complexity)
- A three-day Optum revision period (may vary depending on the complexity)
- Resubmit the deliverable followed by a walkthrough of how we addressed the comments
- A three-day second deliverable review cycle by you
- Resubmit the deliverable
- Deliverable approval by you

In general, we have found that a seven-day first review period works well for most of our state customers. This first review period is followed by a three-day revision period and then a redelivery of the deliverable. Following that is another three-day review period by you. We also include a deliverable walkthrough to introduce reviewers to the deliverable.

When you approve a deliverable, we will place the deliverable under configuration management control. Any subsequent updates to the deliverable must follow approved change control processes, and then will become effective only after appropriate DPHHS and Optum management approval.

We understand that deliverable review takes significant attention, and we are sensitive to the fact that you have other demands on your time. We will work with you to develop a mutually agreeable review schedule that minimizes schedule conflicts as much as possible. To the extent possible, we will avoid queuing excessive deliverables for simultaneous review. We will account for your SME time in the PWP to avoid problems with critical deliverable reviews coinciding with state holidays as soon as possible. During the planning stage of implementation, we will review the deliverable catalog and the deliverable review schedule with you, adjusting as necessary. Any resulting changes will be incorporated into the PWP and used to drive and report on project status.

PMT16 The Contractor shall provide deliverables that at a minimum meet the following quality standards:

a. Provide accurate and comprehensive content, reflecting the specific requirements for the deliverable.

b. Ensure appropriate technical level for the audience.

c. Utilize correct grammar, spelling, and versioning.

d. Ensure diagrams are clear, concise, and value added.

e. Follow industry-related standards.

f. Appropriately define and reference information.

We will apply our quality standards in developing deliverables and documentation for the Optum Provider Services solution. Our team will begin by creating a template or tailoring an existing template. We will customize deliverable content to specific project requirements and peer review the document to verify quality. User, technical, and system documentation, as well as project plans, status reports, correspondence, and other deliverables and documents will be maintained in file formats according to your requirements. All deliverables are subject to internal quality reviews prior to submitting to DPHHS. We will provide deliverables that meet the following quality standards at a minimum:

- Provide accurate and comprehensive content in each deliverable, reflecting the specific requirements for the deliverable. From producing the initial DED to accepting the final deliverable, both DPHHS and Optum personnel will conduct multiple reviews of each deliverable.
- All deliverables are reviewed for appropriate technical level for the intended audience. Many users do not have a technical background, so we provide deliverables that are appropriate for most audiences who lack technical backgrounds. For some deliverables, such as a logical data model or system architecture diagram, we assume the DPHHS reviews have the appropriate background to understand such documents.
- All deliverables are spell-checked and reviewed for correct grammar, spelling, and versioning.
- All figures and diagrams we include in a deliverable are subjected to internal quality review to verify the diagrams are clear, concise, and value added. Any diagram that does not meet our standards will either be upgraded to meet those standards, or will be removed from the deliverable.
- In general, we follow standards as defined in the PMBOK or other industry-related standards. One reason we produce a DED up front is so you can confirm our proposed deliverable format and content meets with your requirements and expectations.

We will appropriately define and reference information as needed within each deliverable. A key deliverable we will develop and maintain for the Provider Services module is the Quality Management Plan. This plan will describe the quality management activities we will perform using our defined processes and procedures.

Optum will use reviews and audits to validate quality within specific areas of the solution for the implementation, deployment, or ongoing services as needed. We will conduct requirements traceability for the Optum Provider Services solution requirements into our test cases and defects. We will verify our teams and Optum-engaged third parties adhere to our quality processes and relevant industry standards. Figure 3.28 shows how our implementation approach includes these quality controls and assurances.

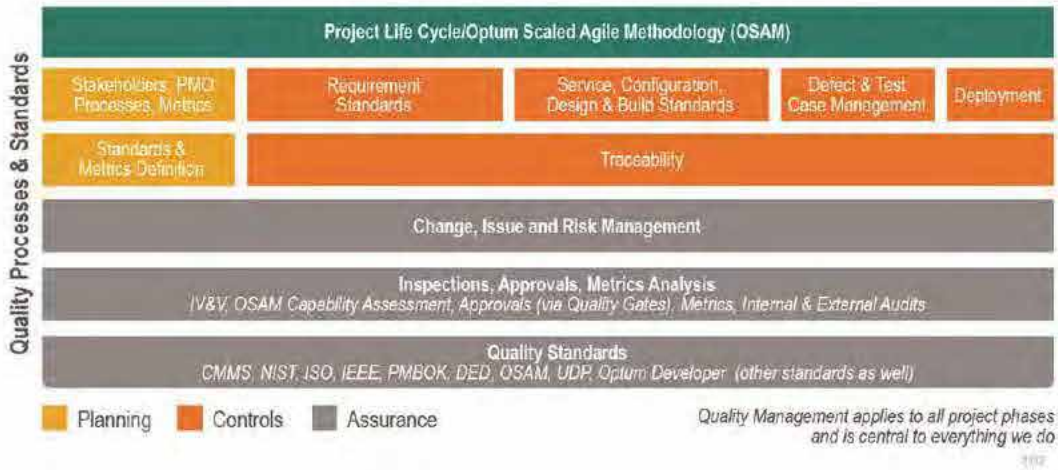


Figure 3.28: Optum Quality Processes and Standards.
We apply strict, consistent quality processes and standards across the entire project lifecycle.

We leverage quality best practices from PMBOK and standards from the International Standards Organization (ISO). We will monitor routine quality assurance measures to make sure daily activities adhere to quality guidelines. Our quality processes cover the major processes as defined by the PMBOK principles of quality planning, quality assurance, and quality control.

PMT17 The Contractor shall submit a monthly status report. The monthly status report must contain, at a minimum:

a. A complete set of updated and current output from the Project Work Plan along with a copy of the corresponding Project schedule files in electronic version.

b. A description of the overall completion status of the Project including schedule variations that report the earned value of the work completed, the planned value of the work completed, and the variance.

c. Planned tasks and activities for the next month.

d. The Deliverable status, with percentage of completion and time ahead or behind schedule for particular tasks.

e. Identification of any staffing issues or changes in the Resource Allocation Matrix.

f. An updated status on all issues being monitored.

g. An updated status on all risks being monitored.

h. Provide metrics necessary to support the State CIO's Legislative Finance Committee (LFC) reporting requirements.

i. Provide testing status and metrics.

j. Provide System enhancement hourly pool total hours used and total hours remaining.

k. An updated status on all SLA being monitored.

Optum will submit a monthly status report addressing all of the items required by the RFP. A key component of the Communication Management Plan is status reporting. As part of project control activities, we will provide weekly and monthly status reports and briefings to DPHHS throughout the life of the project. Both reports will include a dashboard of project health at various levels. Figure 3.29 shows the project health measures we will use.

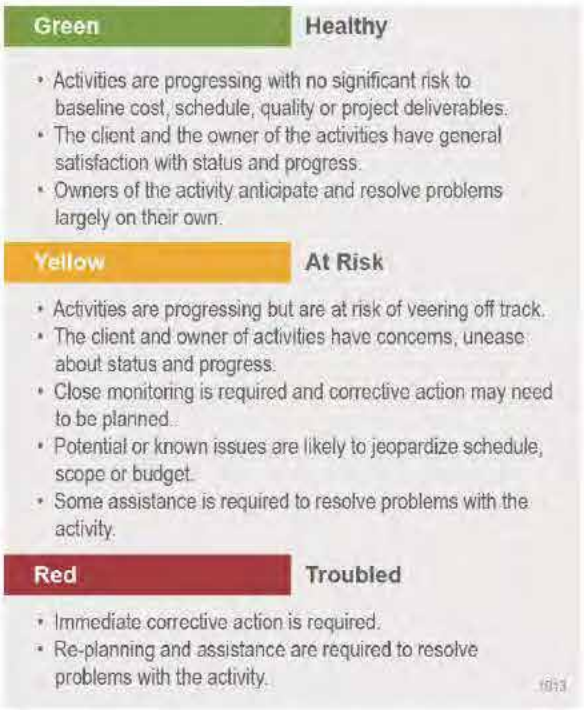


Figure 3.29: Project Health Status.
Our weekly and monthly Provider Services module status reports will include a dashboard of project health at various levels.

The Communication Management Plan will describe how Optum will work with you to produce weekly and monthly status reports and distribute them in your preferred format. The status reports will include information, such as the following:

- Executive summary that briefly describes project status and issues
- List of key activities, deliverables, and milestones completed for the previous reporting period
- Activities in progress
- Key decisions made or needed
- Status of cost, schedule, performance (quality, scope, technical, operations), staffing, and other pertinent metrics
- Cost Performance Index (CPI): Included in a supplementary report from the Earned Value Management System (EVMS) and an indicator of cost efficiency of the work accomplished for a specific period; will use the standard Project Management formula to derive this index
- Schedule Performance Index (SPI): Included in a supplementary report from the EVMS and an indicator of the schedule efficiency of the work accomplished for a specific period; will use the standard Project Management formula to derive this index
- Upcoming key tasks and milestones
- IMS-based look-ahead report and associated steps required to complete upcoming deadlines

- For operational components, achievement of performance standards for the month, and all performance standards that were not met
- Variance reports from the IMS showing tasks that are behind schedule or need escalation
- Planned corrective actions for activities not on schedule
- Risks, issues, and opportunities that must be addressed
- Resolved issues

Figure 3.30 shows a sample monthly project status report.

Provider Services Module Project

Monthly Status Report

Month Ending MM/YYYY

Accomplishments	Key Upcoming Activities
• **Project Oversight** - Deliverable status, milestones, key activities completed - CPV/SPV Earned Value - Testing status and metrics • **IRAAD-C** - Accomplishment #1 - Accomplishment #2 • **Key Decisions Made or Needed** • **Meetings Held** • **System Enhancement Pool** - Total hours - Total hours remaining • **Activities Planned for Next Month**	• *Insert commentary related to upcoming activities and target completion dates*

Color Status (Green, Yellow, Red)			
Scope	Schedule	Benefit	Quality
Green	Yellow	Green	Green
	Reason		

Key Upcoming Milestones (Next 4-6 Weeks)		Risks	
Action Item	Date	Key Risk	Mitigation Strategy
• Action Item #1	MM/DD/YYYY	• Risk #1	*Identify methods to reduce risk*
• Action Item #2	MM/DD/YYYY	• Risk #2	*Identify methods to reduce risk*
• Action Item #3	MM/DD/YYYY	• Risk #3	*Identify methods to reduce risk*

Overall Status Key: G | Y | R

OPTUM

Figure 3.30: Sample Monthly Project Status Report.

Optum will actively monitor and manage the Provider Services module and provide monthly project status reports to DPHHS.

PMT18 The Contractor shall develop and maintain a Project Management Plan (PMP): The purpose of the Project Management Plan is to provide a comprehensive baseline of what needs to be achieved by the project, how it is to be achieved, who will be involved, how it will be reported and measured and how information will be communicated with the project. It will serve as a reference for decision and clarifications. All relevant project plans including but not limited to the Communication Plan, Change Management Plan, Staffing Management Plan, Quality Management Plan, Risk Management Plan, Issue Management Plan and the Work Breakdown Structure are incorporated into the Project Management Plan. It is a living document that evolves as the project progresses and is updated with the latest relevant information as required. The Project Management Plan may be broken into separate documents, but all documents will be considered sections of the Project Management Plan.

Optum will implement a PMP that defines a project management (PM) approach and governance structure that accomplishes the following six core PM objectives:

1. Staff projects with the proper mix of personnel who bring the right qualifications to perform all of the required tasks
2. Deliver the solution and required project deliverables on time and within budget
3. Implement project communications and oversight
4. Deliver quality solutions that reduce errors and improve effectiveness
5. Perform appropriate risk management and internal controls
6. Maintain continuous process improvement through collaboration, surveys, and thorough customer communications

To guide the project, we will create a comprehensive PMP. The PMP and other planning deliverables will define the processes, methods, tools, and resources that we will use to manage project activities.

Our PMP 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. It will serve as a reference for decision and clarifications. All relevant project plans are incorporated into the PMP as component sub-plans. Our PMP will be a living document that evolves as the project progresses and updated with the latest relevant information as required. We break the PMP into separate documents, but all documents are considered sections of the PMP.

We manage an existing library of project planning documents and templates that may be tailored. We will work with you to confirm the content of the PMP and related planning deliverables meet your project requirements. The PMP, PWP and other planning deliverables will serve as the roadmap to coordinate project activities for timely implementation. They will reflect our Optum Delivery Model and include the tasks, milestones, and deliverables necessary to fulfill requirements and deliver the Optum Provider Services solution successfully.

Our project management methodology adheres to the PMI project management standards and is applicable throughout the contract term. The following sections describe the sub-plans we will deliver as part of the PMP.

Communication Management Plan

The Communication Management Plan provides an overall framework for managing and coordinating the wide variety of communications that directly or indirectly take place as part of the Provider Services module. The Communication Management Plan will specify the methods of communications across DPHHS, Optum, and other project stakeholders. It addresses communicators, audiences, messages, communication channels, feedback mechanisms and message timing, and creates a mapping between them. This framework will make sure the Optum team provides relevant, accurate, and consistent project information to DPHHS and other stakeholders in a timely manner. Effective communication creates a bridge between diverse stakeholders who may have different cultural and organizational backgrounds, different levels of expertise, and different perspectives and interests that affect or influence project execution or project outcome.

As part of the PMP, the Communication Management Plan is an evolving document that will be revised when appropriate throughout the life of the project. This plan defines the communication requirements for the project as well as how and when the information is to be distributed. It supports the Stakeholder Management Plan in that it will help the project team manage stakeholder expectations and prevent unwarranted communications.

Effective communication is critical to the success of a project. For this reason, the Communication Management Plan is viewed as one of the key project management sub-plans. This plan will:

- Highlight the importance of effective communication and its impact on the execution of the project
- Identify mechanisms to deliver these key messages
- Establish a formalized structure to sustain communications over the long term

Change Management Plan

The Change Management Plan provides an overall framework for managing and coordinating change requests to the Provider Services module in an organized manner. This plan will:

- Define the change control process in detail
- Discuss how the DPHHS and Optum will work together to start, track, prioritize, and authorize change requests
- Describe the tools we will use to track and communicate change requests
- Address the method for documenting various types of change requests from the project sources authorized to request change
- Outline the notifications and authorizations required before a change will be placed in production

Our objective for change control is simple. It will effectively manage and control project scope. As a result, it will contain project costs and schedule.

Staffing Management Plan

The Staffing Management Plan defines the process we will use to staff the Provider Services module throughout the project lifecycle. This plan describes how Optum will staff the project and maintain compliance with all staffing requirements set forth in the RFP, addressing requirements regarding personnel, resources, and contractor staffing.

Quality Management Plan

The Quality Management Plan outlines the process for continually monitoring and verifying that established quality standards are met throughout the duration of the Provider Services module. The Quality Management Plan documents the processes, evaluation steps, procedures, and tools will we will use to determine that project deliverables meet their stated requirements and that project management processes are consistently followed to maintain project quality, meeting or exceeding DPHHS and stakeholder expectations.

Risk Management Plan

The Risk Management Plan defines the processes we will use to plan for, identify, analyze, respond to, monitor, and control risk for the Provider Services module. It focuses management attention on major issues that threaten the success of a project. Risk management is accomplished in parallel with financial, schedule, quality, and requirements management. It seeks answers to the following questions:

- What concerns exist about the success of the project?
- What are the effects for the overall project if these concerns materialize?

- What actions will reduce the chances that these concerns will materialize?
- What can be done if these concerns materialize?
- What will Optum management need to do if these concerns materialize?
- What will DPHHS need to do if these concerns materialize?

All projects have risks, regardless of their size, nature, or contract type. Without a well-defined risk management approach, project team members may deny and avoid the very issues that should receive the most attention. Identifying project risks, developing a plan to avoid or mitigate risks, and developing contingencies can make the difference between project success and failure. The Risk Management Plan will address the process and procedures for identifying and managing issues that escalate to the status of risk, and the management of issues initially identified as a risk.

Issue Management Plan

The Issue Management Plan provides a framework for managing and coordinating issues that Optum and the DPHHS identify during the project. This plan will help us:

- Validate that we identify, evaluate, and assign issues for resolution
- Verify that we use the change control process for issues that affect project scope, costs, and/or schedule
- Confirm that we document and communicate issues appropriately to stakeholders in a timely manner

This plan follows project management best practices for managing risks and issues using tools, such as IRAAD.

Schedule Management Plan

The Schedule Management Plan describes how Optum develops, baselines, updates, and reports against the Provider Services module schedule, which includes the PWP and Work Breakdown Structure (WBS). It also defines the processes for modifying the schedule to reflect actual progress against planned efforts, applying updates resulting from DPHHS approved changes in requirements and resource allocations. This deliverable defines the process required to maintain clear lines of accountability and will define the format and content requirements for variance reports that highlight major differences between the previously approved baseline version and a recalculated forecast.

PMT19 The Contractor shall develop and maintain a detailed Project Work Plan (PWP) and a Gantt Chart that is aligned with the scope of the work outlined in this RFP. The PWP must identify realistic person hours of effort for each task and identify planned completion dates for all deliverables and milestones. Additionally the PWP must include the elements necessary for the IMS include: start and end dates of major phases, key project milestones, integration points, cross module dependencies, and sufficient information to support the State CIO's Legislative Finance Committee (LFC) reporting requirements. The PWP must be continually refined and updated as the project progresses and will retain the baseline for comparative reporting.

We will develop and maintain a detailed PWP and a Gantt chart that aligns with the scope of the work outlined in this RFP. To accomplish this, we will develop a detailed Schedule Management Plan that defines the processes, roles, and responsibilities according to the work plan that reflects the schedule, effort, duration, and resources required to complete the project as defined in the RFP. We will base the Provider Services module detailed project schedule on our proven methodology and our understanding of the RFP requirements. The schedule will include key

milestone dates along with critical path analysis to understand tasks that we cannot move without affecting milestone dates.

Using our PMO templates and standards, we will manage the IMS in Microsoft Project throughout the project. We will integrate the IMS with the project management team activities. Figure 3.31 shows our steps for developing the IMS that will guide our project planning activities for the project



Figure 3.31: Integrated Master Schedule Development.
We will follow a five-step process for developing the Integrated Master Schedule.

We will create a detailed project schedule baseline at the end of initial project planning and deliver it to you. We will monitor all variations in the schedule against this baseline and only revise the baselined project schedule through approved change control procedures with appropriate DPHHS and Optum management. Together, the PMP, detailed project schedule, and other planning deliverables will serve as the roadmap to coordinate project activities for timely implementation.

Optum will develop a preliminary PWP that addresses the requirements and timetable of the project. All tasks in the work plan integrate with one another so each task has a predecessor/successor relationship with those tasks upon which it depends. A single milestone at the beginning of each work plan, "WBS 1.1—Contract Signed/Project Start," serves as the focal point for controlling the overall time frames calculated in the work plan. It is based on our real-world experience building systems for many state and commercial clients.

During DDI, we will work with you to refine the PWP as we further break down the activities and understand your detailed requirements. When the PWP is agreed upon, we will baseline and maintain it under strict change control. The PWP will be published to the project SharePoint site weekly in cadence with the Weekly Status Report. We will also work with you and your IV&V contractor to establish the necessary task reporting to track any tasks in danger of causing a schedule delay. We have experience in integrated schedule management and working in environments with state agencies, vendors, subcontractors and other partners on numerous projects. A PWP is essential for the successful realization of your enterprise vision. Our PWP will properly account for holidays and out-of-office time for DPHHS and Optum resources as early as possible so potential delays to deliverable reviews and testing can be resolved before the project is delayed. Our PWP will also clearly flag State activities and indicate major milestones.

A viable work plan provides a step-by-step blueprint to accomplishment of individual tasks, integrating those tasks to understand critical path and key interrelationships to verify overall project success. Our work plan brings together our long-term domain knowledge, a detailed technical solution, and common-sense management approaches. The plan will be a living document across the project lifecycle. We will update it as required to reflect any change driven by legislative dynamics, State requirements, technology evolution, or lessons learned.

We use Microsoft Project, an industry-standard project management tool, to develop and maintain the PWP. Microsoft Project enables us to track the progress of the project, monitor and evaluate resource allocation, and produce work plan reports that include the following:

- Project schedule

- Milestone dates
- Deliverable dates
- Gantt chart

Additionally, we will produce ongoing reports using Microsoft Project to include in the overall status reports that are provided to DPHHS. This will help confirm that all parties remain updated on the overall progress of the project. It will also make sure all parties are promptly made aware of any areas where project schedule slippage may occur.

PMT21 The Contractor shall coordinate with the Department and with the module vendors as required by the Department, to support the program-level change management process consistent with the Enterprise Change Management Plan.

Optum will coordinate with DPHHS, SI vendor, IV&V vendor, and with the module vendors to support the program-level change management process consistent with the Enterprise Change Management Plan. We use the PMBOK, as published by the PMI, to define a project scope change management system as the procedures by which project scope and product scope can be changed. Our system follows this methodology and includes the documentation, tracking systems, and approval levels necessary for authorizing changes. Experience has taught us that consistent and well-defined procedures and commitment to formal change management are critical to delivering projects on schedule and within budget.

Change is a common occurrence in the project lifecycle, especially in complex, state-of-the-art system configuration and business process implementation projects, such as this project. As you are well aware, change management is critical to control project schedules, cost, and quality, and ultimately to deliver services that meet your requirements and satisfaction.

Figure 3.32 provides an overview of our change management process.

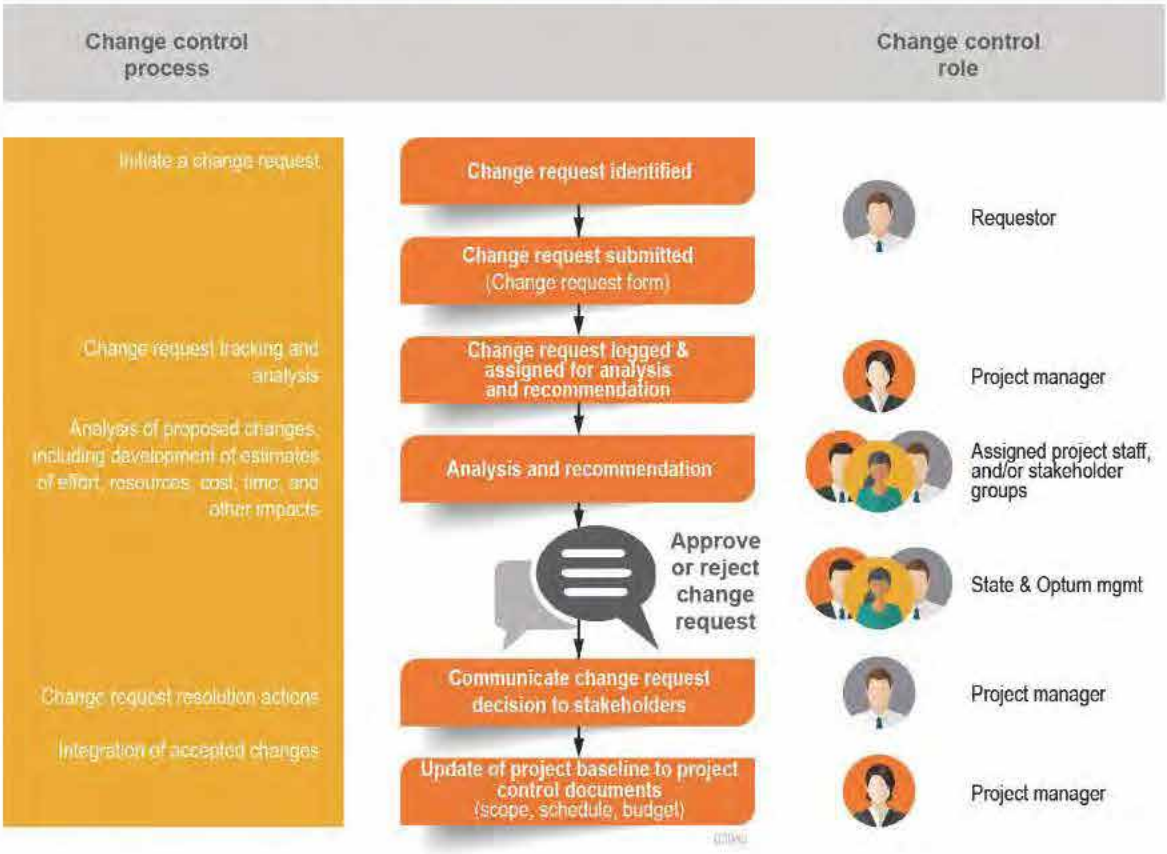


Figure 3.32: Change Management Process.
We will collaborate with you to make sure our process aligns with your requirements.

Change to system software, application software and system hardware will be subject to the approved change management process. As is customary for change management processes, we will evaluate and analyze proposed changes, including developing estimates of effort, resources, cost, time, and other influences. This information is critical for the approval and prioritization processes, all of which we will collaborate with you to attain approval.

The change process starts with a need for change being identified, supported by the change request form. We will use HP ALM to help record, track, and communicate the change request information to project stakeholders. During DDI, we will capture requirements in HP ALM, and then tie change requests to the appropriate requirement in the RTM. This helps all parties understand when changes affect requirements as originally specified. This also indicates that during DDI, change management is closely tied to scope management. During DDI, it is important to avoid scope creep by identifying change requests that are outside the original scope of the contract. We will then work with you to review an approved process for addressing out-of-scope changes. We have been very successful in managing project scope during DDI and look forward to doing the same for you.

The design, development, testing, and implementation of approved changes and enhancements will follow the agreed-upon development and testing processes detailed in our project management approach.

The process for working change requests is divided into multiple steps with some steps repeating. The following table outlines the repeatable process that helps us verify that we do not miss a step in working a change request for our solution.

Step	Description
1.	The requestor creates the change request. A change request may be a result of a help desk inquiry, an issue, a COTS upgrade, or an information-only item. Ongoing changes and unanticipated changes are communicated to us through the change control process. A change request is determined to be a: • Change in business process • Solution software or configuration change • Non-compliance change • Information change
2.	We receive the change request and update the HP ALM COTS tool. Optum initially evaluates the change request and determines or validates the type of request. We then assign a priority of High, Medium, or Low to the change request. There is a fourth priority of Urgent. Urgent is considered a showstopper, and it will follow an escalation path approved by the State based on the terms of the contract.
3.	We prepare an estimate, impact analysis and resolution for the change request. This does not apply to the change request received as Information Only or for Comments Only.
4.	During the project status meeting, we will complete the following tasks together: • Review new change requests • Review estimate, impact analysis, and come to resolution • Set priorities and authorizations to proceed on change requests • Review, act on and approve change requests for closure • Review implementation releases (post) If we receive a new change request at the status meeting, we process it by completing these steps, beginning with Step 1.
5.	We document change request as approved to proceed.
6.	We assign approved change request to our staff for completion. We verify adequate scheduling, testing, and notification.
7.	For a completed change request, we assign a close date in HP ALM and notify stakeholders as appropriate of the instituted change.

We track and manage change activity to the IT environment, application, and infrastructure through our change management process. The change requestor will document activity related to the change, including pre-implementation testing, implementation, validation, and back-out plans. The risk of each change is assessed automatically, using our configuration management database to determine potential impact, and historical change performance data, to determine the likelihood of unplanned impact occurring because of an activity. This risk then drives the level of scrutiny and approval required before we can implement the change.

PMT25 The Contractor shall be required to work collaboratively with the Department and the System Integrator to provide schedule information to be included in the Integrated Master Schedule (IMS). Elements necessary for the IMS include; start and end dates of major phases, key project milestones, integration points, cross module dependencies, and sufficient information to support the State CIO's Legislative Finance Committee (LFC) reporting requirements.

We will work collaboratively with the DPHHS and the SI to provide schedule information to be included in the IMS. Developed in Microsoft Project, our PWP will include all of the tasks necessary to effectively implement our solution for the State. We will work collaboratively with the SI as necessary to incorporate tasks from our PWP into the overall IMS.

We will begin with an existing library of project planning documents and templates. During the Planning Phase, we will work with you to tailor the PMP content and the related planning deliverables to meet your requirements. The PMP will align to our PWP and identify required project deliverables.

PMT27 The Contractor shall coordinate module deliverable and milestone walkthroughs and participate in other module walkthroughs as required by the Department.

Optum will coordinate module deliverable and milestone walkthroughs and participate in other module walkthroughs as required by the DPHHS. Our review cycle for deliverables may vary based on size and complexity. Each review cycle includes the steps we detailed in our response to PMT15.

We conduct walkthroughs of both the DED and the initial version for each deliverable, as applicable. This approach makes certain that our deliverables align with your requirements and provides you the opportunity for correction if a deliverable does not meet your expectations.

PMT29 The Contractor shall submit a monthly System Enhancement Pool report that details tickets invoiced to the hourly pool and must include hours used and hours remaining for the Department's approval.

Optum will submit a monthly System Enhancement Pool report that details tickets invoiced to the hourly pool and includes hours used and hours remaining for DPHHS's approval. This will include the allocation of the following:

- **DDI Base Scope of Work:** 1,500 system enhancement pool hours for the duration of the DDI phase of the contract
- **DDI Option A Scope of Work:** 500 system enhancement pool hours for the duration of the DDI phase of the contract
- **DDI Option B Scope of Work:** 250 system enhancement pool hours for the duration of the DDI phase of the contract
- **Operations Base Scope of Work:** 500 system enhancement pool hours during the Operations phase per operations year
- **Operations Option A Scope of Work:** 100 system enhancement pool hours during the Operations phase per operations year
- **Operations Option B Scope of Work:** 100 system enhancement pool hours during the Operations phase per operations year

Optum personnel will be available to review the System Enhancement Pool report with the DPHHS, or to address any questions or concerns the State may have on any report.

The cost of system enhancement pool hours are included in our fixed price and included in Schedule D-Enhancement Pool Hours. The System Enhancement Pool includes personnel cost for all resources supporting the system enhancement effort. The unused system enhancement pool hours for DDI or a given operations year will be rolled over to the system enhancement pool for Operations or the next operations year. Alternatively, the number or system enhancement pool hours may be adjusted downward, at the discretion of the DPHHS.

PMT31 The Contractor shall cooperate with the State's PMO and the IV&V contractor to give an accurate, honest reporting of the project status.

Optum will cooperate with the State's PMO and the IV&V contractor to give an accurate, honest reporting of the project status. We will update our PWP weekly and provide the scheduled status reports to you detailing the project status and health. Optum will attend weekly and

monthly status meetings with you to review current project status and to address any issues affecting project progress. Our contract manager or project manager, or their designee, will attend status meetings with the DPHHS. Our goal is to have open and honest communication across all parties concerned so the project objectives of the DPHHS can be met.

PMT32 The Contractor shall contribute to the State's and/or the Systems Integration Services collaboration site, technical and non-technical project artifacts for the Contractor's module or module components including requirements, use cases, user stories, storyboards, system design documents, supplemental specifications, test cases, test scripts, test results, user, system and training documentation at the State's direction.

Optum will contribute to the State's and/or the Systems Integration Services collaboration site appropriate technical and non-technical project artifacts for our solution components. This can include requirements, use cases, user stories, storyboards, system design documents, supplemental specifications, test cases, test scripts, test results, and user, system, and training documentation as directed by the State. We will store these artifacts in the dedicated project document repository that we will establish and maintain for the Provider Services module documentation and artifacts. The SharePoint repository will be available at the beginning of the project and throughout the life of the project. We will organize documents and artifacts in the repository in support of CMS certification milestone reviews. Optum will work with you to establish a process for routing project documents, deliverables, and other Optum work products to and from our Provider Services module document repository to you.

3.10.2.2 System Development Methodology

The Contractor will be expected to follow an industry-standard systems development methodology for the initial implementation of the proposed solution and throughout the Contract term. The Offeror must propose a System Development Methodology approach that achieves the expected outcomes of the SDLC-based activities stated below.

OSAM is our proven SDLC. This framework provides early and continuous delivery of quality, fully tested software. Our SDLC methodology incorporates lessons learned, development tools, and templates from our experience delivering HHS projects. The methodology provides a roadmap to produce a stable, sustainable system while reducing project risks that affect budget, schedule, and performance.

OSAM follows the PMI project phases of Initiation, Planning, Execution, Control, and Close. Within the Execution Phase, OSAM will include the activities for configuring, testing, and implementing the solution iteratively. An output of the OSAM activities is the Model Office environment, as described below. This Agile approach is in stark contrast to traditional MMIS projects, where teams develop solutions to meet DDI requirements using a waterfall methodology. Using waterfall, each phase has a defined beginning and end, and a phase only begins when the previous phase ends.

OSAM's rigorous adherence to defined phases, continuous improvement, and lean Agile principles will reduce risk and speed delivery for the solution. Lean software development emphasizes values, such as eliminating waste, building quality early, delivering quickly, and respecting people. OSAM offers flexibility in adjusting the number and length of Program Increments (PIs) to details gained during discovery and initiation, methodology maturation with lessons learned, and DevOps maturation.

As we configure the solution, we will use the DevOps application configuration model. DevOps is an innovative approach to software code management, configuration, and deployment that reduces risk and speeds solution delivery. With a strong emphasis on automation, it promotes collaboration and communication between the development and technical operations teams. DevOps is an important element of our OSAM SDLC.

OSAM offers the following key advantages for the DPHHS:

- Reduces delivery cycle time
- Raises the quality of developed solutions
- Improves the predictability and quality of the deployed releases
- Increases the productivity of overall development organization
- Provides transparency into our project health for the stakeholders
- Encourages higher resource engagement in deployment process

OSAM incorporates Lean Software Development principles and values. It fosters engineering excellence and takes teams and solutions to the next level of Agile maturity. Figure 3.33 illustrates our OSAM SDLC.

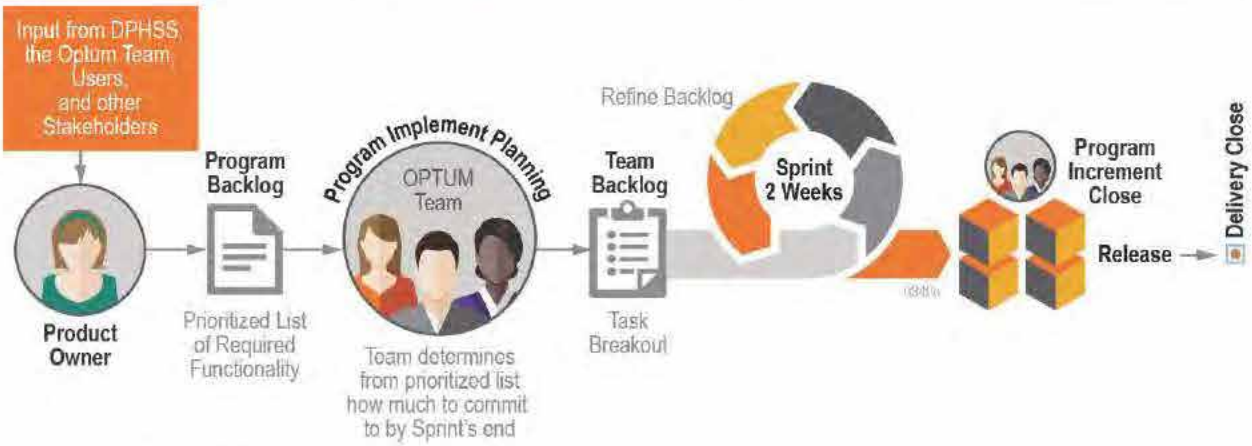


Figure 3.33: OSAM SDLC.
OSAM will enable us to provide early and continuous delivery of a quality, fully tested solution for the DPHHS.

Delivery initiation for the Provider Services module begins with a program backlog, which is a list of the DPHHS requirements written as a list of prioritized capabilities and features defined by the DPHHS and Optum product owners. The program backlog is a single, definitive repository for all future work that will advance the PIs, otherwise known as a release. A PI will comprise three to five two-week sprints and one Hardening, Innovation, and Planning (HIP) sprint, depending on the length of the PI. The HIP sprint includes activities, such as completing the PI testing activities, the next PI Planning event, and demo for the work completed in the PI.

The project team will review the criteria detailed in the program backlog and create strategies to configure and deliver all solution features according to these criteria. The project team members will then conduct the first PI Planning event.

The first PI Planning event will occur before the first PI and the follow on PI Planning events occur during the HIP sprint. Using the prioritized capabilities and features in the program backlog, as well as the list of project schedule milestones to meet during the PI, the project team will create the team backlog, which contains the detailed user stories and tasks for the selected capabilities and features they must meet during the PI. After defining an executable plan and committing to the work, the project team will begin sprinting for that PI.

The project team will complete the two-week sprints to configure, test, and release working software according to the team backlog specifications and the PI milestones. The goal of this stage will be to deliver working software frequently. The project team will complete this work on a fast, predictive, synchronous cadence, and we will conduct sprint reviews.

While sprinting is underway, the project team will continuously update the detailed plan for the next PI and refine the backlogs. When planning and backlog work are complete, and the current PI moves to the HIP sprint, the project team will prepare to hold the next PI Planning event.

During the HIP sprint, the project team conducts PI Close activities. The project team will demonstrate to key stakeholders the solution software package released during this PI. The project team will load the released software package into the Model Office environment for validation and approval in the Model Office sessions, while the released software package also undergoes additional testing phases. The team will conduct a lessons-learned exercise to improve performance over time. After the HIP sprint and PI Close activities are complete, the next PI will begin.

After we complete all six initial configuration PIs, the completed software will enter two additional PIs focused on subsequent testing phases and defect fixes before implementing into a production environment for go-live and the beginning of operations.

Delivery Close occurs for the Provider Services module when the Implementation Phase is complete. The Implementation Phase will complete after the program transitions into operations and system certification is successful. During this phase, we will complete the final traceability review of released deliverables to make sure they satisfy your requirements.

The Implementation Phase and ongoing O&M Phase will overlap from the go-live date through successful system certification. After successful system certification, maintenance and operations team will operate the project through the rest of the contract period, including the remainder of the date of service cutover.

Model Office

A successful implementation is more than a system configuration. It is the realization of mutually dependent business processes that use services to achieve your requirements.

During the Discovery Phase, we will clone the baseline infrastructure to establish the environments and hosting solutions. The Optum Model Office and technical teams will use available sources of the DPHHS requirements to compare the source documentation against the DPHHS requirements. The teams, using the MECT checklists and MITA Framework, will document requirement matches, configuration, and/or customization for each module. This effort will include requirements to support the proposed date-of-service cutover conversion.

Using the outcome of the analysis, the Optum Model Office and technical teams develop level-of-effort estimates for any non-matching requirements to refine the project schedule and inputs into the OSAM process. The Optum technical teams also review and document the system design and architecture as required, such as in the Systems Engineering Management Plan (SEMP).

We will then use the information from this initial analysis to configure the environments, including the Model Office environment, to represent the available the DPHHS requirements. These environments will serve as the basis for engagement with DPHHS to validate and conduct knowledge transfer.

Our Model Office approach will provide the DPHHS with the platform necessary for our project teams to work together in collaboration and deliver the right business solutions, at the right time, solving complex business opportunities.

Our Model Office approach will bring the following advantages and features to the DPHHS:

- Provides business stakeholders and process SMEs the opportunity to become familiar with the product and associated operational processes in the second month of the project, enabling Optum to identify any unknown gaps early in the Implementation Phase
- Drives organizational engagement and adoption of the new solution through early involvement
- Gives the DPHHS early access to the solution, reducing the learning curve and better positioning users for a smooth transition to operations
- Provides an environment that regularly fosters demonstration of the solution to a wide audience

- Uses visual and functional prototypes to facilitate collaboration and validation of project requirements, rather than traditional offline or documentation-based reviews
- Significantly reduces risk through proof of concept-driven configuration
- Preconfigured solution kept through the iterative releases, enabling the DPHHS to preserve the Modification Pool to focus on emerging programmatic requirements rather than federal compliance and provides regular sprint reviews and release demos during sprints and releases

Optum SMEs will conduct Model Office Business Scenario walkthroughs of how the solution addresses the DPHHS' requirements for given capabilities. For example, we can begin a walkthrough with a workflow artifact similar to Figure 3.34.

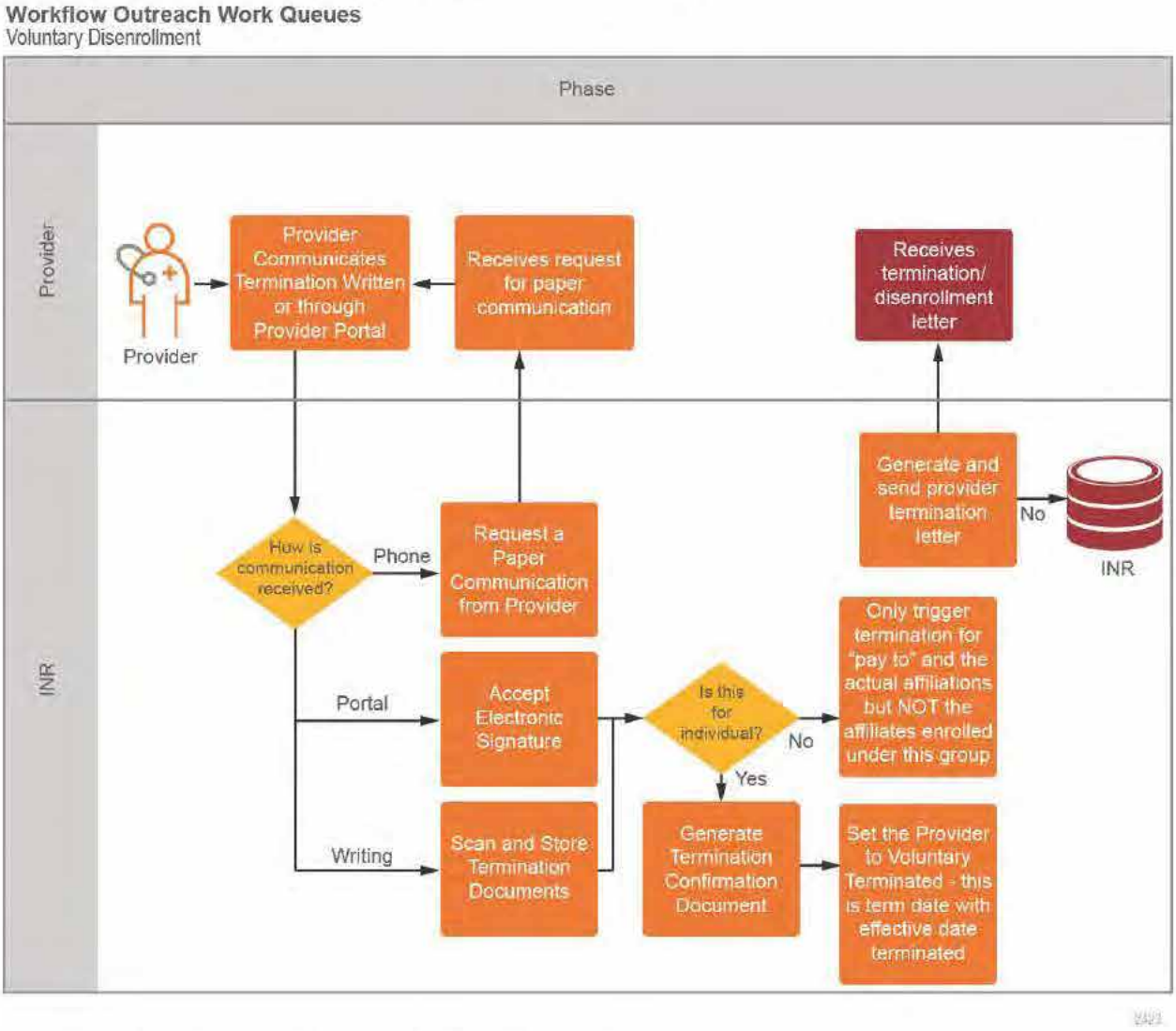


Figure 3.34: Sample Workflow for Model Office Walkthroughs.
Optum SMEs conduct Model Office Business Scenario walkthroughs of how the solution addresses the DPHHS' requirements for given capabilities using artifacts, such as this sample process workflow.

Artifacts like this one begin a collaborative discussion of how the Optum core configuration will interact with all stakeholders. We design these documents to illustrate the people, processes,

and technology we use to achieve the desired business outcome. The primary goal is to understand each step of the process clearly, evaluate if the initial configuration of the system supports the desired outcome, and define the participants required to complete the process. This practice will help us gain the DPHHS buy-in to the functional work stream, eliminate any unnecessary customizations, and initiate detailed analysis of any identified gaps.

Three complementary Optum teams work in parallel to support the Model Office: Model Office team, Data Conversion technical team, and Interfaces technical team.

Model Office team: Optum business and technical team members who work the following functions:

- **Constituent services:** Includes capabilities, such as provider and State portals, call center support, data files, and dashboards and reports
- **Provider enrollment and management:** Includes capabilities, such as enrollment, eligibility, maintenance, monitoring, suspensions/pay holds, reactivations, disenrollment, appeals, provider and State support, data files, training and outreach, and dashboards and reports
- **Enabling services:** Includes capabilities, such as EDI, fulfillment services, in/outbound mail services, and operational reporting

Data Conversion technical team: Responsible for the conversion of critical data of service cutover data necessary for the operations of the solution, which involves:

- Setup and configuration of the data conversion framework
- Coordination with all DPHHS and third-party data sources
- Data profiling
- Source system data extraction
- Data cleansing and transformation
- Target system data loading
- Testing, verification, and reporting

Interfaces technical team: This team is responsible for the configuration of existing internal and external interfaces and, where necessary, design and development of new interfaces to enable the SaaS and BPaaS components of the solution.

As we begin managing your new environment, the results of the process will guide our design and development efforts. Using the initial configuration completed in the Model Office environment, Optum will engage with key the DPHHS and third-party SMEs to conduct a validation of the configured solution in the Model Office environment. Our strategy helps users gain exposure to our solution earlier and provide their critical feedback sooner in the development process.

Our model provides a validation process that invites resources from all interfacing applications/interfaces to verify their respective application functionality and confirm that interactions with each functional area within the solution are working as intended. Users will view a live, working version of the solution and the user interfaces we are developing and testing. We will gather your feedback, update configurations tailoring to your needs, and then review the updates with you. We will continue this iterative process until we reach agreement

that the solution meets your requirements. This approach gives us the opportunity to incorporate key findings up front.

Prior to a release, we will create a deployment package and track approvals throughout the promotion path, documenting approvals from the application owner, release manager, and business stakeholders. The primary objective of the validation phase is to support project discovery activities between the DPHHS and Optum through high-level training activities and requirements validation sessions. The goals of this stage can be defined as:

- Improving our understanding of the DPHHS Medicaid Enterprise and how the product will integrate with the enterprise
- Improving the DPHHS' understanding of the product by providing overview training and functional demonstration against requirements
- Providing opportunities for refinement of the DPHHS enterprise strategy and enterprise IT strategy while maintaining full compliance with CMS's Seven Conditions and Standards

Model Office Work Flow

We will feed any updates needed to the initial configuration into the OSAM process to make the adjustments. After each PI/release, we will provide a demonstration for stakeholders to review the work completed in that PI/release and provide feedback. We will continue this iterative review process until we reach agreement that the solution meets the DPHHS' requirements. Figure 3.35 illustrates the Model Office review process.



Figure 3.35: Model Office Review Process.
OSAM will enable us to provide early and continuous delivery of a quality, fully tested solution for the DPHHS.

As new requirements are discovered, we will document them using our requirements traceability tool and update the RTM deliverable. The updated RTM will become the basis for traceability throughout all stages of the project.

While the Optum Model Office approach brings great flexibility to the DPHHS, the project governance and discipline channels the flexibility to deliver the required capabilities timely, with quality. Our project leadership team will work with you to provide regularly spaced project deliverables and orchestrate functionality reviews and approvals to keep the implementation on time.

Our Model Office approach will provide the DPHHS the platform necessary for our project teams to work together and deliver the right business solutions, at the right time, to solve complex business opportunities.

Delivery Initiation

In addition to the discovery activities previously mentioned, the program backlog is being reviewed, revised, and prioritized. Thus, the capabilities and features are placed into one of the PIs for the Implementation Phase.

For each release, the Model Office teams will create the necessary requirement and solution/design artifacts to support each MMIS service and execute the supporting analysis, configuration, non-disruptive customization, and test activities. Starting in Release 4, the Optum business and operational teams will begin creating and/or updating operational support documents, such as training, desktop procedures, and user support documentation.

Program Increment Planning Session

With the Delivery Initiation kick-off, we will write the initial requirements found in discovery, including the benefit configuration grid, into capabilities, features, and user stories. During the first PI Planning session, our project leadership team will review, prioritize, and schedule the features and user stories into a PI.

As appropriate, the PI Planning session will also include features and user stories for incorporating incoming product releases. These product releases are expected monthly. When a product release is merged, separate regression testing will occur to validate the stability of that product release with the DPHHS configurations before incorporating it into the solution.

During user story writing as well as ongoing PI Planning, we will document requirements using our RTM and update the RTM deliverable. The updated RTM will become the basis for traceability throughout all implementation phases of the project.

Sprinting

During sprinting for a PI, the technical teams will use the user stories to complete configuration activities. For example, the user stories for the benefit grid/benefit plans will configure what is already built into the base product to support the DPHHS-specific needs, such as member aid codes, pricing, and programs. The Optum technical teams will also review and document the system design and architecture where necessary. We will document the solution design in the SEMP and other design documentation.

While the base product undergoes configuration, the Data Conversion and Interfaces technical teams will load converted and interface data that support the sprint's user stories. This data will be de-identified prior to making the data available for teams to use as part of testing or Model Office activities.

While we expect some customization, primarily for interfaces, the project solution is already designed and developed, and will now require only configuration of the DPHHS specifics to operate.

As configuration completes, the user stories' acceptance criteria will be used for testing. During sprinting, we will perform unit, smoke, regression, and integration testing. The smoke and regression tests will be culled from the base product and tailored, as necessary, to support the configured solution.

Ongoing PI Planning

While sprinting activities are underway, the backlogs for future PIs undergo refinement and prioritization in preparation for the next round of PI Planning. We will add additional features and user stories to include any items identified as part of the SEMP.

Hardening, Innovation, and Planning Sprint/PI Close

During the HIP sprint/PI Close, the Model Office teams will demonstrate the configured solution that results from the PI activities to the DPHHS and identified stakeholders.

As part of PI Close, we will promote the configured solution to the next environment for product acceptance testing, our internal acceptance testing. We will also use this configured solution in Model Office sessions for ongoing requirement validation and/or clarifications. Where additional configuration or changes are identified, these changes will incorporate into the Ongoing PI Planning and feed into the next PI Planning session. Then the process starts over again, until all releases are complete.

When the entire solution is configured to the DPHHS' requirements and integration and product acceptance test are successfully completed, additional testing will begin.

Go-Live/Implementation

When testing is complete, and joint agreement is acknowledged between the DPHHS and Optum to proceed with go-live, Optum will deploy the final PI into the production environment. We will use deployment controls that track and document approvals from the application owner, release manager, and business stakeholders. These controls give us a validation process for interfacing applications and interfaces to validate their applications function correctly and work as intended post-deployment.

We developed a comprehensive checklist of activities to promote low-risk deployments. The checklists promote a controlled and repeatable release process. The following table describes the deployment checklist in more detail.

Deployment Checklist	Description
Operational Readiness Verification	Hardware, software requirements, and design documentation, pre-production testing (including unit, integration, UAT, and Initial Operating Capability [IOC]), and validation, conducting necessary load and stress tests, and SLA compliance
Configuration Management	Rules configurations, code, database scripts, and other artifacts checked in/tagged for release, including executable and documentation artifacts - requirement specifications, user stories, architecture documents, object models, and scenario diagrams
User Guide and Training	Issue online guides and conduct online/classroom training to help clinician and technical staff for using and operating the system; all necessary training completed prior to rollout
Customer Communication Plans and Change/Release approvals	Governs stakeholder communications, including executive management, development and operations teams, users, and change/release management committees with necessary approvals in place prior to release/deployment
Help Desk Communication and Training occur	Conduct training for help desk staff regarding the system and issue help aids and scripts describing how to fix and escalate issues when they occur
Rollback Plans	Issue detailed plan for rolling back releases, if the rollout does not go as planned
Disaster Recovery and Business Resumption Plans	Detailed disaster recovery plan developed, tested, communicated, and accepted, including restoring access controls, databases, and other services

Deployment Checklist	Description
Post-deployment Validation/Approval for Operational Start	Conduct validation of system to verify deployment is complete and ready for operational use

After go-live/implementation, the OSAM processes will continue to support release stabilization and certification achievement.

Delivery Close Phase

At this point, the Delivery Close Phase begins. We will manage the ongoing operations activities through the Maintenance and Operations processes and procedures.

Optum will evaluate and convert data into current, industry-standard formats whenever possible.

3.10.2.3 Requirements Management

The Contractor must work with the DPHHS MPATH Team to confirm the Contractor's understanding of the RFP requirements and to reconcile the RFP requirements for the scope of work against the proposed solution. The Offeror must describe their approach to meet each of the detailed Requirements Management requirements defined in Attachment F, Requirements Matrix.

We follow a mature requirements management approach to verify that our solution adheres to the RFP requirements and project scope of work while accounting for any variances. Our approach includes activities for requirements planning, validation, traceability, and control.

Requirements Planning

Our requirements planning strategy for our solution is to work with you to align your departmental objectives and requirements with our COTS-based and MITA-aligned solution. Throughout the project, we will perform rigorous quality checks and testing to make certain that the solution performs to specifications. We will apply our PMI-based methodology and proven approach to methodically and systematically design, configure, and implement our solution.

As we developed this proposal, we loaded your RFP requirements into the HP ALM COTS requirements management tool and traced the requirements to their related RFP response and proposed solution. This approach will help us verify our teams and any Optum-engaged third parties adhere to your requirements and any specified, relevant industry standards. We will load any changes to the requirements into our RTM tool as part of the Planning Phase to form the initial baseline requirements for the Provider Services module.

Requirements Validation

We will accomplish requirements validation during Model Office sessions. During Model Office sessions, your stakeholders will view a live, working version of the Optum Provider Services solution. It will include current configurations and user interfaces preconfigured according to your publicly available policy documents, manuals, fee schedules, and RFP requirements.

We will work with you to review the services, gather your feedback, and update configurations to tailor the solution to meet your requirements, and then confirm these updates with you. We will document requirements using our requirements traceability tool and update the RTM deliverable. Upon your approval, the updated RTM will become the basis for traceability for the rest of the project. This iterative approach will make requirements validation more interactive, enabling your stakeholders to see and understand the solution early in the project lifecycle.

Requirement Traceability

HP ALM will be our requirements traceability repository and reporting tool. With ALM, we can update, maintain, collaborate, and share requirements. Using this tool, we can link your requirements and MITA, MECT 2.1.1, product configuration and testing artifacts, and defects. We will also leverage the tool's reporting capabilities to provide you visibility into progress against requirements. Figure 3.36 shows an example of the HP ALM requirements repository.



Figure 3.36: Sample HP ALM Requirements Repository.
HP ALM allows teams to update, maintain, collaborate, and share requirements.

RQM01 During the requirements validation session TRADE SECRET t demonstrate a fully functioning solution that has been initially configured based on the Contr J of the requirements described in the RFP and publicly available policy documents, manuals, and fee schedules.

As mentioned earlier, your publicly available policy documents, manuals, fee schedules, and RFP requirements will enable us to configure a working version of the Optum Provider Services solution. During Model Office sessions, we will work with you to review pre-configured components and confirm our understanding of the requirements. As we validate requirements, we will document them using our requirements traceability tool and update the RTM. Upon your approval, the updated RTM will become the basis for traceability for the rest of the project. We will follow standard project management practices for approval and acceptances at each milestone of the SDLC.

RQM02 The Contractor shall work with the Department to confirm the Contractor's understanding of the requirements and to clarify and/or elaborate requirements where necessary to achieve desired business outcomes.

We organize the Model Office sessions according to the solution modules (e.g., provider, member). After we establish the PMO, each module team will conduct a detailed analysis of their respective requirements. While these activities will require SME participation from your staff, we realize and appreciate that their time is limited. As such, our approach will rely on our knowledge of your requirements

During Model Office sessions, we will work with you to review, refine, and seek approval for all preliminary requirements for each work stream. We will clarify goals and objectives to meet your stakeholders' needs. As we refine requirements during these sessions, we will update the RTM.

We will use the RTM to document relationships between all the requirements documented during requirements analysis and system design activities.

RQM03 The Contractor shall document any gaps between the initially configured solution and the business requirements in the requirements management tool. Gaps must show bi-directional traceability with applicable business requirement(s), design, test cases, test results, MECT criteria and certification artifacts.

We will document requirements using our collaborative requirements gathering tools and produce system requirements specification documents and other key deliverables. We will use HP ALM as the requirements traceability repository and reporting tool to document any gaps between the initially configured solution and the business requirements. With ALM, we can update, maintain, collaborate, and share requirements. Using this tool, we can link your requirements and MITA, MECT, product configuration and testing artifacts, and defects. We will also leverage the tool's reporting capabilities to enable you to view progress against requirements. Figure 3.37 shows an example of the HP ALM requirements repository.



Figure 3.37: Sample HP ALM Requirements Repository.
HP ALM allows teams to update, maintain, collaborate, and share requirements.

Our requirements management process will help us verify that requirements are consistently, accurately, and completely:

- Identified
- Documented
- Analyzed
- Validated
- Updated
- Traced
- Reported

As described earlier, we loaded your RFP requirements into HP ALM and traced the requirements to their related MECT objectives during proposal development. We will load revised or updated Provider Services module requirements into HP ALM as part of the Initiation and Planning Phases of the project to form the initial baseline requirements for the project.

Validating requirements during the early phases of the project offers the DPHHS the following benefits:

- Prioritizing requirements to expedite features
- Quicker solution configuration resulting from requirements validation activities
- Better-defined test cases and scenarios, which can reduce rework
- Joint understanding of requirements early, which can reduce changes to implement later
- Reduced number of defects

After establishing the baseline requirements, we will track the requirements using HP ALM. ALM allows us to associate artifacts, such as test cases and results, to each requirement so we can show how specific requirements are being met. It also provides flexible reporting capabilities that will help us produce an RTM with each release of the solution; therefore, we can demonstrate to the DPHHS how a given release satisfies a set of requirements. Before final production and go-live of the Optum Provider Services solution, we will produce a final, comprehensive RTM that proves that each project requirement is fulfilled.

RQM04 The Contractor shall, during requirement validation, provide designated Department staff access to a fully functioning environment to become familiar with the solution.

Our RTM tool provides flexibility for role-based permissions. We will provide authorized users access to the fully functioning environment during requirements validation so that they may become comfortable with our solution.

RQM05 The Contractor shall utilize project control tools to formally track all requirements and related design, configuration, testing, and certification artifacts. The Contractor's requirements management tool shall ensure approved changes to requirements are linked back the approved change request.

We will track requirements within our RTM tool and maintain related design, configuration, testing, and certification artifacts in our SharePoint repository as well as testing tools. These artifacts will be available through HP ALM dynamic APIs and links. HP ALM will have complete end-to-end traceability and retain details linking the requirement back to the change request. Authorized users will have access to reports on the status of each requirement in the development process. HP ALM includes features that can link changes to requirements, and specifications are accomplished in a controlled manner.

RQM06 The Contractor shall develop, maintain and submit a Requirements Traceability Matrix (RTM) to track detailed requirements and their realization throughout all project phases. This should include how the requirement is realized (e.g., configuration, custom development, base functionality). All revisions must be reviewed and approved by the State.

We will develop, maintain, and submit an RTM to the DPHHS for approval to track detailed requirements through all phases of the project. The RTM will indicate how we realize each requirement (e.g., configuration, custom development, base functionality). Upon establishing the baseline requirements, we will track the requirements using HP ALM. The DPHHS will have access to the RTM throughout the life of the contract and be able to review all revisions of the RTM.

Throughout development, we will document and maintain solution requirements in the RTM. The documented requirements will form the basis for usage scenarios and detailed business process workflows. The RTM will document where each requirement is accounted for within the design documents, code modules, and testing artifacts.

Before final production and go-live, we will produce a final, comprehensive RTM that proves we have met each project requirement. As new requirements are discovered or refined, we will document them in HP ALM and update the RTM. The RTM will serve as the basis for traceability throughout the life of the project.

RQM07 The Contractor's requirements management tool shall have the ability to manage requirements traceability by module(s), MITA business area, MITA business process and MECT checklists.

HP ALM allows complete traceability of requirements as they move though development, testing, and implementation within the Optum Provider Services solution. HP ALM will enable us to associate artifacts, such as test cases and results, to each requirement to show how we are meeting requirements. It will also provide requirements traceability by module, MITA business area, MITA business process, and MECT checklist.

3.10.2.4 Design Configuration, and Build

The Contractor shall undertake activities to resolve gaps between the RFP requirements and the proposed solution. Once designs have been approved by DPHHS, the Contractor shall configure and/or customize the solution based on the desired business outcomes. The Offeror must describe their approach to meet each of the Detailed Design, Configuration, and Build requirements defined in Attachment F, Requirements Matrix.

Our solution is configurable; therefore, we can tailor it to your unique business requirements. Our solution accommodates custom coding while preserving the integrity of the core software so we can readily apply upgrades and new releases as if no custom code existed. Configurability and extensibility are critical features of COTS-based SaaS solutions like our proposed solution to support your provider services requirements. Without configurability and extensibility, a project is simply a traditional, custom, one-of-a-kind MMIS development effort instead of a configured service implementation like the one you seek.

Benefits

- Full transparency
- Full audit capabilities
- Easy maintenance and update
- Abbreviated implementation timelines
- Lower Total Cost of Ownership

Highly configurable solutions help our commercial and state government clients accomplish the following:

- Accommodate business rules, constraints, and validations through parameter settings—without software coding—and store them with full visibility and transparency
- Maintain an audit trail of parameter changes so we can track each change to a particular user at a particular moment in time
- Accommodate changes to parameters so we can implement new rules, constraints, and validations rapidly to keep pace with policy changes
- Enable business analysts to perform implementations without software coders because the solutions are intuitively configurable
- Realize a lower Total Cost of Ownership (TCO) compared to alternative solutions

To support configuration of the Optum Provider Services solution, we will perform the following steps:

1. Conduct gap analysis of the solution against the RFP requirements

2. Document and review State-specific requirements that are not in the base solution
3. Separate the requirements that require configuration from those that require customization
4. Create features and user stories for the identified configuration items
5. Execute the component configuration based on the details contained in the user stories for the new tenant
6. Execute required testing against the completed user stories and review testing with the DPHHS
7. Deploy the completed configurations to the new tenant, update relevant documentation, and review with the DPHHS
8. Conduct Model Office sessions or a demonstration after each release according to the OSAM process
9. Continue iteratively with the OSAM process for all components until all configuration releases are complete and follow-on testing stages are ready for execution

DCB01 The Contractor's solution shall accommodate customer preferences for communications by electronic inbox, written correspondence, email, text, and phone.

Our solution has data fields that can accommodate customer preferences for communications by electronic inbox, written correspondence, email, text, and phone. This data field is configurable and can accommodate new types of communication preferences as needed.

DCB02 The Contractor shall develop and submit a design session schedule, agendas, and minutes for review by the Department.

Optum will create and submit a schedule for design sessions with the DPHHS. We will make the best use of your staff members' time and minimize disruption to their day-to-day activities so they can focus on their key responsibilities. We will work with you in scheduling our sessions to accommodate all stakeholders.

Our project managers have valuable experience delivering enterprise solutions for state and commercial customers. They will follow PMP and Agile project management methodologies to manage the project and facilitate productive meetings with the Department. Our standard process for conducting customer meetings is to do the following:

- Make sure meetings begin on time
- Create and send agendas at least 24 hours before meetings
- Take meeting minutes
- Verify the meeting is required and topics are relevant for the audience
- Make sure we send meeting agendas to the DPHHS for review and approval within 24 hours of the meeting
- Save meeting agendas in the project document repository

DCB03 The Contractor shall conduct collaborative design sessions to address all gaps identified during requirements validation.

Optum commits to conducting collaborative design sessions with the DPHHS' SMEs. Before the design sessions, we will work with your project lead in creating a schedule to identify, define,

and plan activities for the session. This preparation will allow our sessions to be collaborative and set attendee expectations for the sessions.

Our teams will come prepared with identified gaps, which they will share with attendees three days before the meetings. Based on our experience, pre-work will help us keep the sessions moving forward and make the best use of your SMEs' time.

DCB04 The Contractor shall, in the design sessions, recommend solutions for each configuration gap, as defined in requirements validation, that will produce the desired business outcomes. If a gap cannot be addressed via configuration, the Department may consider making policy changes before approving customizations to the solution.

As described earlier, our teams will attend design sessions prepared with identified gaps, which they will share with attendees three days before the meetings. We will recommend solutions for the DPHHS while keeping an open mind during these sessions. In our experience, some of the best solutions originate from brainstorming with our customers.

Optum will work with the DPHHS to consider recommending policy changes based on our experience in the provider services area.

DCB05 The Contractor shall demonstrate completed functionality frequently as the solution is configured/built, using a fully functioning environment.

We know that the DPHHS wants to achieve system efficiency around specific core functionality, including controls, edits, and audits. In addition, you want enhanced functionality that works right the first time with a lower cost and quicker implementation timeframes. The Optum Model Office approach will provide you with enhanced solution agility through service configuration and a frequent feedback cycle on those configurations. Through Model Office, your stakeholders will view a live, working version of the Optum Provider Services solution, current configurations, and user interfaces, all preconfigured according to your RFP requirements. We will then work with you to review the services, gather your feedback, update configurations to further refine and tailor the solution to meet your requirements, and confirm these updates with you.

DCB06 The Contractor shall migrate completed releases promptly through various testing levels all the way to User Acceptance Testing (UAT).

We will migrate completed releases of the Optum Provider Services solution through testing, all the way to UAT, by following our phased testing approach. Figure 3.38 shows this approach.

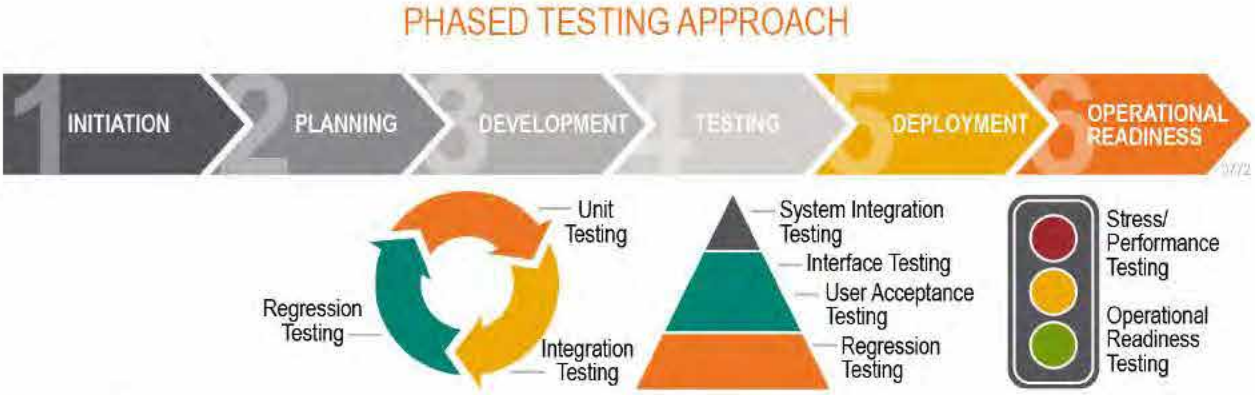


Figure 3.38: Phased Testing Approach
Our testing approach will validate the stability of each release of the Optum Provider Services solution.

Our phased testing approach will give the DPHHS the following benefits:

- **Release stability:** Optum teams make sure all critical defects are resolved before implementation, resulting in production stability. Our quality teams are the stakeholders in approving components for release. They will not approve releases if there are critical defects, resulting in release stability in Test and Production environments. We conduct thorough System Integration Testing, UAT training, and UAT activities with State staff enabling us to find defects earlier and to deliver stable, quality solutions to our customers.
- **Agile approach to UAT:** We use an Agile approach during UAT to quickly implement approved requests from State staff participating in UAT. Examples include requested changes to metadata, data models (adding or removing data fields), adding indexes, and creating materialized views to enhance performance. We release multiple versions of the code during UAT to accommodate requested changes so these changes can be tested thoroughly during UAT.
- **Regression testing:** After UAT, we lock the code and perform regression testing to confirm changes have not introduced problems into previously stable code and integration points.
- **Strict change control:** Our strict change control processes allow only a few authorized users to move code into production, which keeps unauthorized changes from entering production. Our processes also keep well-meaning individuals from fixing code in production to quickly accommodate a user request.
- **Low defect rate:** Our defect rate upon production release is very low since Optum resolves all critical defects before go-live. Our goal is to find defects in the lower environments and as early as possible. This is enabled by automated regression testing, special test scripts, and fully functional testing environments.

DCB07 The Contractor shall provide the design for online help approach and documentation, as appropriate.

[redacted]



DCB08 The Contractor shall work with the Systems Integrator and the Department to establish required interfaces as defined in the detailed scope of work.

We will work with the Systems Integrator and the Department to establish the required interfaces. Our integration layer is built on SOA principles using a lightweight ESB and integration platform. Because of its inherent flexibility, loose coupling, and SOA framework, it enables our solution to scale and provides easy integration of new services, vendors, and applications.

Our integration layer supports multiple data file transfer protocols and data formats, including:

- Data file transfer protocols:
  - FTP
  - SFTP
  - JMS, AMQP
  - SOAP Web services
  - APIs
- Data formats supported:
  - JSON
  - XML

- COBOL copybook
- ANSI X.12 Healthcare Standards
- HL7 Messages
- Proprietary formats

The integration layer has an HHS-specific design, including a canonical data model built on the X.12 and HL7 standards, and mirrors the data definition of the X.12 and HL7 transactions. For example, provider data is represented to reflect the information contained in the ANSI X.12 274x253 Provider Directory transaction standard. Adoption of industry standards for the canonical model data definitions eliminates the need to develop transaction-specific data dictionaries and transaction-specific data maps.

DCB09 The Contractor shall provide office space for Contractor staff and meeting rooms as necessary to support the scope of work and contractual obligations.

We will establish project office space within three miles of the DPHHS' headquarters at 111 North Sanders Street in Helena. The facility will be the primary location where the implementation, operations, and turnover phase activities occur. We have proven experience rapidly setting up facilities to support our client's operations—you can be confident that we will support you on day one.

We will work with our corporate real estate team to acquire the facility that best fits the project. The Optum facility will include security and adequate space to accommodate the on-site project team. It will include standard office features, such as accommodations for teleconferences, connectivity for WebEx meetings, projector equipment, and white boards. It will also include access to one or more conference and training rooms to accommodate meetings with the project team, the DPHHS' employees, and stakeholders as needed.

We will use the following criteria to narrow the search and select the best options for establishing our project office:

- ADA accessibility
- Class A/Class B office facility owned by reputable and financially stable landlords
- Maximum flexibility in lease terms to support renewals and expansions, as needed, to meet project needs
- Secure reception area
- Ample available parking
- Easy access to major highways or freeways
- Amenities (e.g., restaurants, shops, banking) available in the facility or within walking distance

As Figure 3.40 shows, we have identified four facilities that meet our specific criteria. All are located within three miles of the DPHHS' headquarters.

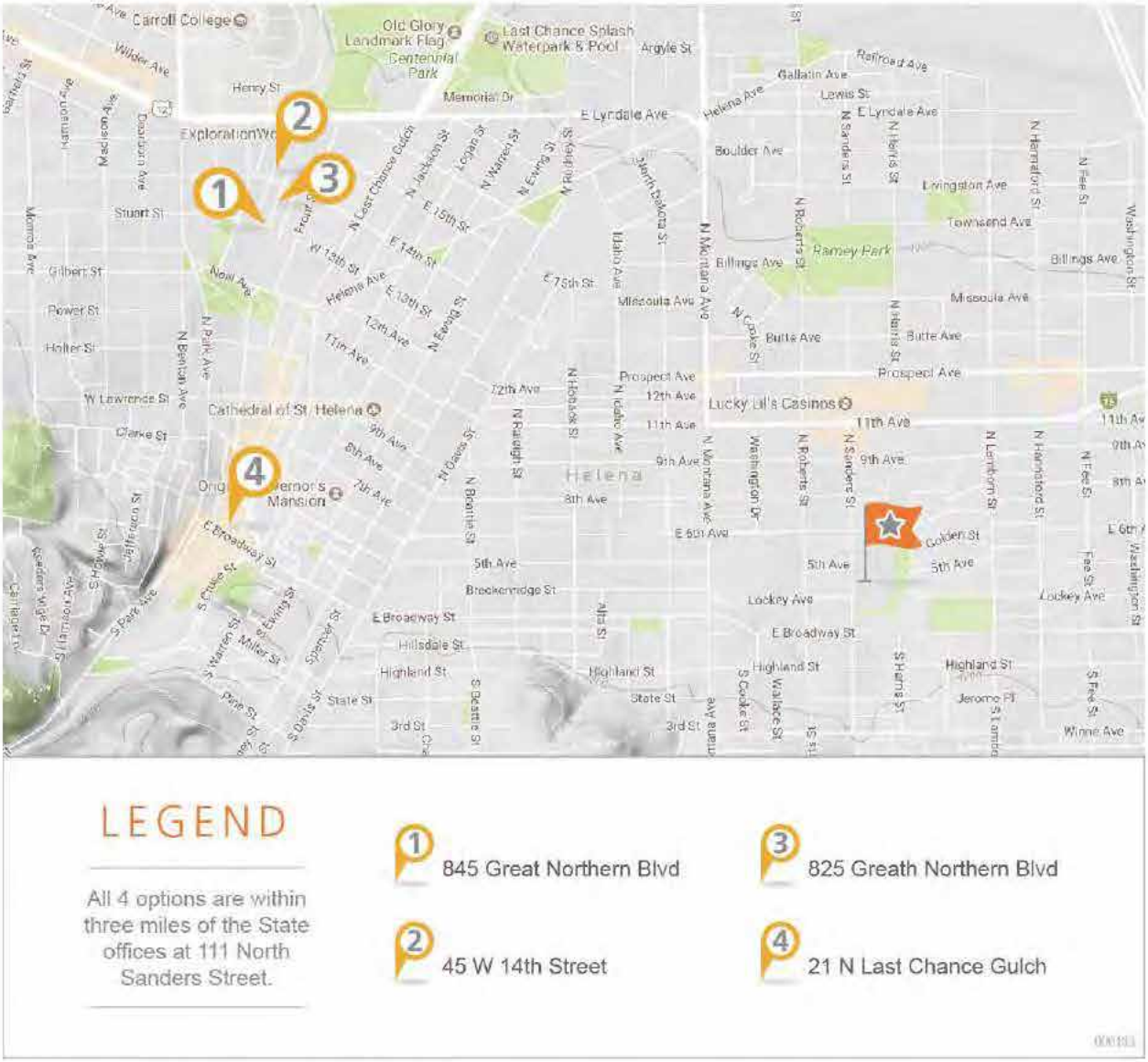


Figure 3.40: Location of Optum Office Options.
All four options for the office meet the requirements of the RFP and the Optum standards for corporate facilities—all are within three miles of the DPHHS offices at 111 North Sanders Street in Helena.

The following table contains photographs and information about these potential locations.

	Image	Address	Available Sq. Ft.	Total Sq. Ft.
1.		845 Great Northern Blvd Helena, MT 59601	3,095	7,783

	Image	Address	Available Sq. Ft.	Total Sq. Ft.
2.		40 W 14th Street Helena, MT 59601	3,414	20,715
3.		825 Great Northern Blvd Helena, MT 59601	3,428	28,919
4.		21 North Last Chance Gulch Helena, MT 59601	500 - 3,200	82,930

Before contract award, our project management team and corporate real estate representatives will perform site visits to each location. Following the site visits, we will determine the option that best meets project requirements. We will present details of the selected site to you for review and approval following contract award.

DCB11 The Contractor shall develop auditing and general controls to ensure the effective use of the technical architecture and data in meeting requirements.

[redacted]

[redacted]

[redacted]

DCB12 The Contractor must provide all technology and equipment for contractor staff necessary to support and complete the scope of work and the contractual obligations.

We will provide all technology and equipment necessary for our staff to fully complete the scope of work and support functions to fulfill all contractual obligations. All our staff members are assigned appropriate tools like fully functional laptops with all needed software. Additional software can be procured from a comprehensive application store, as needed, and can be installed quickly.

DCB13 The Contractor shall be responsible for operating and maintaining any software needed to support all module components and project tools in use by the Contractor.

We will be responsible for operating and maintaining all software needed to support all module components and project tools.

DCB14 The Contractor's solution shall have the ability to print a properly formatted representation of the entire screen (including sections not displayed without scrolling) and associated data in the application.

Our portals for the Optum Provider Services solution are built using best-in-class Web development tools. This allows us to make use of formatting services to enable our customers to print Web pages using a special print view button to print pages formatted by the page width. The portals also support using the print page function of the browser to print current view.

DCB15 The Contractor shall provide recommendations for simplified business rules and business processes to the Department.

We will make recommendations for simplified business rules and processes while working collaboratively during design sessions between our technical, business, and process experts and the DPHHS' SMEs. We have found that multi-functional teams are well positioned to look for opportunities to improve the overall process.

DCB18 The Contractor shall configure, support and maintain all components of the solution in a manner that reflects performance expectations described in this RFP.

We will meet or exceed the performance expectations the DPHHS defined in the RFP to make sure we are the vendor of choice for the DPHHS and other states. Throughout the life of the project, our focus will be to understand your requirements and provide exceptional performance. We will achieve this by making sure we review changes accurately, obtain required stakeholder signoffs, and develop, update, and maintain documentation as necessary.

We developed our solution to meet and exceed the expectations of our current and future customers. We will maintain the solution to our exacting high standards so the DPHHS will always have access to latest features of this solution.

DCB19 The Contractor's solution shall be free of any software components that are the result of legacy code transformation.

The software components within the Optum Provider Services solution are not the result of legacy code transformation. We built our solution using the latest SOA and cloud-like technologies. As a result, our MITA-aligned solution will advance efficiency and effectiveness across the DPHHS' operations.

Key features of our solution that align with the goals for this project include the following:

- SOA approach
- Emphasis on configuration over custom development
- MITA alignment, including enhancing MITA maturity and the use of SOA principles
- SaaS solution, developed for future requirements and expansion
- Highly available, redundant, and secure infrastructure
- Transparent operations with low TCO

DCB20 The Contractor's solution shall provide Web based content that is supported by standard web browsers and are mobile and tablet compatible.

As the following table shows, the Optum Provider Services solution is technology-neutral and poses no client system limitations. Because our portals are accessible from the DPHHS website using a browser, our solution does not require a specific operating system or additional plug-ins and controls.

System Requirements	Limitations
CPU Limitations	None
Operation System Limitations	None
Web Browser Compatibility Limitations	None
Framework, Plug-in or Application Requirements	None

Our solution supports industry-standard Web browsers[3] that include the following:

- Microsoft Internet Explorer 7.0 or higher
- Mozilla Firefox 3.6 or higher
- Apple Safari 3 or higher
- Google Chrome 10 or higher
- Opera 43

The solution portals also support browsing on personal computing devices, including iPhone, iPad, Android phones and tablets as well as Windows mobile phones and tablets. We follow Mobile Web Best Practices (MWBP) as recommended by the World Wide Web Consortium (W3C). As a result, users can access the Optum Provider Services solution using the device most convenient for them.

We will host the solution portals on the Optum FISMA Environment, which we built on a highly scalable infrastructure. We can provision additional capacity as business demand grows. No user hardware limitations exist. Using our purpose-built portals, authorized users (e.g., providers, the DPHHS' stakeholders) can access the Optum Provider Services solution as security permissions allow.

The solution framework complies with federal accessibility regulations, including Section 508 of the Rehabilitation Act of 1973, amended 1998, as well as industry-leading W3C accessibility tenants. We will periodically review our solution to support continuing compliance with industry standards.

DCB21 The Contractor's solution shall allow the Department to edit and change any static text in the application and correspondence templates. All static text must be approved by the Department.

The Optum Provider Services solution is highly configurable to support the unique needs and nuances of each state's Medicaid and HHS programs. The solution enables the configuration of static text in the application and templates, as well as unique user roles. We will review existing templates with you and discuss your specific static text requirements in the design, configuration, and build stage of the project. Based on your feedback, we will make appropriate changes to the solution before implementation. After the project moves into steady state operations, all static text changes will go through our agreed upon change control and release management processes and will require your approval.

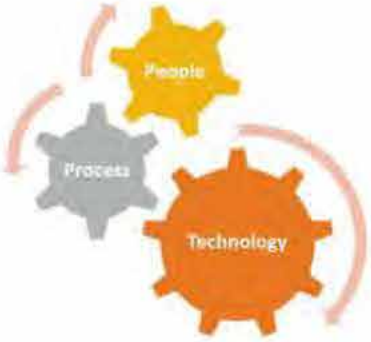
[3] According to **netmarketshare.com**, the above listed browsers and OS combinations cover 98 percent of Internet traffic (https://www.netmarketshare.com/browser-market-share.aspx?qprid=2&qpcustomd=0).

3.10.2.5 Data Conversion, Cleansing and Migration

Data conversion, cleansing, and migration activities required to support the scope of work contained in this RFP include planning, identifying and analyzing conversion specifications, testing, execution and coordination of all data and file conversion, migration and data cleansing processes.

Data conversion often encounters risks and issues related to the complexities in defining the relationship between source and target data structures, differences in the data required for processing between legacy and new systems and the historical changes to processing requirements and valid codes that may result in data inconsistencies and missing data conditions. The Offeror must describe their approach to meet each of the detailed data conversion, cleansing and migration requirements defined in Attachment F, Requirements Matrix.

Sound data conversion practices are key to successful solution implementation. The three pillars of our data conversion strategy are people, process, and technology.



We will leverage people, process, and technology to help the DPHHS achieve your goals, which include the following:

- Providing a modern, Web-based self-service solution for providers to enroll in Montana Healthcare Programs
- Awareness and vigilance against project risk; controlling risk by imposing realism into the planning process rather than assuming the best possible outcome will always occur
- Reducing cost and implementation time
- Using IT to improve the efficiency and effectiveness of the DPHHS' operations at all organizational levels

We will help the DPHHS achieve these goals using our proven data conversion framework with experienced team members (people) while leveraging simplified and tested procedures (process) and best-in-class tools (technology).

Optum Data Conversion Overview

Data conversion involves the planning and development, testing, migration, and conversion of data and files required to support the implementation and operation of the Optum Provider Services solution. Our strategy for data migration and conversion begins with a full understanding of the character and purpose of the data in both the source and target systems. We will transpose this understanding into conversion, testing, and execution specifications during the planning phase. The result will be our comprehensive Conversion Plan.

Expertise

Every Optum project includes conversion as a key task.

- 20+ years of successful conversion experience in commercial and government markets
- Extensive library of lessons learned/best practices
- Involvement of staff with deep data conversion knowledge
- Project history that extends beyond Medicaid

The key to successful data conversion, particularly one involving a Medicaid enterprise, is preserving information from the source transactional data while rendering the data in an optimized format for use in our solution. It is vitally important we do not lose data in the conversion and loading process because we do not know every future need for the legacy data. We set the stage for this during the initial Planning Phase as we develop the Conversion Plan and associated tasks that will ultimately result in the successful conversion of legacy data.

Our conversion process will not affect the integrity of the data received from the source systems. Whenever we apply approved transformations, we will retain the original content and data values by putting the new data in different tables or additional columns within the existing tables. This approach will maintain the quality of your data.

We will use OSAM to drive each release or program increment to enable the overall work by converting and synchronizing the required data. Mirroring the workflow of the overall Optum Provider Services solution, we will iteratively employ our data conversion processes and tools. As we progress, we will document the design, testing, and execution specifications as we continuously refine the Conversion Plan.

Results

We deliver high-quality data conversion more reliably than traditional methods.

Our data conversion solution is proven in many Medicaid MCO and data warehouse implementations. It allows data to ingest more quickly and more reliably while mitigating the risk of volume fluctuations and data quality issues.

Optum Data Conversion Framework

We use a data conversion framework that consists of a multi-step process, protecting the integrity of the DPHHS data first and foremost through the entire process. Figure 3.41 shows an example of conversion architecture.

[redacted]

The conversion framework we use consists of a three-tiered approach to the extraction, transformation, importation, and movement of your data into the target systems. Applying an iterative approach enables us to place quality checkpoints within the process to confirm the integrity of your data and verify the correct mapping of source-to-target tables and fields. Our conversion framework is flexible and enables us to include those data elements necessary for the proper operation of your provider services solution. Figure 3.41 illustrates the full scope of input capabilities of our framework.

Best Practice

Data conversion best practices include:

- Library of lessons learned/best practices
- Involvement of subject matter experts who specialize in data conversion
- Project history hat expands beyond Medicaid

Optum Data Conversion Process

[redacted]

Extract Source Data

We will load data extract files in the staging area to prepare for further processing. In the staging area, we will profile and analyze the data for accuracy, formatting, and content. The process map in Figure 3.42 illustrates our overall data conversion process. Each vertical box represents a key process area that we use in all of our projects. We will repeat this process for each release of our solution.

Data Cleansing

We will share the profile analysis results with the DPHHS and develop data cleansing rules for any data anomalies that do not agree with expected values. For each solution release, we will quantify and document data quality issues, such as invalid record relationships, data type redefinitions, or invalid content.

After we extract data from the source systems and identify its target location, we will conduct a field-by-field analysis. This approach will help us determine the conversion requirements for each data element, including format, valid values, and source. Optum functional area teams will identify target data requirements. In coordination with Optum, the DPHHS will identify source data requirements. Based on the requirements, we will document the conversion method (conversion rules and specifications) for each field according to the following primary conversion approaches:

- **Direct conversion:** Data converted from a field in the legacy system to a column in a new system table, which requires no manipulation of the data
- **Logical conversion:** Data converted from a field, or combination of fields, in the legacy system to a column in a new system table, which requires additional consolidation, calculation, or manipulation of the data (includes crosswalks of valid values and HIPAA code sets)
- **Derived conversion:** Data that is defaulted, calculated, or generated in the new system
- **Default:** Data that defaults to new system values

Conversion mapping documents is central to the data conversion process. Throughout the project, we will maintain target data information within these documents. We will communicate changes affecting the target data structure to your technical team.

The conversion mapping documents will list files identified as conversion sources for tables to be manually loaded within the new system. These documents will also list files that will require us to write conversion routines. We will work with your designated team members to identify programs for each functional area noted in the mapping documents. If the mapping documents were developed as part of the legacy system, the conversion programs can leverage them. We will identify programs developed as part of the Optum Provider Services solution that we can leverage for conversion by the functional areas.

Data Transformation

As we progress through each conversion phase, we will transform the data based on the needs of our solution and agreed-upon specifications. In addition to format conversions, we will identify additional data elements necessary to maintain business meaning and optimize processing, replication, and reporting. This is a particularly important step because many of our program iterations and Model Office steps require clean claims, provider, member, and associated data. We will present and discuss with you the results of the data profiles and the suitability of the data for each step.

Our ETL analysts will construct the conversion jobs according to the specifications in the mapping manager tool. Constructing conversion jobs is an iterative process. It requires a significant amount of flexibility to stay in step with the new system.

The ETL analysts will use the mapping report generated from the conversion mapping tool to determine the best method for designing and developing each conversion ETL process. We will use our ETL tool to build mappings that will incorporate the business rules and data linkages defined in the mapping specifications.

Missing Data

We expect some tables and fields in the legacy source data might be missing required fields for our solution. We propose writing business rules to populate this data in consultation with you. Additionally, we expect that some tables within our solution might not have exact corresponding legacy source data. In these instances, we populate the tables manually. For example, we might find some legacy source data in the existing business rules within the legacy system source code instead of in legacy files or tables. To begin this process, we will first identify solution tables that we will manually populate. After we identify the list of manually configured tables, we will gather the data to populate these tables, turning the data into manual source data. In the target system, we can enter this information manually or capture it in a spreadsheet to use as a source file for conversion.

Iterative Test Extractions

Within each iteration cycle, we will conduct quality checks to validate the accuracy of converted data against expected results, based on the application of transformation rules to source data-in-scope for the test. For example, we will conduct statistically significant sample size audits to check for outcome violations on various data elements. We will also automatically verify count balances at the file and table level and perform unit and system testing for conversion and load programs.

Testing and Verification

The verification process is continual and iterative. This is required to control the initial and ongoing data transformation and quality assessment processes. We will conduct unit testing through acceptance testing throughout the data conversion lifecycle. Before the final target loading, we will load and verify a subset of the data in a test database.

We will identify all subtasks and deliverables related to conversion testing in the work plan and address them in the Data Conversion Test Plan, which covers the following:

- Development and execution of unit and system testing for all conversion and load programs
- Quality check procedures
- Post-conversion data testing and auditing
- Objective pass/fail criteria or metrics, as appropriate
- Conversion Test Results Document

Data Loading

After completing the planning and analysis phase, we will move data to the target database. Loading the converted data from the staging files into the system database (test, staging, and production tables) will consist of running the files through a set of ETL processes.

Final target loading will start from scratch on a production database with proven data conversion procedures. We will collect target audit statistics and verify them against source data statistics and expectations. The target database will load to the approved and tested model with tested, profiled, and transformed data.

Manual Data Conversion

Our approach relies on data profiling, which results in scripting that builds data conversion paths for every permutation found in the data. If specific requirements require some records to remain unconverted, we will manage that. In such cases, we will alter our script to divert the affected data to a sequestration staging area, where we will retain or archive it according to your requirements.

Data Validation and Reporting

Data validation occurs throughout the conversion process. We will follow processes that count the records and fields in the input files and balance these records and field counts to verify that no data was excluded during the loading process. When we load the data, we will perform additional data integrity checks to validate the newly loaded data displays correctly for the user.

Inherent Edits

Each execution of the conversion process for a given set of tables within a component produces error reports. These reports document data anomalies, inconsistencies, and errors encountered during the process. The ETL tool produces reporting that breaks down, by functional area, execution duration statistics, as well as information on valid and rejected counts. We will review these reports to determine whether the conversion job executed successfully. If the report indicates runtime issues, we will conduct additional analysis to determine if the issue is data-related or inherent in the conversion process design.

If our review of these reports reveals design or conversion process errors, the ETL analyst will correct the conversion programs, roll back the failed attempt, and re-execute the conversion run. If the review indicates problematic data, the ETL analyst will forward the reports to the DPHHS and Optum SMEs for review. The SMEs will decide whether to correct the data in the source files (on the source system), allow the data to convert as is, or alter the mapping specifications to accommodate the data.

Balancing and Reconciliation

A structured process for verifying the accuracy of converted data is essential to validate a smooth, efficient final file conversion of legacy system data into the new Optum Provider Services solution. We will use the DPHHS' production data for conversion and development testing. Our ETL toolset will apply the appropriate masking to sensitive data to validate that PHI and PII are not used improperly.

The Data Conversion Test Plan will describe the levels of data verification activity. The plan will define the toolsets that track errors and error resolution. It will also provide examples of error, balancing, and validation reports by functional area.

We will verify conversion data using various strategies:

- **Validation of conversion mapping specifications:** Validates against the conversion crosswalk to verify programs comply with the specifications for conversion.
- **Balancing and comparison:** Compares the output of converted data with data in the source file at the macro and micro level. At the macro level, we will run counts of records and categories of records to make sure the counts in the source file match the counts

loaded to our solution. This will confirm records are not lost or added during conversion. At the micro level, we will compare sample records from the source file and target table to verify all data properly converted.

- **Testing target system functionality:** Tests new system functionality using converted data. This will verify that the new system is processing data correctly and the converted data passes all editing or business rules.

These three strategies will provide a thorough evaluation of the accuracy of the converted data at the macro and micro level. By validating against the conversion mapping document, we will demonstrate the programs operate as designed.

Parallel testing and data reconciliation: Before the final conversion, we will perform trial conversions. We will conduct walkthroughs of completed file and table conversions for the functional area teams and will submit these results for approval. In addition, the team will conduct parallel system and component runs to validate conversion tests results. They will submit the results to the functional area teams for approval. If available, the functional area teams can compare the data displayed on legacy system screens to the converted data displayed on the corresponding portal Web page.

Manual load quality assurance: We will perform rigorous verification and validation assessments on manually entered data before and during the replacement system implementation.

Final conversion will occur when we transform, migrate, and load the complete set of conversion data into the Optum Provider Services solution production databases. Our functional area teams will work with the DPHHS to determine the definition of complete set of data for the final conversion. They will also determine the processes that will verify that the conversion has been successful.

DC01 The Contractor shall convert all member and provider data history for any member or provider that has been active within the past three years and three (3) years of all applicable operational data from the State's legacy systems. The Department may require additional data to be converted on an exception basis to support ongoing business needs (e.g., TPL recovery, SURS recovery and drug rebate). The Contractor shall produce comparative reports for all converted data. Any data quality issues will be addressed by the State within each source system.

Optum will convert all provider, reference, and associated data, including electronic files and records for the cut off period of three years as requested by the DPHHS. In addition, we will collaborate with you to identify, validate, and convert additional data as required to support your goals for the Provider Services module.

Data validation occurs throughout the conversion process. We will follow processes that count the records and fields in the input files and balance these records and field counts to verify that no data was excluded during the loading process. When we load the data, we will perform additional data integrity checks to validate the newly loaded data displays correctly for the user.

During the conversion process, we will conduct balancing and reconciliation of data records at the provider level and at the element level. Optum will produce and review detailed reports with the DPHHS.

DC02 The Contractor shall provide authorized Department or other designated staff access to an environment to validate converted data and provide support for the data validation effort.

Optum will work collaboratively with you to transform and load the data from your various data sources and legacy systems. We will work with the DPHHS team to perform a thorough analysis before conversion and loading. Both teams will work to confirm the record layouts, data

elements, and valid values. In addition, we will work together to verify that the necessary scrubbing and transformation based on the business rules developed with the DPHHS align with the approved conversion plan.

DC03 The Contractor shall work with the State to identify the data elements from existing legacy systems that will or will not be converted to the Contractor's solution. The Contractor shall work with the State to achieve desired business outcomes without familiar data elements.

We expect some tables and fields in the legacy source data might be missing required fields for the Optum Provider Services solution. We propose writing business rules to populate this data in consultation with the DPHHS. We also expect that some tables within our solution might not have exactly corresponding legacy source data. In these instances, we will populate the tables manually. For example, we might find some legacy source data in the existing business rules within the legacy system source code instead of in legacy files or tables.

To begin this process, we will first identify solution tables that we will manually populate. After we identify the list of manually configured tables, we will gather the data to populate these tables, turning the data into manual source data. In the target system, we can enter this information manually or capture it in a spreadsheet to use as a source file for conversion.

DC04 The Contractor shall work with the State to identify data elements or fields in the Contractor's solution that are not available to be converted from the legacy system, and whether the conversion programs should fill them with default or initial values.

We expect some tables and fields in the legacy source data might not be available for conversion. Our team will propose multiple options to the State and through consultation will create mapping rules for each field. Rules can include setting default values or creating calculated values, or if the data is not relevant, dropping the data. These rules will execute only after your review and approval.

DC05 The Contractor must perform one or more trial conversions as necessary, before final conversion of the data, and present the results to the State.

Our approach to data conversion is an iterative process. Within each iteration cycle, we will conduct quality checks to validate the accuracy of converted data against expected results, based on the application of transformation rules. As requested, we will conduct statistically significant sample size trials to check for outcome violations on various data elements. We will also automatically verify count balances at the file and table level and perform unit and system testing for conversion and load programs. After every trial, Optum will present the results to the DPHHS for review.

Before the final conversion, we will perform trial conversions. We will conduct walkthroughs of completed file and table conversions for the functional area teams and will submit these results for your review. In addition, we will conduct parallel system and component runs to validate conversion tests results and then submit the results to the functional area teams for approval. If available, the functional area teams can compare the data displayed on legacy system screens to the converted data displayed on the corresponding portal Web page.

DC06 The Contractor shall produce the reports necessary to demonstrate adequate checks and balances within the data conversion process.

We will verify conversion data using various strategies and reports, including the following:

- **Validation of conversion mapping specifications:** We will create the mapping document based on the above analysis and conduct review sessions with the DPHHS to review mapping, edits, and business rules. The sessions will help explain mapping to the

DPHHS SMEs, validate our mapping, and help to understand the institutional knowledge present with the SMEs.

- **Balancing and comparison:** We will compare the output of converted data with data in the source file at the macro and micro level. At the macro level, we will run counts of records and categories of records to make sure the counts in the source file match the counts loaded to our solution. This will confirm records are not lost or added during conversion. At the micro level, we will compare sample records from the source file and target table to verify all data properly converted.
- **Testing target system functionality:** Using converted data, we will test new system functionality. This will verify that the new system is processing data correctly and the converted data passes all editing or business rules.

These three strategies will provide a thorough evaluation of the accuracy of the converted data at the macro and micro level. By validating against the conversion mapping document, we will demonstrate the programs operate as designed.

After executing each file conversion attempt, we will review results using specified guidelines, whether the test is preliminary or final. To evaluate the accuracy of converted data, we use varying levels of validation in sequence within each strategy:

Balancing: We compare the file and record counts from the data source (legacy system) with the file and record counts of processed records within each conversion process.

Error report review: Each execution of the conversion process for a given set of data within a component may produce error reports. The reports will document data anomalies, inconsistencies, and errors encountered during the process. We will review each report to determine the root cause.

Level I data validation: This process involves comparing actual data fields on target system tables with the source data from the existing system. We use various toolsets to randomly select records from the source files. Corresponding records from replacement system tables are then selected. We will compare each field to the source data using the mapping specifications found in the crosswalk. We will prepare and retain documentation of this field-by-field comparison.

Level II data validation: This process involves reviewing selected cross sections of data in component systems with comparisons to similar cross sections of data within the legacy system.

Level III data validation: This process involves viewing and inspecting converted data using our system functionality in the conversion environment.

DC08 The Contractor shall convert electronic documents identified by the Department in a format approved by the Department.

We will inventory and convert electronic documents to the required format to meet the DPHHS' requirements. After we convert the documents, we will work with you to enhance the existing metadata and re-index the documents for storage in Optum FISMA Environment storage. We will also share a copy of the documents for secondary storage, as the DPHHS requires.

DC09 The Contractor shall provide convenient access to electronic documents from systems being replaced.

After we convert electronic documents from the systems we are replacing, we will load the documents to the Optum FISMA Environment storage. We will re-index the documents so that correct documents are tagged to the specific provider master record or other master source as relevant. Authorized providers and SMEs will access the documents from the provider portal.

3.10.2.6 Testing

Testing is a critical component for successful implementation of any system configuration/development effort, therefore, in depth, process driven, fully documented testing processes are required for all implementations and configuration changes within the Montana Healthcare Programs enterprise. The testing activities shall include planning, managing and executing a comprehensive testing effort to include unit, system, regression, parallel, integration and UAT.

Prior to implementing a new release, the Contractor is responsible for ensuring that all required tests are performed and evidence that each component meets or exceeds all relevant functional, technical, security, and performance requirements is provided. The Offeror must describe their approach to meet each of the detailed testing requirements defined in Attachment F, Requirements Matrix.

Communication

A key element of our testing strategy is communication. We will provide:

- A high degree of collaboration in a mul i-vendor environment
- Transparency with the DPHHS, MPATH, and other stakeholders
- Interdependencies built into our integrated project plan so hat impacts of testing on other projects and systems is managed and tracked

The goal of testing is to deliver an Optum Provider Services solution that fully complies with your requirements. Our team understands the complexities of testing large-scale, enterprise Medicaid solutions. We have extensive experience converting and testing MMIS historical data, collaborating with managed care companies, and working in multi-vendor environments. We will use our experience, knowledge, and proven processes to deliver a fully tested and operational Optum Provider Services solution.

Because we will implement the solution in a dynamic multi-vendor enterprise environment, close interaction with other parties such as MPATH and the SI contractor will be an important element of testing. Our testing strategy will focus on communication and collaboration. It will leverage all best practices and procedures to minimize risk and maximize quality. Our strategy will combine our testing methodology and approach with frequent, open, and transparent communication. You will benefit from our experience in delivering a system that meets your requirements.

We base our testing approach on our comprehensive, disciplined, and repeatable testing processes. Our complete set of testing processes described in this section will demonstrate that the Optum Provider Services solution fully meets the requirements defined in your RFP. We will implement a comprehensive testing program that is driven by the CMS Testing Framework and our Optum Delivery Model. Our model includes a proven testing methodology, which we have used on more than a dozen similar and successful state enterprise HHS implementations.

Optum will deliver a preliminary Master Test Strategy after completing requirements validation. We will work with the Department to determine the exact content and format of the plan. We will review draft content in a joint walkthrough with you.

Figure 3.43 shows an example of the Table of Contents of the Release Test Plan.

Table of Contents

1. Introduction
2. Referenced Documents
3. Overview
4. Assumptions/Constraints/Risks
5. Release Test Approach
6. Planned Test Types
7. Testing Interfaces
8. Performance Testing
9. Defect Management
10. Roles & Responsibilities
11. Test Environments
12. Release Plan
13. Test Data Sources
14. Acronyms

Figure 3.43: Test Release Plan.
The Test Release Plan includes details on testing approach per release.

We will deliver a final version during the development and configuration stage. Our testing methodology is consistent with the principles and methodology presented within the CMS Testing Framework that establishes, defines, and organizes guidelines for testing new and existing CMS business applications and infrastructure prior to their deployment to a production environment. The Master Test Strategy deliverable will include the following information:

- Testing strategy and approach for the following testing types:
  - System & Integration testing
  - Regression testing
  - Parallel testing
  - Performance and load testing
  - Manual and automated or scripted testing
  - User Acceptance Testing
- Planning and preparing the test/staging environment
- Approach to conducting each test level
- UAT support
- Testing nonfunctional requirements
- Test documentation (e.g., test cases, test case results)
- Quality control/quality assurance

- Bi-traceability to requirements and design
- Tools, techniques, and methods
- Reporting mechanisms, traceability, and metrics
- Defects and resolution
- Entrance and exit criteria for each test level, including alignment with industry standards
- Configuration management for each test level
- Testing roles and responsibilities
- Acceptance criteria

Our testing methodology consists of four broad activities to assess system quality and readiness for operations. All are equally critical to the success of a testing effort and are summarized as follows:

- **Planning:** Planning includes confirming the proposed testing strategy. We verify the proposed testing types, focus, and approach are appropriate, comprehensive, and integrated with the planned activities across the solution.
- **Preparation:** We write the test cases, document the testing methodology, and establish the test environments. We develop the detailed test cases identified during planning and document expected results.
- **Execution:** Upon completion, review, and approval of the outputs of the preparation activity, test teams begin executing the test cases. They compare actual test results with the expected results. The teams research and resolve any discrepancies found and execute the test again as appropriate.
- **Review and verification:** Verification of actual test results begins with the execution of the first test and continues until test cases are executed and passed. We record and review the results of tests, both successful and unsuccessful.

Throughout the life of the project, we will perform all required testing and provide you evidence of test completion. This approach will validate that each solution component meets or exceeds all relevant functional, technical, security, and performance requirements.

Our many years of experience in testing (not only for customers but also for our own internal systems, which support millions of people) will be useful for your solution.

TEST02 At a minimum, the Contractor shall provide sufficient segregated environments to support testing processes that are equivalent to the following:

a. Integration Testing: End-to-end testing performed to expose defects in the interfaces and in the interactions between integrated module components or other systems and validate the system's readiness to meet non-functional requirements.

b. System testing: The process of demonstrating that a program, function, or integrated system components meets its requirements and objectives as stated in the requirements specification.

c. Regression Testing: Testing of a previously tested function following modification to ensure that defects have not been introduced or uncovered, as a result of the changes made. It is performed each time the software or its environment is changed, and typically involves automated testing scripts.

d. Parallel Testing: Validates that the system achieves the same results as compared to another system (e.g., a legacy system) or previous software version.

e. Performance and Load Testing: Verifies the performance of a system will meet service level agreements and also measures the behavior of the system with increasing load (e.g. number of parallel users and/or numbers of transactions to determine what load can be handled by the system).

f. User Acceptance Test: Testing conducted by the user or customer to determine whether or not a system satisfies the defined user acceptance criteria in an isolated environment.

With a comprehensive and Department-approved Master Test Strategy and methodology in place, we will conduct testing of the Optum Provider Services solution leveraging the environments needed for the engagement. Testing will occur in multiple phases to deliver a quality solution. We will incorporate these test phases early in the overall process and continue throughout implementation, both pre- and post-go live. Each test phase will have its own entry and exit criteria. We will use disciplined, repeatable processes during the execution of testing. For each test phase, we will develop test cases based on the RTM to make certain the solution meets your requirements. Figure 3.44 illustrates how our staged testing progression combines with the implementation approach and SDLC.

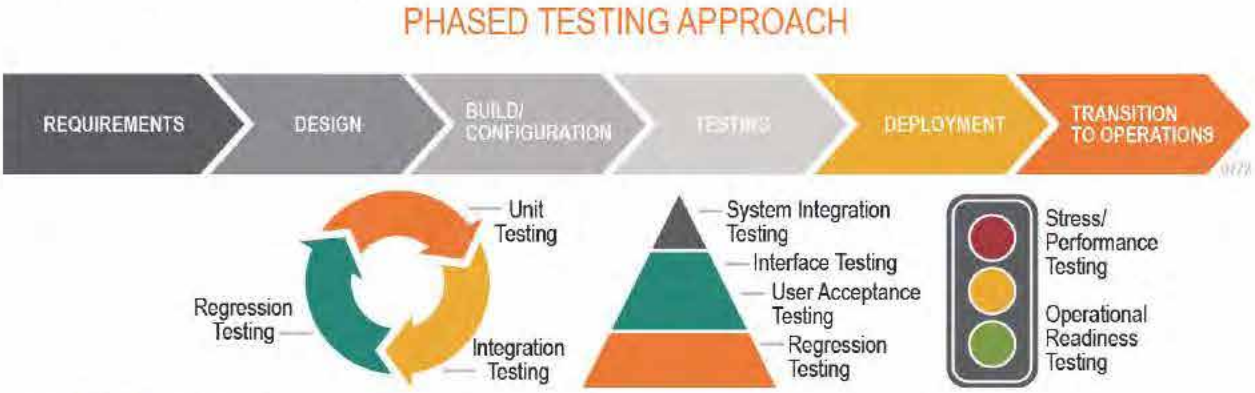


Figure 3.44: Phased Testing Approach

Our test phases closely align to our iterative design and development approach, described previously in our discussion of our implementation approach.

At the conclusion of our internal solution-centered testing, your acceptance testing, and joint operational readiness testing, we will produce formal test results deliverables for your review and approval. Successful completion of testing, resolution of any outstanding defects in accordance with RFP requirements, and your acceptance of test deliverables will serve as entry criteria to implementation of the Optum Provider Services solution into production.

The following table describes the testing stages we will use.

Test Stage	Description
System & Integration Testing	The objective of System & Integration Testing (SIT) is to verify the solution meets the functional requirements established and the solution sub-components communicate effectively within the integrated solution as a whole. The test cases cover details, such as navigation, the required input for each report/query/process, and the expected result of each transaction. SIT is more formal than a Unit Test and Unit Testing is a prerequisite. SIT is planned and executed for each sprint within a release, based on the approved requirements for that sprint. It will also verify the integrated solution and data flows for external interfaces and trading partners, including clearinghouses and intermediaries. For each type of transmission, we will test the time lag between transaction receipt by the system and notification of receipt to the data originator. The testing conducted between the integrated systems includes real time and batch interfaces. The test cases cover details such as simulating carrier integration, the required input for each report/query/process, and the expected result of each transaction as well as exercise the unique interface and integration points across the services. We will execute test cases to verify the functionality and outputs are correct and complete in the solution. Successful execution of the Test Plan will validate the functionalities. Our testing team will direct Integration Testing activities and operate the solution as defined by the Test Plan. We will provide error resolution and technical support throughout integration testing to facilitate the successful execution of the Integration Test Plan. We will base our SIT on your requirements. The satisfactory completion of each test case will indicate the successful completion of Integration Testing.
Regression Testing	Regression testing analyzes the impact of the new functionality on the existing solution and the data conversion testing. Testing for this stage will be developed as part of the initial Integration Testing effort and will be augmented over the life of the program. We will identify data and test cases and leverage them throughout the testing phases to verify pre-existing functionality has not changed. We will automate as much of this testing as possible. Regression testing also occurs for every product release prior to acceptance of a product release to deploy.
Parallel Testing	Parallel testing is one of the key inputs into the overall testing activities. The goal of this stage is to verify the operational processes and procedures compared to another actual system. Actual application users handle the required tasks in real-world scenarios according to operations processes and procedures and verify it against the other system. After meeting entry criteria and receiving stakeholder agreement, Optum will execute, measure, and report parallel activities. The QA team will provide support during development, execution and defect analysis throughout this stage. At the completion of successful parallel test, Optum will recommend and get approval of the system to proceed to production and go live activities will be approved to commence.
Performance Load/Stress Testing	Optum Enterprise Performance Testing confirms that we meet performance, availability and stability objectives for systems and applications. We conduct performance testing for new applications, application or infrastructure changes, troubleshooting, and hardware and software comparison and evaluation. Our automated tools simulate high user volumes within a dedicated load of data. Support for application protocols includes HTTP/HTML, Web services, mobile, database/ODBC, Citrix, RTE, and video streaming. We maintain a dedicated Internet connection with 400 MB/1GB burst for testing Internet applications. Our performance management tools are fully integrated to facilitate comprehensive reporting and analysis. We support multiple test types, including load, stress, stability, and resiliency testing. Load testing measures how the application will behave under peak user volumes. Stress testing pushes the application to above-expected user volume and helps us identify a break point. Resiliency testing determines application behavior in failover conditions. Stability tests run for extended durations to identify underlying issues, such as memory leaks that may not be noticeable until the application has been under load

Test Stage	Description
	for several hours. As we prepare for Enterprise Performance Testing, we will work with you to define goals, test case requirements, and scenarios. We will develop test cases based on documented workflows that are critical to your business or are most frequently used by your users. Performance test engineers execute tests based on test scenarios we design with your SMEs. We will provide reports after each test to help you conduct in-depth analysis and compare tests. Performance test benefits include: • Reduced infrastructure costs by sizing components correctly • Increased application stability by: – Baselining infrastructure and application performance before releases, upgrades or changes – Determining if applications and infrastructure will support the expected level of users and transaction volumes – Testing application performance to plan for unexpected increases in usage volume – Identifying failover issues and application resiliency under load • Improved user experience by: – Confirming the user experience remains unchanged and stable under stressful conditions, such as failures with architecture or dependent services – Identifying bottlenecks, performance issues, and opportunities for tuning
End-to-End (E2E) Testing	E2E Testing identifies system dependencies and verifies data integrity is maintained across the entire system. QA verifies the system is integrated to all external or third party systems defined in the requirements including functional and non-functional requirements. QA executes scenarios, both positive and negative, that test the flow of the system from beginning to the end. E2E Testing includes full workflow execution of all cycles (e.g., daily, weekly, monthly) using converted and interface data as much as possible. E2E scenarios are developed using real-world Medicaid scenarios, as well as program-specific pain points for the DPHHS. Scenarios usually start with daily system and manual tasks, followed by additional cycles, such as weekly and monthly. Test scenarios may also be grouped into cycles to leverage commonality and optimize the critical path. The satisfactory completion of every test case and your sign off on the test results will indicate the successful completion of E2E Testing. Where possible, E2E scenarios may be executed in earlier testing stages to allow for earlier validation of scenarios or identification of defects.
User Acceptance Testing	The primary goal of UAT is for Optum build confidence that the solution meets the business needs of your program. We will jointly define scenarios to validate the solution and tailor UAT activities to those scenarios. Business use case examples may include support for grievance and appeal research, provider or member contacts and escalations, or report and dashboard data analysis. After stakeholder agreement and meeting entry criteria, Optum will aid, measure, and report UAT activities. The QA team will provide support during development, execution, and defect analysis throughout the UAT stage.

TEST03 The Contractor must identify and resolve interdependencies that restrict or impede required testing of the Contractor's solution, other enterprise modules, or module components from performing required testing. Unless otherwise identified by the State strategies to resolve interdependencies must be reviewed and approved by the State prior to implementing the resolution strategy.

We will help quantify testing tasks for which we anticipate your participation. This includes both the task duration and level of effort in hours. During project planning, we will work to incorporate tasks and dependencies for third parties. We will address issue resolution as quickly and promptly as possible where interdependencies between vendors exist and bring it to you for review, so that there will be no undue delays or potential conflicts.

TEST04 The Contractor shall perform testing and present the results for each of the following test levels: Performance Test results, System Test results, Parallel Test results, Regression Test results, Integration Test results. Test results shall be traced to the use case/user story and design documentation being tested.

The testing management tool reporting functionality will provide an accurate window into testing progress. It will give the DPHHS and Optum project management staff a perspective on the progress of testing tasks.

For example, HP ALM can provide the up-to-the minute details regarding test case execution, requirements-to-test case coverage, and defect status. This data will be automatically compiled in the Test Summary and Detail Report, as Figure 3.45 illustrates.

Functional Areas	Total Test Cases	Total Completed	Passed	Failed	Blocked	In Progress	No Run	N/A
Claims / Claims History / Rx Claims	225	225	224	1	0	0	0	0
Provider	15	15	15	0	0	0	0	0
Member	12	12	10	2	0	0	0	0
Authorizations - Medical Inpatient	300	300	300	0	0	0	0	0
Authorizations - Medical Outpatient	300	300	300	0	0	0	0	0
Authorizations - Behavioral Inpatient	300	300	300	0	0	0	0	0
Authorizations - Behavioral Outpatient	300	300	300	0	0	0	0	0
Totals	1452	1452	1449	3	0	0	0	0

Figure 3.45: Testing Progress Report Example.
We can easily produce reports to monitor the testing progress and report issues to the DPHHS.

The summary will include the scope, test scenarios, test case description, metrics, and overview of test results for each test case, including test logs and notes.

We will produce a final Test Summary and Detail Report at the end of each release. This report will include a summary of all test cases with their completed status, an exported copy of each test task, and supporting documentation. Figure 3.46 shows an example of the Table of Contents of the Test Summary and Detail report.

Table of Contents

1. Project Description
2. Project Scope
3. Requirements
4. Test Phases and Execution
5. Defect and Error Summary
6. Execution Summary / Recommendation
7. Risks
8. Sign-offs
9. Appendix Items
    - 9.1 Parallel Test Schedule
    - 9.2 Documentation

Figure 3.46: Test Summary and Detail Report Contents.
The Test Summary and Detail Report includes details on test case execution and defect status.

In addition to the above core test and defect reporting, as necessary, we will provide you with reports as referential data is updated in our test environments. We will apply new or updated reference information to the test environment mirroring production. We will receive referential data update requests during the project and in particular during the Test Phase preparation and test execution. The QA team will capture the date and time of the request. This team will request the appropriate update be run and capture the date and time the request was completed. We will verify the update and inform the requesting area of the update.

We will develop test cases and scripts based on the RTM to validate the solution meets your requirements. We will deliver the test results for the required phases using the Test Summary and Detail Reports format. The State will benefit from RTM to validate all requirements are met within the solution.

TEST05 The Contractor shall provide sufficient environments and resources for the following:

a. Synchronize the software and the data from the production environment and testing and impact analysis environment at a minimum on a quarterly basis or at the discretion of the Department.

b. Synchronize the software and the data from the production environment and training environment following software deployments.

c. Provide a fully functioning online test environment, which includes batch and online programs, files, and supporting systems.

d. Provide technical and functional support to create and analyze "what-if" scenarios and compare results between scenarios in the impact analysis environment. Provide an analysis of outcomes in impact analysis environment and another environment, such as production or test.

e. Provide State, Contractor, and IV&V staff a minimum of read-only access to all environments and tools.

f. Provide sufficient resources to support the execution of automated regression testing.

h. Provide comparative analysis support of regression testing results.

i. Conduct testing of approved system configuration changes, corrections or enhancements or before implementation.

j. Allow Department resources and contractors designated by the Department to create and edit appropriate data to support testing efforts, including provider, member, and reference data.

Optum will work with the DPHHS on the environments that are needed and update the environments in an agreed upon schedule at a quarterly minimum update with the appropriate access levels. The team can upgrade the environments to the latest software version and verify the functionality (e.g., batch, online, files, and supporting systems). We will provide a functional test environment that will enable testing of batch and online programs and supporting systems.

We will also show examples of what if scenarios and provide the necessary support of analysis. The comparisons will look at outcomes from an impact analysis from other environments to determine the impact of the change.

The DPHHS will have the necessary access to all environments and tools. At a minimum, this will be read-only access.

Our support will include comparative analysis of testing results for regression testing and we will provide resources to support regression testing for both manual and automated testing. We will also assist in the testing of approved system configuration changes, corrections, or enhancements before implementation and make certain that the DPHHS has appropriate access to tools and environments that will allow them to create and edit appropriate data to support their testing efforts.

TEST06 The Contractor shall ensure, in order to release code to UAT or production, it must meet the minimum acceptable defect levels:

- Critical: 100% have been resolved.
- High: 100% have been resolved.

We will work with the DPHHS to verify we address and resolve 100 percent of critical and high-priority defects before production implementation. For UAT, we will continue to address all critical and high defects and discuss all open defects before UAT implementation. We will work with you on defining priority level. Our typical priority levels are as follows:

Priority	Description
P1 – Critical	Blocks all business functions or a new functionality to be tested and testing works. If case code was move to production, business does not have a viable or acceptable workaround to use.

Priority	Description
P2 – High	Affect major business functions and there is no workaround for the impacted business functions, however other business functions are working correctly so the overall functionality is not blocked.
P3 – Medium	Loss of business function or other problem where workaround is present.
P4 – Low	Minor loss of business function, or other problem where easy workaround is present.

The defect management process implementation will be triggered through our online defect management tools to deliver quality applications in less time. We will enter all defects into the defect management tool for further analysis, tracking, and closure. Key features of the tool include streamlined integration with version control tools that makes it easy to track defects across solution components and configuration items. Our mature defect management process will enable us to validate the quality of our solution before entering production.

TEST07 The Contractor shall plan and execute testing for all inbound and outbound interfaces, ensure accurate and secure data transmission between the solution and the ESB and coordinate with external entities as appropriate.

We will plan and execute testing for all inbound and outbound interfaces and validate accurate and secure data transmission between our solution and the ESB. The testing we conduct between the integrated systems for the solution will include real time and batch interfaces. The test cases will cover details, such as simulating carrier integration, required input for each report/query/process, and the expected result of each transaction. The test cases will also exercise the unique interface and integration points across the services.

We will execute test cases to verify the functionality and outputs are correct and complete in the solution. Successful execution of the Release Test Plan will validate the functionalities. Our testing team will direct interface testing activities and operate the solution as defined by the Release Test Plan. We will provide error resolution and technical support throughout integration testing to facilitate the successful execution of the Release Test Plan.

TEST08 The Department plans to perform UAT on all software releases as part of the contract. The Contractor's approach to establishing testing environments should not impact the Department's ability to conduct continuous UAT in a separate, dedicated environment.

The primary goal of UAT is for Optum to assure DPHHS that the solution meets the business needs of the program. We will jointly define scenarios to validate the solution and tailor UAT activities to those scenarios. Business use case examples may include support for grievance and appeal research, provider or member contacts and escalations, or report and dashboard data analysis. After stakeholder agreement and meeting entry criteria, Optum will aid, measure, and report UAT activities in a separate, dedicated testing environment. We will provide support during development, execution, and defect analysis throughout the UAT stage.

TEST09 The Contractor shall facilitate UAT as follows:

a. Provide test cases and scripts from previous test levels.

b. Assist the Department in developing UAT test cases.

c. Provide a dedicated UAT environment to the Department and maintain the environment as needed to support continuous UAT throughout design, configure/build and testing.

d. Refresh data, execute processes, and migrate releases or code fixes as requested or on an agreed-upon schedule.

e. Provide test data.

f. Provide a mechanism for the Department to enter defects into the online defect-tracking tool.

Optum will work with the DPHHS to provide test cases and scripts from previous test levels and define scenarios to validate the solution, tailoring UAT activities to those scenarios. We will assist you in the development of your UAT test cases. Business use case examples may include support for grievance and appeal research, provider or member contacts and escalations, or report and dashboard data analysis.

After stakeholder agreement and meeting entry criteria, Optum will aid, measure and report UAT activities in a separate, dedicated testing environment. We will maintain the environment to support continuous UAT from the design phase through the testing phase. We will provide support during development, execution, and defect analysis throughout the UAT stage. We will perform all necessary activities, such as refreshing data and migrating releases and code fixes as required.

Optum will also provide support in creating test data and triaging defects discovered during UAT testing. We will provide the DPHHS with a method for entering defects into the online defect tracking tool. As a provider of benefits and services to our own client base across the country, we conduct UAT tests from both a supplier and user perspective. This experience translates to our understanding of user needs. We will stand ready to assist you as well as provide advice and counsel to you on the development of UAT.

TEST10 The Contractor shall provide Department resources or their designee access to test cases, test results and defect tracking via online tools. The Department reserves the right to inspect artifacts and results at any time.

Optum will provide the DPHHS access to the testing management tool that holds test cases, test results, and defects. You will be able to review and inspect all testing artifacts as needed.

The artifacts will describe the scope, approach, resources, and schedule of intended testing activities.

Optum has defined a documentation strategy and approach by which documentation and other key project artifacts will be developed, maintained, and made readily available to the DPHHS' authorized users.

TEST11 The Department reserves the right to conduct independent testing of the solution at any time. The Contractor must cooperate with the Department or its designee, and provide environments, data, and technical support for independent testing.

Optum will work with the DPHHS on all independent testing that is required to verify the functionality of the solution. We will work with mocked/stage data and not any data that contains PHI or PII.

TEST12 The Contractor's testing environments shall be sized to be capable of mirroring the production System in its infrastructure, files, databases, processing, and reporting.

We will provide an environment that mirrors production so that we can verify the system is able to perform at expected levels of performance.

The test environments recommended will support testing activities required for phased development approaches. Test environments may be required to support parallel testing efforts. We will make these decisions based on finalization of the project's development and implementation strategies and define them in the Release Test Plan. We will use our experience to provide the effective environments in balance with costs to the State.

TEST13 The Contractor shall work proactively with the State's designated testing resources to review all test results and provide the necessary system and functional information to create verification procedures and user acceptance test cases.

Optum will provide the DPHHS access to the testing management tool that holds test cases, test results, and defects. You will be able to review and inspect all testing artifacts as needed.

We will work with the DPHHS to develop the UAT Plan. It will include the timeline and description of the overall processes we will leverage throughout UAT. The plan will include a responsibility assignment matrix (RACI) with roles and responsibilities clearly defined.

To build out the test cases and procedures, we will create data sets in the environments that we identified for use in the UAT. We will use different quality gates to indicate that the data we created is ready for use as part of the entrance into the UAT execution phase.

TEST14 The Contractor shall coordinate with the Department and specific module component vendors to conduct integration testing.

The testing conducted between the integrated systems includes real time and batch interfaces. Optum will work with other vendors subject to Non-Disclosure Agreements or other security/confidentiality agreements. The test cases cover details, such as simulating carrier integration, the required input for each report/query/process, and the expected result of each transaction as well as exercise the unique interface and integration points across the services.

We will execute test cases to verify the functionality and outputs are correct and complete in the solution. Successful execution of the Release Test Plan will validate the functionalities. Our testing team will direct interface testing activities and operate the solution as defined by the Test Plan. We will provide error resolution and technical support throughout integration testing to facilitate the successful execution of the Release Test Plan.

TEST19 The Contractor shall develop test criteria and algorithms for expected outcomes prior to production of reports.

Optum will create and review with the State test criteria, test cases and scripts for expected outcomes as part of the test case creation. This will help us verify functionality based on the expected outcome and requirements.

We will design test cases to support the various, identified test scenarios that are relevant to a particular functional or technical requirement defined as in-scope for the testing phase. To best satisfy and meet client expectations, we will design test cases in a manner that provides testable measures and clear acceptance criteria. This practice will support our ability to measure the quality of the solution we have developed against the requirement criteria. It will enable us to validate that we have met the business expectation as defined and designed. As part of this effort, we will employ full traceability of requirements and trace the requirements to test cases and any subsequent defects.

TEST20 The Contractor shall ensure that the Project Work Plan allocates sufficient time to the State's user acceptance testing activities relative to the detailed scope of work, requirements and gaps, the number of manually executed test cases, and the complexity. of module integration. The Contractor' will be responsible for extended user acceptance testing if the proposed testing duration is not sufficient for the State to validate the module.

Optum will work with the DPHHS on creating and executing a PWP that addresses the DPHHS' UAT needs. If necessary, Optum will meet with you on any extension that is required so that enough testing time is given to complete UAT activities.

3.10.2.7 Training

The Contractor must provide training to designated MPATH team members, DPHHS training staff and other staff responsible for training to achieve an understanding of the new system, services, or release. The training will incorporate a train-the-trainer model so that participants can, in turn, provide training to additional users. Users must become proficient in using and viewing information in the Contractor's solution in order to ensure effective and efficient business operations and service delivery. The Offeror must describe their approach to meet each of the detailed training requirements defined in Attachment F, Requirements Matrix.

A comprehensive training program will help your MPATH, the DPHHS, and other authorized users realize the full value of the Optum Provider Services solution. Our training approach is flexible and responsive to changing demands. We will collaborate with you on the overall curriculum, course content, and schedule well in advance of training delivery. We will follow a train-the-trainer model to enable training participants to train other users. Our strategy for training is to introduce users to the new solution, empower them to make data-driven decisions, and be more effective and efficient in their everyday roles. We will offer solution training to the DPHHS, MPATH, third parties, as needed, and Optum throughout the life of the project:

Benefits

Well timed training combined with high-quality training documents:

- Unlock the power, versatility, and utility the Optum Provider Services solu ion provides to users
- Make sure our staff members assigned to meet your needs are well-informed, prepared and mo ivated employees
- Keep your user community's knowledge current with their real-time experience with the solution
- Give developers, analysts, and administrators a practical understanding of DPHHS goals and objectives

- **Implementation training:** During implementation, our training will focus on preparing MPATH, the DPHHS, third-party partners, and Optum users for testing and go-live operations.
  - In preparation for UAT, we will train involved individuals on the solution so they can adequately participate in the testing activities.
  - Prior to go-live, we will conduct intensive training for solution users to prepare them for full-production the day operations begin.
  - We will also conduct train-the-trainer sessions for identified State trainers who will then train remaining State staff.
- **Operations training:** During operations, we will conduct user training for the DPHHS project team and the Optum Provider Services user community. Our training program will help users be productive and successful in performing their required service functions throughout the project lifecycle:
  - New hires and new-to-Optum Provider Services staff members will receive their onboard processing and training before being assigned to work on the project.
  - The user community and project support staff will receive training, as appropriate, on solution modifications or procedural changes.

- **Turnover training:** During turnover, we will train the user community and appropriate MPATH, the DPHHS, and other designated staff on aspects of turnover of the solution.

ADDIE Instructional Design Methodology

We will minimize project risk by implementing the industry-standard ADDIE instructional design methodology, which has the following phases:

- **Analyze:** Optum will work with you to determine your training requirements. Instructional designers will evaluate the scope of the project to determine specific training needs and the most effective training delivery for trainees.
- **Design:** Based on the analysis performed, our instructional designers will determine the purpose and desired outcome of the training, the groups that need training, the required content, and the finalized delivery method for the training. We will set and approve trainee objectives in collaboration with you.
- **Develop:** Instructional designers will work with our SMEs to create training materials. These will include facilitator guides, participant guides, visual aids, Computer-based Training (CBT), videos, trainee activities, and other materials needed to support the training. We will submit all training materials to you for approval.
- **Implement:** We will deliver training using different methods, such as self-study, e-learning, CBT, and Instructor-led Training (ILT). We will work with you to select the best delivery method for your staff and stakeholders.
- **Evaluate:** The DPHHS, instructional designers, trainers, and our SMEs will work together to evaluate training effectiveness and modify training, as needed, over time.

Figure 3.47 shows the ADDIE phases and methodology.

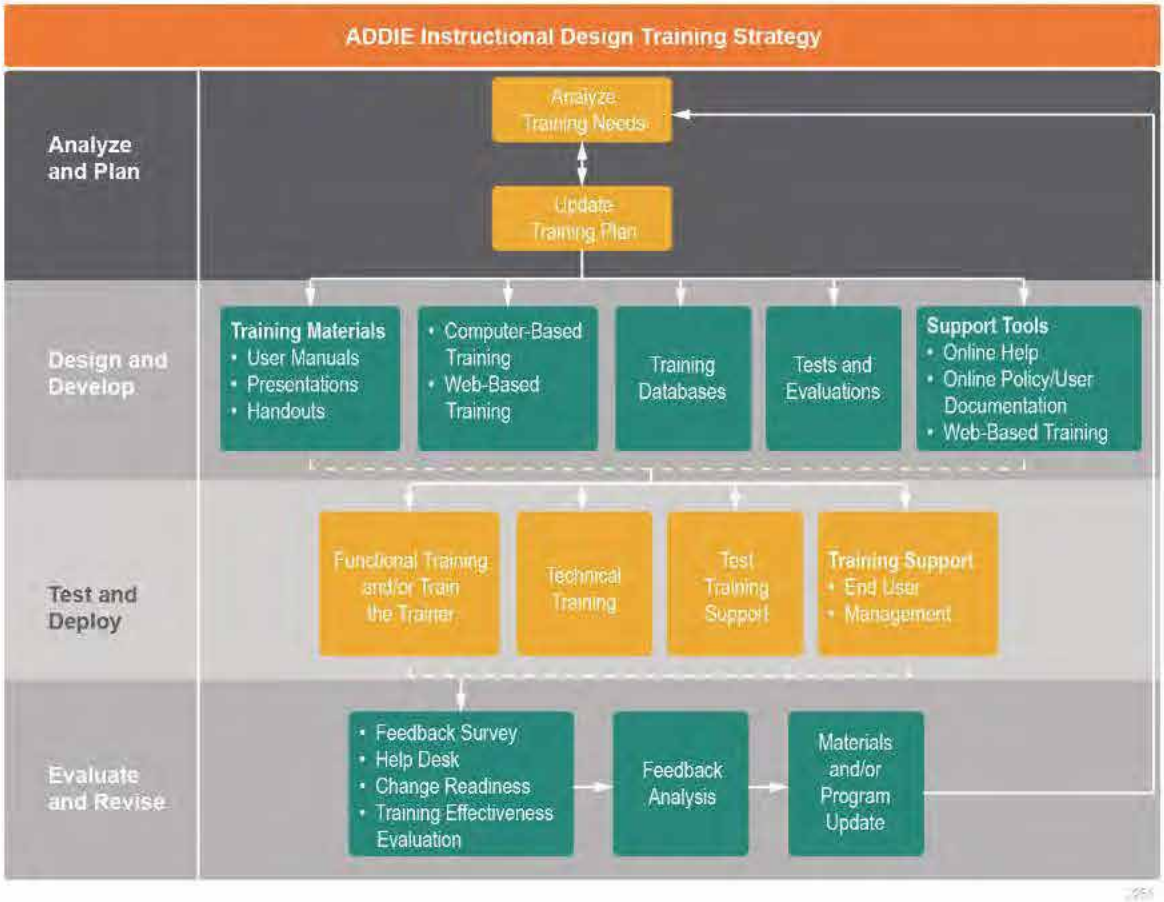


Figure 3.47: ADDIE Instructional Design Strategy.
As the DPHHS' needs or requirements evolve during operations, we will use our collaborative ADDIE ID model to process modifications to Optum Provider Services solution training elements.

We will leverage a collaborative planning, development, implementation, and evaluation process that we have fine-tuned across many commercial and government Medicaid implementations. Using this process, we will engage the DPHHS' stakeholders, supervisors, and managers by soliciting their participation and input as SMEs across the ADDIE phases. We will solicit participation and input during each stage of the instructional design process for new or modified training course units and materials. This strategy will help us keep training materials current with changes to solution features and functionality. It will also help us maintain stakeholder buy-in and ownership of Optum Provider Services business, system, and training changes. Working together, the DPHHS and Optum can quickly update and improve training and materials as needs change during implementation and operations.

Our straightforward process makes it easy for you to monitor, review, and approve our plans for training. You will know that we are adjusting our training as your program changes so that we focus on both program goals and training needs as we proceed. Although we plan for the best possible training outcome, we realize that careful evaluation and adjustments are necessary to reduce risk for the project. We will accomplish this through a strong partnership.

Training Plan

To prepare for training, we will create an initial comprehensive Training Plan upon completion of the Design Phase. We will design the plan according to your requirements to facilitate user

knowledge and use of the new solution and will conduct a joint walkthrough with you to review the draft plan and materials. Training materials will include the training curriculum we will follow to educate users. After the walkthrough, we will update or revise content based on your feedback and submit the plan to you for review and approval. After development and configuration, we will deliver a final version of the plan and training materials. We will maintain the Training Plan throughout the life of the project.

The Training Plan will clearly outline the training strategy and training schedule, serving as our roadmap for developing and implementing solution training. The plan will describe the delivery method, structure, timeline, and evaluation methods for training. It will include the following information:

- **Training approach:** Describes of our training approach with a focus on the train-the-trainer methodology, training objectives, and desired outcomes
- **Delivery methods:** Outlines our training delivery methods, such as self-paced CBT and Web-based training (WBT) modules
- **Training schedule:** Shows the schedules of our training courses
- **Training curriculum and courses:** Describes the curriculum we will present during training and describes the training courses
- **User groups and needs analysis:** Identifies the users we will train (e.g., Optum Provider Services solution users, the DPHHS, MPATH, stakeholders), and describes how we will conduct an assessment of each target audience to determine their knowledge and skills
- **Documentation and maintenance:** Describes our proposed training materials and documentation and our approach for updating and maintaining them through all project phases
- **Training on new functionality:** Explains our approach to providing the training required to support new functionality or major software releases that change the user interaction
- **Feedback:** Describes our process for obtaining feedback (e.g., end-of-training survey) and incorporating feedback into our training to improve the effectiveness of our train-the-trainer approach
- **Evaluation methods:** Describes our methods for evaluating the effectiveness of training, such as end-to-end scenarios and knowledge checks

We will review the Training Plan with you at least annually and update it for operations to describe the training required to support the operational aspects of our solution. The Training Plan will guide the training design and delivery for various audiences supported during operations. The groups we train will include users from the DPHHS, MPATH, third-party vendors, and Optum support staff learners. If we identify System Enhancement Pool activities that affect training, we will update the Training Plan as needed. Figure 3.48 shows a sample Training Plan table of contents.

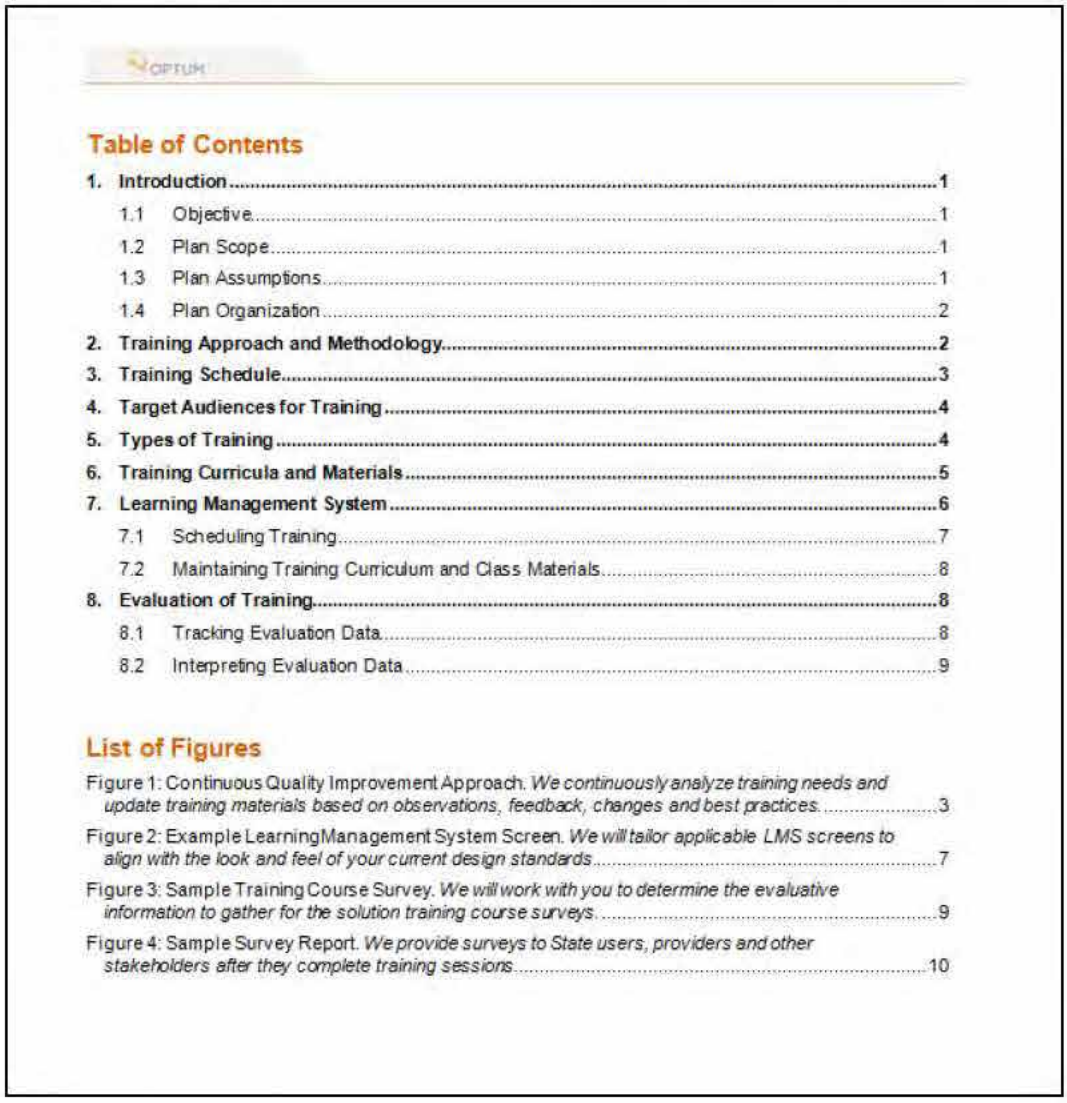


Table of Contents

1. Introduction 1
1.1 Objective 1
1.2 Plan Scope 1
1.3 Plan Assumptions 1
1.4 Plan Organization 2
2. Training Approach and Methodology 2
3. Training Schedule 3
4. Target Audiences for Training 4
5. Types of Training 4
6. Training Curricula and Materials 5
7. Learning Management System 6
7.1 Scheduling Training 7
7.2 Maintaining Training Curriculum and Class Materials 8
8. Evaluation of Training 8
8.1 Tracking Evaluation Data 8
8.2 Interpreting Evaluation Data 9

List of Figures

Figure 1: Continuous Quality Improvement Approach. *We continuously analyze training needs and update training materials based on observations, feedback, changes and best practices.* 3
Figure 2: Example LearningManagement System Screen. *We will tailor applicable LMS screens to align with the look and feel of your current design standards* 7
Figure 3: Sample Training Course Survey. *We will work with you to determine the evaluative information to gather for the solution training course surveys.* 9
Figure 4: Sample Survey Report. *We provide surveys to State users, providers and other stakeholders after they complete training sessions.* 10

Figure 3.48: Training Plan Table of Contents.

We will conduct a joint walkthrough with you to review the draft Training Plan and materials, updating them as needed.

Learning Management System

Optum uses a Learning Management System (LMS) to provide and maintain training materials and deliverables. Our LMS is already deployed inside and outside of our company and is used by thousands of employees, clients, and customers. We configure access to the LMS so that authorized users can access their role-specific materials through the LMS portal. We will manage curriculum through the LMS; therefore, users can schedule their time around competing work priorities. Figure 3.49 shows an example of an LMS home page.



Figure 3.49: Sample LMS Home Page.
We can tailor the LMS to meet your training requirements.

During initial and ongoing training, we will offer online self-paced and ILT training though the LMS. The LMS will store material that includes the following:

- Calendar of ILT training sessions and webinar events
- Webinars
- eLearning videos
- CBT modules
- WBT modules
- LMS procedures
- User manuals
- Reference materials
- Approved training plans
- Lifecycle training documentation, such as facilitation materials, activities, user guides, and At-a-Glance guides

Users will receive training on using the LMS appropriate for their roles. When new users register in the LMS, the system will generate an email containing instructions for using the tool. The LMS home page will contain user-friendly helpful hints to navigate the LMS portal. From the LMS, trainees can manage their training enrollment, complete CBTs, and provide class evaluations. We will track attendance, registration, and training completion through the LMS. This includes completion of online training webinars. The LMS will provide reports to the

DPHHS and Optum detailing participation rates. We will record training webinars and place them in the LMS so that authorized users can access them at their convenience.

During implementation, the LMS will be available to authorized trainers, MPATH team members, your staff, and designated third-party vendors to access appropriate training and materials.

Training Schedule

We will create and maintain a full training schedule for implementation, as Figure 3.50 illustrates.

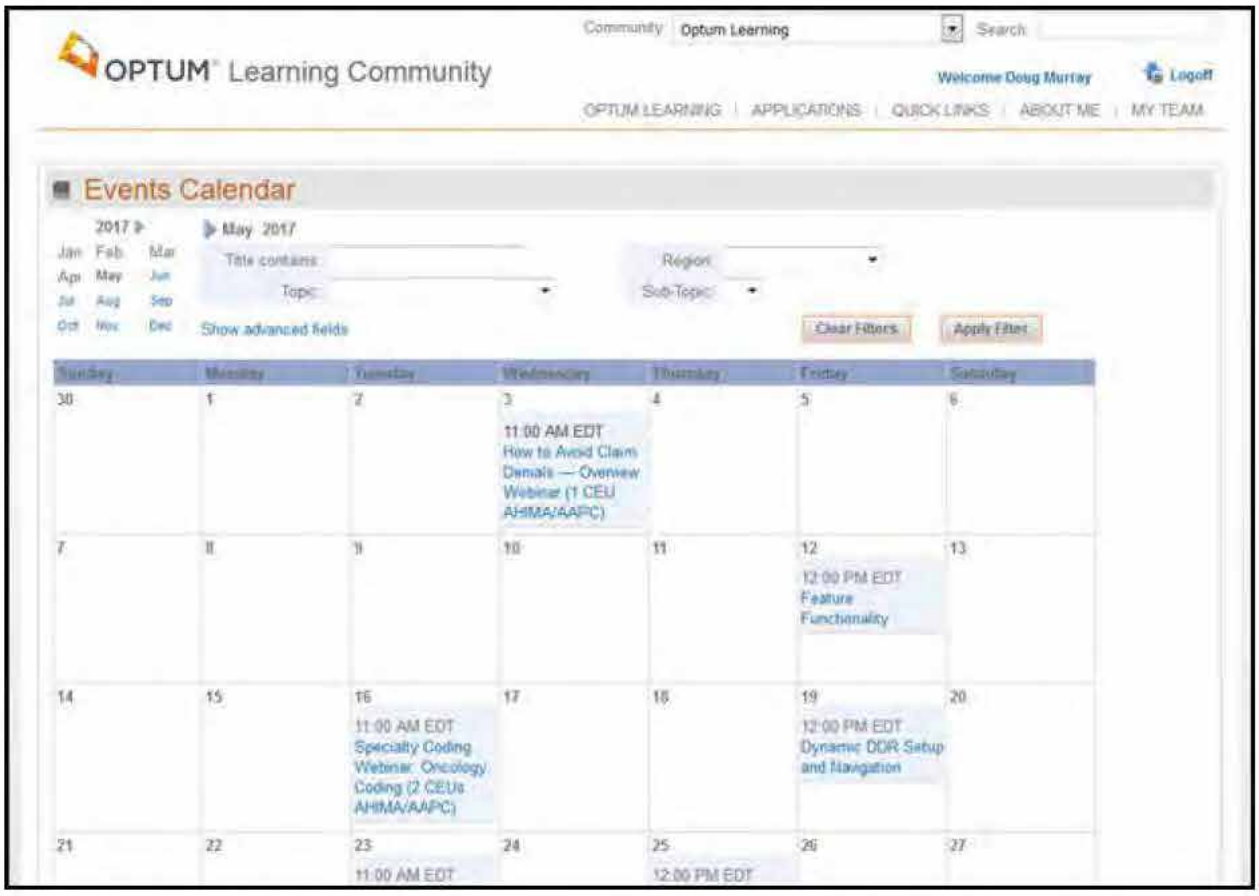


Figure 3.50: Sample Training Schedule.
We will post the training schedule to our LMS for easy access, viewing, and enrollment by users.

After the DPHHS approves the training schedule and training materials, we will perform preparatory activities, such as posting the training schedule in the LMS for easy access, viewing, and enrollment by users. They will access the training schedule easily from LMS links to coordinate training around other job priorities. The training schedule will include the schedule of user classes. We will deliver training at various points throughout implementation and operations as described in the PWP.

Training will begin with supervisors and managers, who will follow the same curriculum as the operations teams. As the operations supervisory team transitions from the classroom, the supervisory team will conduct on-the-job training. This will continue until users achieve necessary competency levels to successfully perform their roles in the production environment.

During implementation, we will train individuals who need to navigate solution applications when they are assigned to the project. This will include individuals involved in UAT. During UAT, users will perform tasks with the Optum Provider Services solution applications with real-world scenarios to validate that the applications will function as expected before go-live.

Training Materials

We will design, develop, and deliver training based on ADDIE concepts, including content specific to the features of our solution. We will update training materials within 45 days of a release moving into production. To provide meaningful documentation, our training staff members will collaborate with the developers of our solution's user interface, reports, and models. They will also collaborate with those preparing system documentation and online help.

Our implementation preparatory activities will include finalizing the training content and posting online CBT and WBT training materials and course units within the LMS. Because LMS access is configurable, authorized users can retrieve their role-specific materials through the LMS portal. As we complete these preparatory activities, our instructional design team will meet with the Optum training delivery team to initiate train-the-trainer activities.

After our solution goes live, we will implement a quarterly curriculum update cycle. This approach will help us capture changes in the training content as close to real time as possible and maintain up-to-date materials. Training material changes can originate from different sources, including the following:

- Company-wide initiatives
- System releases and updates
- Process updates
- Business partner feedback
- Training delivery feedback

The training team will participate in quality review meetings and work with operations and the DPHHS if we determine additional training can improve quality metrics. These metrics can include complying with customer service requirements, adhering to process, and meeting client requirements. If we identify gaps, the training team will provide support by providing classroom training, one-on-one instruction, or additional self-guided learning materials.

Train-the-Trainer

Optum trainers undergo extensive outcome-based training on quality training techniques. To prepare Provider Services module trainers, we will use our mature train-the-trainer process. It includes curriculum hand-off (instructional designers to trainers), material review, practice, and observation of first-time delivery. Using this approach, we reduce risk for the Provider Services module, and validate our trainers are prepared to deliver quality instruction. Our train-the-trainer approach has three components:

1. **Trainer readiness:** The instructional designer or the training lead will conduct the train-the-trainer readiness sessions. These sessions will include:
   - Materials walkthrough and discussion of key learning points in each lesson
   - System demonstration, if applicable
   - Review of PowerPoint slides, trainer guide notes, and any other training resource documents designed for the trainer's use

- Designated preparation time the trainer can use for additional study, curriculum review, or other preparation

2. **Trainer readiness evaluation:** The evaluation comprises observation and assessment of trainers before classroom delivery. It confirms they understand the Optum Provider Services solution business, system, and operational concepts and content to prepare trainees for success in production. This includes a complete training demonstration and teach-back so that the instructional designer or training lead can assess the participant's knowledge and training skills. The evaluation can occur during or after the train-the-trainer session. After watching the training demonstration, the instructional designer or training lead will complete a teach-back evaluation form.
3. **Trainer observation and feedback:** During the trainer's first classroom session, the training lead or manager will sit in as an observer to verify the trainer's competency in the classroom environment. The observer will complete a teach-back evaluation form to document the findings. He or she will share the evaluation findings with the teacher to identify areas for improvement and provide positive reinforcement.

Figure 3.51 illustrates our train-the-trainer model.

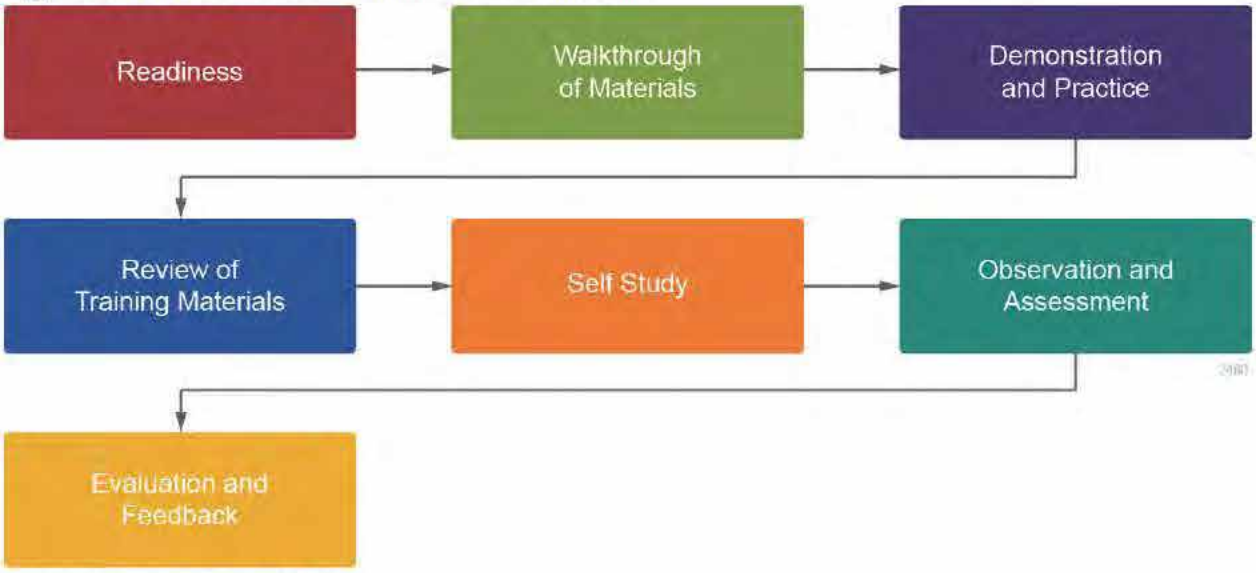


Figure 3.51: Train-the-Trainer Model.
Our train-the-trainer model will reduce risk for the Provider Services module by making sure our trainers are prepared to deliver quality instruction.

Evaluation

We will evaluate the effectiveness of training and measure the transfer of knowledge using various methods. The team will choose each method based on audience needs and base success parameters for these measures on the project SLAs. The evaluations include the following:

- **End-to-end scenarios:** We test trainees on a process from start to finish. The scoring determines if the trainee is ready to move to the floor or if remediation is required.
- **Knowledge check:** We phrase key topics that we addressed during training as questions. Participants provide an answer based on their retention of the material.

We will design each assessment method so that the DPHHS and our staff have an appropriate understanding of business requirements, processes, and how to use the relevant systems for their work.

We will also implement the end-of-training survey. This will gauge the comfort level of the trainees upon leaving the class. We will load the training evaluation tool into the LMS. Each trainee will receive a request from the LMS to complete an evaluation survey. The system will generate a report of the survey results, which our training team will analyze to identify opportunities for improvement and trends.

Training team leadership will communicate the training evaluation results to the DPHHS and our operations and project managers. We will formulate recommendations and identify improvements we can make for future curriculum revisions and delivery.

After we implement our solution, the training team will participate in quality metric meetings. We will work with you and your key stakeholders to identify gaps in knowledge or skills. If we identify training gaps, we will adapt the curriculum to include additional material, a training update, or identify other approaches to meet training participant needs. Instructional designers will determine where a training need exists and recommend the appropriate solution to meet that need.

Curriculum Development

Our curriculum development methodology is outcome-focused and customer-centric. We will tailor development to your goals and objectives and design our curriculum to deliver accurate and timely results. We use a standard, modular design for all of our training courses, including high-level agendas for each training class. These will include a description of the staff and users to train. The curriculum we develop will provide the most concise and effective learning experience possible. We will base the curriculum design and agendas on the learning needs identified for the roles supporting your providers. We will also rely on lessons learned from our past development and implementation of a diverse catalog of training curricula. The resulting curriculum design for the Optum Provider Services solution will have these fundamental objectives:

- Verify that training content is accurate and consistent with current the DPHHS business processes
- Focus training content only on information that is critically relevant and necessary for learners to have success in their roles
- Present key learning concepts to build on and reinforce previously covered skills and topics
- Incorporate appropriate levels of interactivity into the training content, including hands-on practice and realistic case scenarios that simulate day-to-day job responsibilities
- Create training content that is easy to update in support of ever-changing business needs

User Groups

We will tailor our solution training program to support specified user roles. Because users will have varying levels of exposure to the solution, we propose a multi-tiered training curriculum with proficiency levels from beginner to expert. The following table shows examples of training courses we will design to help users in different user groups successfully perform their jobs.

Trainee Group	Topic Areas	Training	Delivery Medium
Optum Provider Services solution users	• Member services • Provider enrollment and maintenance • Portal features and usage	Courses designed for the users' functions to maximize quality and productivity	• Classroom training • Online training • User manuals/job aids
State/MPATH	• Portal features and usage • Reporting	Courses designed to help understand the Optum architecture and how to conduct transactions on the Optum platform	• Classroom training • Online training • User manuals/job aids

Training Delivery Methods

We use a collaborative and multifaceted approach to training delivery. The training materials and delivery we provide will be appropriate for each job role to meet the training objectives. We will offer virtual and classroom training delivery.

Instructor-led Training: Optum will provide a simulated training production environment that will mimic the system functionality that authorized users will experience in daily operations. Partitioned from the production environment, the training environment will support hands-on, face-to-face, and remote-access training.

Instructor-led skills labs are an effective learning method to cover advanced skills or updated operational processes. Skills labs focus on meeting specific performance metrics. We can customize the labs to include any combination of instructor-led lecture and discussion, hands-on practice, and interactive exercises and activities.

Results

Our training strategy is results-based and client-focused.

- Continuous project lifecycle support to user communities
- Favorable survey feedback consistently received from state and commercial clients nationwide
- Consistently meets client-specific organizational and programmatic training goals

Web-based training: We will provide users access to Web-based training, or eLearning, courses they can access anytime, anywhere over the Internet. Web-based training resources will help users in long-term learning, enabling them to participate in training remotely and independently. Options include on-demand training in various self-directed formats, such as recorded webinars and training videos. In addition, we will provide WebEx phone and remote access/video conferencing capabilities that enable off-site users to participate in on-site, real-time training events without traveling. We can record and save WebEx sessions for on-demand access by new users and users who want to review previous training sessions.

Online self-paced training: We will provide video, CBT, and WBT modules in the LMS. Users can complete these training modules at their own pace, 24 hours a day, 365 days a year.

We can attribute a large part of our success with commercial state projects to the continuing support we provide to user communities with our full lifecycle training. We will work with you so that all aspects of our training meet and exceed your standards and expectations.

TRN01 The Contractor shall provide technical training to agency project resources and designated contractors to develop an understanding of how to monitor the system using available tools and dashboards while leveraging technical and functional documentation and/or reports.

We will provide the technical training to Agency project resources and designated stakeholders to understand how to monitor the Optum Provider Services solution and system using tools and dashboards. This training will include technical and functional documentation, as well as reports generated from the solution.

TRN04 The Contractor shall update training materials when changes occur.

We will work with you to review training materials and curriculum regularly to make sure they align with your training requirements and our quality standards, updating them as needed. Training material changes can originate from different sources, including the following:

- Company-wide initiatives
- System releases and updates
- Process updates
- Business partner feedback
- Training delivery feedback

Ongoing reviews of training materials will help us capture changes in the training content as close to real time as possible and maintain up-to-date materials.

TRN05 The Contractor shall collaborate with the agency to finalize a training schedule.

We will work with you to create and maintain a training schedule for all project phases. We will post and manage the schedule within the LMS we use for the project. Training participants will have access to the LMS 24 hours a day, 365 days a year, except during scheduled downtime that the DPHHS has approved.

TRN06 The Contractor shall maintain and update the training environment with training data to use during user training.

We will partition, maintain, and update a separate user training environment from the production environment. Within this partitioned environment, we will train users on the functionality of the solution without affecting production data. This training environment will enable training participants to work with data, processes, hardware, and software similar to the ones they will encounter as system users. We will refresh the training data and components periodically to provide continuous improvement for our training programs and classes.

TRN07 The Contractor shall provide train-the-trainer sessions for Agency resources or designated agency resources and other staff responsible for training.

We will use our mature train-the-trainer process for Agency and designated resources that will be responsible for training. After completing this training, trainers will qualify to continue the direct instruction to Agency users as you have specified, reducing risk for the Provider Services module.

A trainer's skillset is critical for effective curriculum delivery. Optum trainers participate in extensive outcome-based training and testing on quality training techniques. We have a fully developed train-the-trainer process from curriculum hand-off to teach-backs and observation of first time delivery. This approach enables us to make sure trainers are prepared to deliver the appropriate training to users.

We will use a three-step train-the-trainer approach:

1. **Trainer readiness:** The instructional designer or the training lead will conduct the train-the-trainer readiness sessions. These sessions will include:
   - Materials walkthrough and discussion of key learning points in each lesson
   - System demonstration, if applicable
   - Review of PowerPoint slides, trainer guide notes, and any other training resource documents designed for the trainer's use
   - Designated preparation time the trainer can use for additional study, curriculum review, or other preparation
2. **Trainer readiness evaluation:** This includes a complete training demonstration and teach-back so that the instructional designer or training lead can assess the participant's knowledge and training skills. The evaluation can occur during or after the train-the-trainer session. After watching the training demonstration, the instructional designer or training lead will complete a teach-back evaluation form.
3. **Trainer observation and feedback:** During the trainer's first classroom session, the training lead or manager will sit in as an observer to verify the trainer's competency in the classroom environment. The observer will complete a teach-back evaluation form to document the findings. He or she will share the evaluation findings with the teacher to identify areas for improvement and provide positive reinforcement.

TRN08 The Contractor shall utilize a variety of delivery methods to best meet the training objectives. Examples include online self-paced training presentations, in-person classroom setting, written material, and demonstrations.

We use a collaborative and multifaceted approach to training delivery. The training materials and delivery we provide will be appropriate for each job role to meet the training objectives. We will offer virtual and classroom training delivery. These methods will include:

- **Online self-paced training:** Video, CBT and WBT modules, as appropriate
- **In-person classroom training:** Instructor-led sessions through classroom, trainer-led skills lab, demonstrations, or individual/small group training
- **Written material:** Independent learning guides and training materials appropriate for specific job roles

Class participant materials can include student manuals, desk reference guides, activities, and other supporting documentation. Each instructor-led training event will include a trainer guide with instructions for presenting the material, including talking points and activity instructions. These materials will help the trainer deliver a comprehensive training experience in the classroom or online during Web-based learning events.

The DPHHS will review and approve all training locations and materials in advance through the life of the contract. This review and approval will verify your staff and stakeholders acquire the knowledge, skills, and resources they need to perform their day-to-day work.

Our LMS will house our online training content and will manage registrations, as well as track attendance and course completions for reporting. Users will receive training on using the LMS appropriate for their roles. When new users register in the LMS, we will generate an email containing instructions for using the LMS. The LMS home page also contains user-friendly helpful hints to navigate the LMS portal.

TRN09 The Contractor must provide training necessary to support new functionality and/or major software releases that materially change the user interaction.

We will provide training when a new functionality or software release affects the user's ability to work with our solution. We will update the training materials, deliver appropriate training, and assess user understanding. This approach will validate user understanding of the changes and how to incorporate the new knowledge into their daily work.

TRN10 The Contractor shall provide training to Agency staff and other designated module vendors on the overall data management strategy and investigating data or process issues related to module integration.

We will work with you and your designated module vendors to provide training on our solution data management strategy and module integration. We understand the importance of our solution's interoperability with the other MPATH modules to your overall modernization effort for the Montana Healthcare Programs enterprise.

TRN11 The Contractor shall develop and maintain electronic training guides and materials to support the Train the Trainer instruction.

We will develop and maintain the training materials to support the train-the-trainer program, storing the documentation in LMS. As previously noted, each instructor-led training event will include a trainer guide with instructions for presenting the material, including talking points and activity instructions. These materials will help the trainer deliver a comprehensive training experience.

TRN13 The Contractor shall provide training and support to State staff and individuals designated by the State (e.g., IV&V, QA/QC vendor), on the use of DDI tools provided by the contractor. This may include traceability tools, document repositories and testing tools.

We will provide training and support to your staff and designated individuals on using our project management tools we will use during DDI. These tools will include the following:

- **Microsoft SharePoint document repository:** Deliverables and project-related work product storage and management
- **Microsoft Project:** The tasks, milestones, and deliverables logically sequenced for this project
- **HP Application Lifecycle Management (ALM):** ALM software for requirements traceability, test management, and defect tracking
- **ServiceNow:** Change control, help desk ticketing, and incident reporting
- **IRAAD:** The Issues, Risks, Actions, Assumptions, Decisions (IRAAD) tool to track project action items, decisions, issues, risks, and defects

TRN14 The Contractor shall provide training on the system for UAT testers. The Contractor shall provide updated User and System Documentation to UAT testers to support the UAT effort.

We will deliver training for UAT testers before implementation. Our updated iterations of user and system documentation will be available for UAT testers. Delivering training before UAT helps users gain the knowledge they need to thoroughly test the solution. UAT testers will help us validate the Optum Provider Services solution meets the needs of your users. Feedback from UAT testers will also help us identify opportunities for improving our documentation. Based on lessons learned and feedback we receive during UAT, we will update documentation and training materials, as needed, before implementation training.

3.10.2.8 Implementation and Acceptance

Prior to implementation, the Contractor must demonstrate readiness to implement the solution and to provide operational support and maintenance of the proposed solution(s) for the remainder of the Contract term. The Contractor is responsible for managing the end-to-end implementation of the proposed solution. DPHHS expects the Contractor to help formulate strategies for a successful transition.

DPHHS must formally approve the implementation of the solution based on pre-defined acceptance criteria. DPHHS's acceptance of the solution will initiate the Operations, Maintenance and Configuration phase of the contract. The Offeror must describe their approach to meet each of the implementation and acceptance requirements defined in Attachment F, Requirements Matrix.

As a leader in information and technology-enabled health and business services, we have extensive experience implementing products and services to various government and private clients. These successful implementations give Optum a strategic advantage by knowing which strategies work best in a given situation. The Optum Provider Services solution will leverage this experience in implementation planning and operational readiness to make sure the State achieves the ideal implementation outcome.

Implementation Planning

Throughout our implementation plans, we include proven communication protocols, which are integral for our successful, on-time delivery culture. Optum develops a big picture strategic goal that clearly defines the objectives and critical tactics for success. Furthermore, we develop each communication plan iteratively based on the needs of each client's implementation plan. The plan aligns with each client's identified stakeholder communication channels. This well-constructed communication provides a platform to disseminate accurate communication and reinforce a culture that commits to a successful Provider Services module implementation.

In concert with best practices set forth by the PMI, ITIL v3, and other industry leaders, we will plan and execute our product implementation with you and your stakeholders experience foremost in mind. Verifying that client business objectives are met at the desired, agreed-upon timeline, our solution provides an implementation approach that is rapid, business-focused, and broadly adaptive.

Optum will produce an implementation plan and release schedule that supports the deadlines approved by the DPHHS. We will update and manage our proven release management processes that support multi-vendor engagements to meet your goals, and deliver our solution with the least risk. As the implementation plans are documented, Optum will consult the DPHHS and other stakeholders to verify all stakeholder feedback is reviewed, analyzed, and adapted to the plans. These joint activities will help us determine the implementation strategy that best fits your needs while formalizing release schedules that contain accurate task relationships, durations, start and end dates, and other pertinent information.

This exercise will reduce implementation risk by verifying the master integration plan is realistic and achievable.

Figure 3.52 provides an end-to-end snapshot of the process that Optum will follow during the Provider Services module implementation.

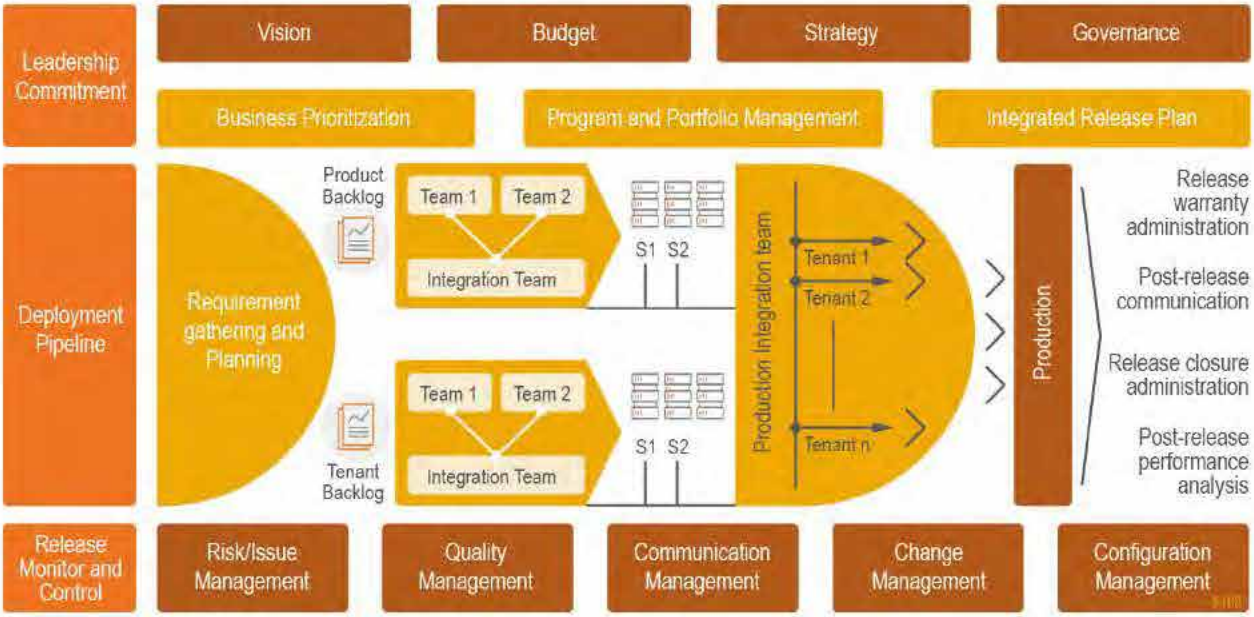


Figure 3.52: Provider Services Module Release Management Process.
The Provider Services module provides a proven release management process to communicate with all stakeholders, mitigate risks, and provide assurance that releases will be non-disruptive.

Furthermore, Optum will coordinate all release activities with the DPHHS and the other vendors supporting MPATH. This will include developing a release management process appropriate for your multi-vendor approach, managing code promotion into the production environment and maintaining an updated release schedule. To align with strategies that continuously deliver successful implementations, Optum will regularly and proactively review the Provider Services module implementation plans and schedules to verify updates and modifications necessary to deliver a successful product implementation are captured accurately. Cognizant of the effects that such updates can have on the DPHHS or other stakeholders' plans, we will review changes to previously agreed-upon plans thoroughly following appropriate impact analysis and approval through established procedures.

Adhering to the strategic and tactical instructions provided in the Attachment F, Requirements Matrix, Optum will provide release schedule information to the DPHHS and other stakeholders on an agreed-upon frequency.

As the Provider Services module is configured, Optum will use the DevOps application configuration model. DevOps is an innovative approach to software code management, configuration, and deployment that reduces risk and speeds solution delivery. With a strong emphasis on automation, it promotes collaboration and communication between the development and technical operations teams. DevOps is an important element of our OSAM SDLC. We are constantly evaluating new tools to provide our teams with additional capabilities and will always employ the most appropriate toolset.

Operational Readiness

Comprehensive testing and readiness reviews are standard elements of our implementation approach, and we have successfully performed these reviews on projects similar to the Optum Provider Services solution. We will work with you to coordinate operational readiness activities. During readiness planning and preparation, we will focus on activities, detailed checklists and

summations, communication and reporting. We will complete and remediate any issues before we demonstrate our end-to-end system readiness on the operational start date.

While we will conduct the majority of readiness just before the operational start date, we will commit to conducting readiness assessment activities throughout the operation as we implement new processes or technologies. Our readiness methodology will position us to continually learn, assess and remediate issues. Our readiness phased approach will enable us to conduct a full end-to-end assessment and demonstrate all functional and contractual requirements.

Our iterative development and delivery approach offers you many advantages and includes:

- Faster time to value as releases are implemented more quickly
- Development follows a continuous improvement cycle, exposing flaws faster and reducing waste

Our operational readiness activities will begin during UAT. As you perform UAT of our solution before go-live, we will assist you throughout the process. In support of UAT, we will begin operational support of each release as it is tested. Support for our solution users is a key component of operational readiness, and it actually begins prior to go-live. We begin user support activities as part of the operational readiness test activities that occur during implementation. We will provide the defined help desk services to support the Optum Provider Services solution. We will establish and provision the help desk as part of operational readiness activities, so that upon go-live, we are poised and ready to support your users.

During operational readiness testing, we will perform specific implementation and operations functions described in the Operation Readiness Review Checklist. This will help us validate that the solution is installed and configured in the production environment, and end users have been satisfactorily trained. These tasks may include performing final file conversions, validating network performance, establishing end user support, and updating the work plan and other project documentation.

After fully testing our solution interfaces during integration testing, we will work with the identified state personnel resources to plan and schedule operational readiness activities and final production deployment. These final integration steps are built into our deployment checklists. When deployed, we will conduct final validation within the production environment and stay in frequent communication with the state personnel resources to monitor and validate that interfaces are functioning as designed.

We have conducted operational readiness activities for the State of Arkansas and Indiana, among others, according to the planning methodology and readiness testing approach described above. By following our proven processes, our customers enjoy the benefits of release stability, an Agile approach to UAT, regression testing, strict change control, and a low defect rate.

Technology

DevOps promises to revolutionize the landscape of software configuration, development, deployment, and maintenance. As Figure 3.53 illustrates, a comprehensive suite of tools complements our DevOps framework.



[redacted]

[redacted]

Security

At Optum, security is the responsibility of every staff member. We employ advanced security tools and techniques to stay ahead of those who would compromise the data under our stewardship. On an annual basis, we invest heavily in its security posture by employing security professionals to actively defend against cyber threats around the world. These investments apply to all aspects of our posture, including our physical security (building access), logical security (network and internal computing security), and our education programs for employees and our provider communities alike. Optum, and by extension, the DPHHS Provider Services module, will benefit from this investment and heightened security posture.

As we implement our solution, we will keep the information assets DPHHS entrusts to us under the same rigorous security standards as all data entrusted to the organization. By applying advanced security principles and practices, we will not waver in our commitment to prevent that data from falling into unauthorized hands.

Optum constantly evolves security practices to meet the threats of today and tomorrow. Our security professionals scan the globe for the latest emerging threats, and take measure to prevent our systems from being affected. Our posture has succeeded in preventing data loss to some of the more high profile cases in recent news, such as the recent ransomware attacks targeting providers, Petya, and Wannacry. Petya, in particular, targeted health care providers.

This is consistent with recent reports[4] indicating that approximately 88 percent of all ransomware attacks target health care entities.

Our security posture does not merely focus on perimeter security; it percolates through all aspects of our operating environment. Developers are particularly motivated to write simpler, cleaner code, because well-written and readable code is inherently more secure.

Some of the tools we use to make our code, frameworks, and backend processes secure are:

- Static code analysis before every deployment
- Formal Architecture Review Boards (ARB)
- Formal and informal code reviews
- Restricted access to sensitive code
- Periodic evaluation of vendor certifications
- Periodic vulnerability scanning

In addition, we implement best practice checklist-based code reviews because we have experience with major improvements in code quality when multiple reviewers review code using standardized tools. We use static code review checklists to enforce standards in coding and automated testing.

[redacted]

[4] Healthcare IT News: "Ransomware: 88 percent of U.S. attacks hit healthcare entities" 07 Sept, 2016, http://www.healthcareitnews.com/news/ransomware-88-percent-us-attacks-hit-healthcare-entities

[redacted]

Release Management

We use a proven, field-tested implementation and release process that we will adapt to facilitate our solution delivery. Our release management process considers multi-vendor, multi-stakeholder environments, and is driven by people, process, and technology.

The Optum release management methodology promotes successful deployments and non-disruptive releases. Using this methodology, we continually apply changes to our critical health care systems using processes and procedures that minimize or eliminate disruption to existing operations, while preserving the integrity of existing COTS products.

Complementing our implementation strategy is the release management process. This process will capture and present all processes and tools that we will use to deliver a successful release of our solution. The process encapsulates all activities that Optum will perform to verify integrity of the solution.

Through coordination with the DPHHS, and other MPATH vendors and third parties, we will update our release management process to support your multi-vendor approach. Leveraging processes and tools that have been employed to manage previous releases, the DPHHS-specific Application Configuration and Maintenance Plan will document activities, phase-gates, and other processes that Optum will execute to manage and validate code releases through the environments.

In addition, we will address maintaining an updated release schedule as part of this plan. We will deliver the Application Configuration and Maintenance Plan to the DPHHS according to the schedule identified in the Attachment F, Requirements Matrix, documentation requirement DOC04.

For each respective DPHHS Provider Services module release, previously identified stakeholders will create, review, and approve a release plan. Key personnel from the DPHHS, Optum, and other vendors will work together to confirm the release plans include activities and timelines that all responsible parties can meet realistically. Furthermore, these sessions will help identify, plan for, and determine response for potential project risks that can ensue and capture in the IRAAD.

Through effective planning, organizing, staffing, and leading, the project team will engage DPHHS personnel to help promote transparency of actions across all stakeholders. This will help all parties remain properly informed and in a position to deliver a successful product release.

Following the best practices set forth by previous successful release management endeavors, Optum will create an approval/deployment package and send it for stakeholder approval. ServiceNow acts as our solution's CMDB. This is crucial in our deployment process by setting up appropriate governance and controls on the deployment process.

Release Deployment/Code Promotion to Production

Pursuant to activities/tasks documented as part of the Application Configuration and Maintenance Plan, Optum will use a deployment readiness checklist to verify each release deployed to the DPHHS production environment meets or exceeds the quality level established.

In addition to verifying the deployment readiness checklist is complete with all the deployment activities, schedule and back out procedures, we will capture each potential deployment risk, along with link(s) provided to each risk mitigation strategy.

Before release deployment, Optum will invite the DPHHS stakeholders to take part in, and provide sign-off on all deployment activities. As part of the go/no-go meetings, we will present key metrics to appropriate stakeholders. This will help determine whether code can be promoted to production environments, or if further data on code quality, test results, or other criteria is required.

Before deploying the DPHHS Provider Services module code to the production environment, we will prepare the DPHHS team with various trainings, dry runs, and simulation exercises to better prepare stakeholders for the final deployment exercise. Our Maintenance and Operations teams will execute production deployment and our command center will monitor it.

The Provider Services module environments, as Figure 3.54 illustrates, represent a logical flow of code promotion through various development and test environments, culminating in either Model Office (pre go-live) or production.

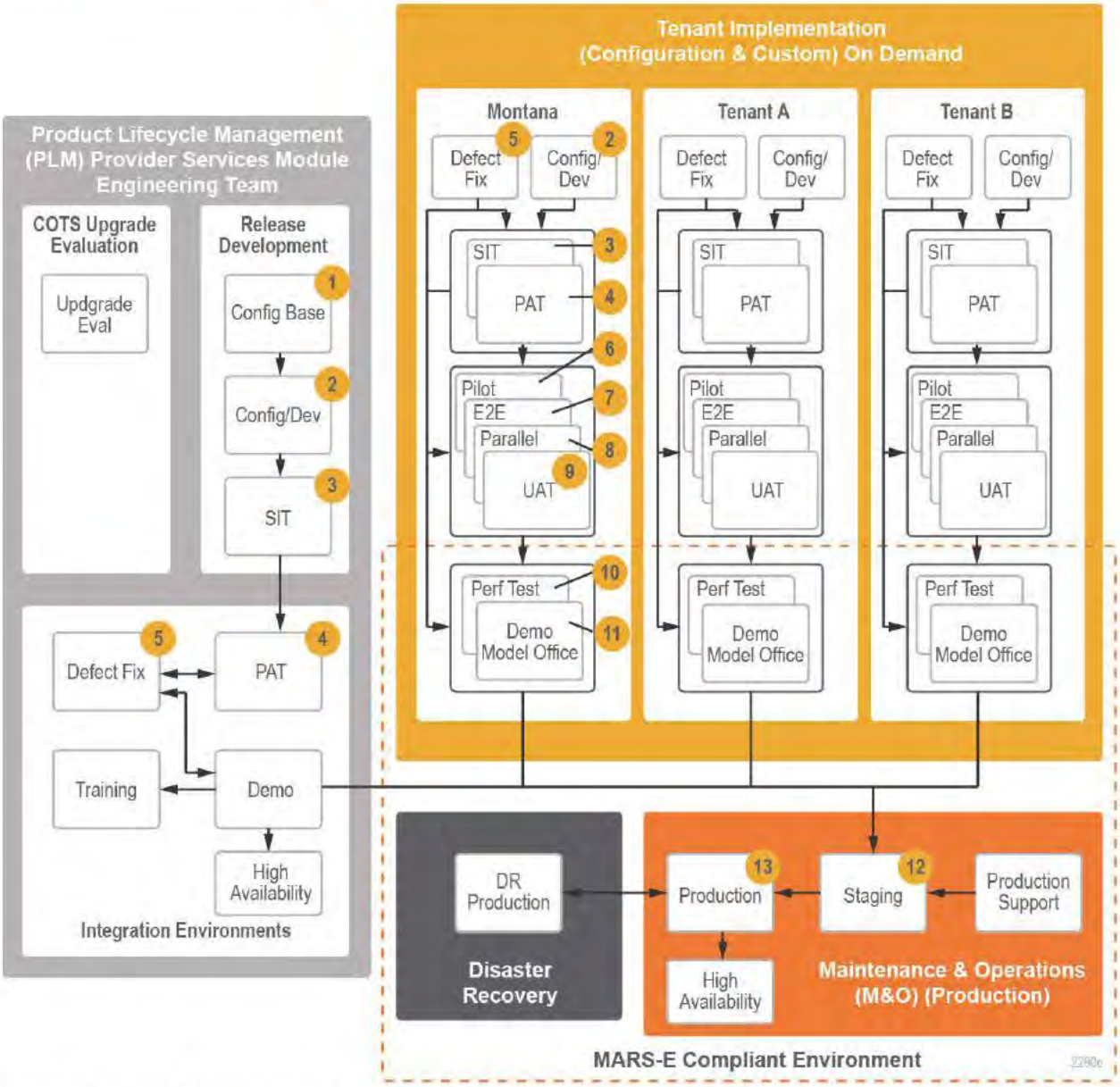


Figure 3.54: Provider Services module Environment.
Optum provides a dynamic set of environments to promote and test changes in a controlled and risk mitigating manner, providing the DPHHS Provider Services module program assurance that releases will be non-disruptive.

Before deploying a release to a DPHHS-specific production environment, Optum will manage and test each release's code through the DPHHS-specific configuration, PAT, UAT, Model Office, and staging environments. The initial configuration environments will load with the Provider Services module base product code, followed by configuring and testing the base code to meet your specific requirements. We will also execute interfaces and data conversion loading and testing. To verify that the release meets acceptance criteria and client objectives, while adhering to established business rules, we will use PAT and UAT environments.

In addition, the DPHHS and Optum will complete, accept, and sign-off regression testing before authorizing the release for deployment into the DPHHS production environment. In most

environments, we will use converted, but de-identified, data in test cases. In lower environments, we may create data to execute unit and limited integration tests.

With reference to the Provider Services environments that Figure 3.54 depicts, the following is a step-by-step overview of activities that we will execute during the initial implementation of our solution.

1. Optum will retrieve a configuration neutral copy of the most up-to-date baseline Optum Provider Services solution and clone it to the DPHHS-specific release development environment.
2. We will then configure the baseline solution to meet your requirements. Post initial configuration, Optum will use this environment to perform additional configurations, execute unit testing, and verify that configurations meet your business rules and objectives. If custom development is required, we will perform that activity in this environment through extensions.
3. Optum will move the DPHHS-specific codebase to a SIT environment. In this environment, we will execute the code integration testing. Clustered together with the PAT instance, SIT verifies integration across multiple Provider Services module components and applications to support the requirement specifications.
4. This phase also includes building a regression suite, reusing existing test cases to verify previously released code continues to work as expected with each code release. Integration test scenarios, developed by our engineering team and QA resources, are leveraged to create the regression suite. To support a multi-tenant environment, the regression suite will include tests from the Provider Services module base product and other tenants, to verify that all tenant environments continue to work as expected without unexpected interruptions from the Provider Services module configurations.
5. Post successful integration testing, the integrated code will promote to a PAT environment. Executed by the Optum business team, business process scenarios verify the user story acceptance criteria and overall business process needs have been met.
6. Subsequent to fixing of identified defects, the DPHHS Provider Services module-specific code is then loaded to the Demo/Model Office environment. This loading allows the Model Office activities to continue with the latest available code, while allowing additional testing to occur in parallel.
7. Optum will resolve defects identified during testing endeavors in a defect fix environment. Following the end-to-end defect management lifecycle process, the bug fixes will continuously integrate with the most up-to-date the DPHHS Provider Services module code. In most cases, we will continuously test the product code until identified defects have been resolved, re-tested, and closed. All critical errors must be in closed-status before moving to next steps.
8. Garnering an approval from the Optum business group, the DPHHS Provider Services module product code will then promote to pilot testing. As part of pilot testing, Optum will conduct trading partner testing to verify that the trading partners and the solution can transmit and receive files. We will also verify that software and integrations previously developed and tested still perform correctly after introduction of new builds/releases, whether it includes defect fixes, configuration, interfaces, or product code merge. In coordination with the DPHHS and other MPATH vendors, Optum will selectively identify providers and provider groups with which to perform limited scenario pilot testing.

9. We will execute E2E testing to verify that system dependencies and data integrity are maintained across the entire solution. The Testing Lead will verify that the system is integrated with all external or third-party systems as defined as part of the DPHHS Provider Services module configuration requirements. This includes functional and non-functional requirements. QA executes scenarios, both positive and negative, that test the flow of the system from beginning to the end. Converted (de-identified) and interface data is used for full workflow execution of all cycles (e.g., daily, weekly, or monthly).
10. As required by project needs, following successful E2E testing, Optum will conduct parallel testing to verify the solution is operating like the legacy system, with explainable variances due to updates in business rules or other departmental objectives. Data run through the legacy system will load and process through the tenant-configured system to verify and compare results.
11. We will perform UAT with input and participation by identified the DPHHS personnel. The goal of this phase will be to verify that the overall business process needs have been met, and the solution is ready for use. Developed by the Optum business group, the business process scenarios used at this stage will focus on the system supporting business processes sought by the DPHHS.
12. After successful UAT, the DPHHS Provider Services module code will migrate to a MARS-E compliant environment. Optum will execute performance testing to confirm application performance (benchmark, load, stress, capacity, stability, scalability, elasticity, speed) and verify the solution and all integrations meet all defined performance requirements in a production-like environment.
13. During Model Office sessions, we will use your business and operations requirements to demonstrate the Provider Services module system behavior to the DPHHS. Feedback collected as part of these sessions will help us close any gaps in code configuration.
14. Post successful Model Office sessions and performance tests, we will migrate the DPHHS Provider Services module code to our staging environment. This environment will enable further execution of additional testing, security assessments, Operational Readiness Testing (ORT), and final Regression Testing. Optum will verify that the system can support the DPHHS' day-to-day Medicaid business operations and that it is ready for operational usage.
15. Actual application users will handle the required tasks in real-world scenarios according to operations processes and procedures. The operations team will develop operational process scenarios, with the DPHHS' input as required. Optum will hold a go/no-go meeting to gather approval for code promotion to the DPHHS production environment.
16. After successful completion of ORT, we will submit to the DPHHS a letter indicating the proposed solution is ready for implementation.
17. Upon receipt of the State's approval, implementation of the solution can commence according to the agreed upon Implementation Plan.
18. Optum will provide confirmation after deployment/implementation into the production environment and the completion of three calendar days of operations without significant operational issues (no critical or high defects).
19. Full acceptance of the solution occurs when Optum receives approval for go-live from the DPHHS. In concert with the release schedule signed-off by the DPHHS and/or other

pre-determined stakeholders, code will be pushed to the production environment. Optum will communicate the deployment broadcast across identified stakeholders' channels.

As part of the release management process, Optum will version each tenant specific codebase using this release numbering structure:

[MajorReleaseYearYY].[MajorReleaseMonthMM].[BreakfixRelease]

Example(s):

Release criteria	Release number assigned
Major release during May 2018	18.5.0
Minor release (break fix) that follows (same month)	18.5.1
Major release during June 2018	18.6.0

In addition, each Provider Services module COTS component will carry its own version or release numbers as provided by the components' manufacturers.

Release Schedule

As discussed previously in the sub-section, Optum will coordinate with the DPHHS and other stakeholders to document a release schedule that identifies all end-to-end release activities. This deliverable will capture a release management process that is congruent with the DPHHS' multi-vendor approach. Our release schedule will document the detailed activities that we will execute as we manage code promotion into your production environment.

The DPHHS Provider Services module implementation will follow a staggered/phased approach implementation that benefits the DPHHS by:

- Minimizing the project risk by being able to halt or back out the implementation processes, if necessary
- The flexibility to review and make modifications/improvements based on lessons learned from previous releases
- Deeper stakeholder engagement

Adhering to our Agile framework, we will enhance the components of the Provider Services module iteratively, even as the DPHHS initial implementation executes. Optum will use the most up-to-date baseline Provider Services module source code to configure DPHHS requirements. Whether a release is introduced because of changes in local, state, or federal mandates, updates to client business rules, or any other market demand, the baseline Provider Services module product code is updated and integrated as needed. During implementation, the DPHHS-specific code will integrate daily in various configuration/development environments. As a result, the product will always carry the most current product capabilities as part of the Provider Services module implementation.

Conforming to the modular and interoperable requirements set forth by CMS, the comprehensive Provider Services module product is delivered using various COTS products that are bundled together to meet each respective client's business objectives. Because of this bundling, each respective COTS application Optum will use to deliver the Optum Provider Services solution will be updated with the respective manufacturer's release schedule. To verify compatibility and to avoid breaks in production processes, COTS applications will only be upgraded after they have been regression tested for backwards compatibility.

The current Provider Services module release strategy is as follows:

- Product Releases
  - Frequency: Quarterly (January, April, July, and October) for major releases and as needed for break fixes
  - Automated regression for all product releases (major or break fix)
  - Major releases
    - Contain the latest upgrades to the COTS components
    - Contain common product enhancements as defined in the product roadmap
    - Contain changes driven by CMS regulations, security, and compliance that apply to all states
    - Follow Agile development lifecycle
    - Pushed to tenant implementation Config/Dev environment
  - Break fix
    - Might be specific to one or multiple tenants
- COTS Upgrade Strategy
  - Frequency: Two COTS upgrades every year (April and October).
  - Upgrades will be evaluated and tested in an upgrade evaluation environment.
  - After the upgrade is tested in the upgrade evaluation environment, it will push to the PLM configuration, custom development, and SIT environments for the next release.
  - The subsequent release will start the development in the upgraded PLM configuration, custom development, and SIT environments.
  - After deploying the upgrade into production, the newly upgraded version will push to the tenant implementation environment the next working day.

Release Risk and Issue Mitigation

Implementing the Provider Services module using an iterative, broadly applicable method will help the DPHHS, stakeholders, and Optum identify and mitigate all identified release risks. For each release, Optum will plan, organize, staff, and lead IRAAD sessions. We can then identify, capture, and plan for as early in the project as possible.

This strategy helps address the most critical risks as early as possible in the release implementation lifecycle. This results in a measurable reduction in scope and schedule risks that relate directly to a reduction in budget risks.

Through collaboration, all stakeholders can better identify risks proactively. We accomplish this by performing combined analysis on risks to determine the best response. When required, Optum, along with other stakeholders, will engage in performing a cost versus benefit analysis on any risk to determine the best mitigation policy.

To verify all risks are understood, with responses agreed upon by all applicable stakeholders, Optum will exercise PMI's proven risk mitigation methodology. Before accepting a respective risk's mitigation or other response strategy, each risk response must be:

- **Bought into:** The DPHHS, other affected vendors/stakeholders, and Optum must all agree with the response strategy selected for each respective risk.
- **Approved:** All identified stakeholders must approve each respective risk's response.
- **Realistic:** Mitigation/other response strategy selected for the respective risk must be realistic and achievable.
- **Formal:** Each risk response must be documented, approved, and broadcasted to applicable project stakeholders.

Our extensive experience in implementing products and services helps us build upon our existing knowledge base while leveraging proven strategies, templates, and other tools. With thorough planning, communication, risk management, and prudent execution, our implementation/release strategies provide the DPHHS Provider Services module implementation with the agility and velocity necessary to deliver project scope while also being on time and within budget.

After go-live/implementation, the OSAM processes will continue to support release stabilization and certification achievement.

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.

As detailed in the release management sub-section above, Optum will meet the proposed process for deploying each proposed solution(s) to production by:

- After successful completion of ORT, we will provide you a letter indicating the proposed solution is ready for implementation.
- Upon receipt of the State's approval, implementation of the solution can commence according to the agreed upon Implementation Plan.
- Optum will provide confirmation after deployment/implementation into the production environment and the completion of three calendar days of operations without significant operational issues (no critical or high defects).
- Full acceptance of the solution occurs when we receive approval for go-live from the DPHHS. In concert with the release schedule signed-off by the DPHHS and/or other pre-determined stakeholders, code will be pushed to the production environment. Optum will communicate the deployment broadcast across identified stakeholders' channels.

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.

We will monitor our solution upon implementation using multiple monitoring processes and compiling objective statistical data reflecting system performance. This monitoring is vital and will provide:

- Notification to Optum Maintenance and Operations directly when issues arise

- The ability to start restoration efforts quickly by not having to wait for users to report issues
- Alert to issues before users are affected, providing proactive service restoration
- The increase of the service's availability and decrease of the Mean Time to Restore (MTTR)

Optum will monitor, measure, and optimize system and application performance to verify consistent and superior response time, enhanced stability, and required scalability. Our recommended monitoring tools will capture the availability status of each monitored environment. Monitored environments identify, record, report, and analyze equipment or system alarms and conditions that can lead to abnormal operations.

Available operational dashboards will provide the DPHHS insight into the performance and operation of our solution. These dashboards will enable tracking and compliance with the KPIs required in the operation of the Provider Services module.

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.

We will execute multiple test cycles and phases for the Optum Provider Services solution to demonstrate the system infrastructure is operational and meets federal and State architectural, technical, security, and privacy requirements, as well as the business and functional requirements. During testing, we will work with the DPHHS to make sure we capture and meet the business and functional requirements. We will rely on the comprehensive knowledge and experience of our combined teams to validate the other aspects of implementation function as expected and described in this response. Our Model Office and testing results will demonstrate the functionality of the solution.

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.

The methodologies Optum employs enables the constant monitoring of the Optum Provider Services solution. To validate solution performance, we will meet or exceed all of the State's defined SLAs.

Optum Enterprise Performance Testing confirms that Optum meets performance, availability, and stability objectives for systems and applications. We conduct performance testing for new applications, application, or infrastructure changes, troubleshooting, and hardware and software comparison and evaluation. Our automated tools simulate high user volumes within a dedicated load of data. Support for application protocols includes HTTP/HTML, Web services, mobile, database/ODBC, Citrix, RTE, and video streaming. Optum maintains a dedicated Internet connection with 400 MB/1GB burst for testing Internet applications. Our performance management tools are fully integrated to facilitate comprehensive reporting and analysis.

We support multiple test types, including load, stress, stability, and resiliency testing. Load testing measures how the application will behave under peak user volumes. Stress testing pushes the application to above-expected user volume and helps us identify a break point. Resiliency testing determines application behavior in failover conditions. Stability tests run for extended durations to identify underlying issues, such as memory leaks that may not be noticeable until the application has been under load for several hours.

As Optum prepares for Enterprise Performance Testing, Optum will work with the DPHHS to define goals, script requirements, and scenarios. We will develop test scripts based on

documented workflows that are critical to your business or are most frequently used by your users. Performance test engineers execute tests based on test scenarios that Optum designs with the DPHHS' SMEs. We will provide reports after each test to help you conduct in-depth analysis and compare tests. Performance test benefits include the following:

- Evaluation of system performance against required KPIs and SLAs
- Reduced infrastructure costs by sizing components correctly
- Increased application stability by:
  - Baselining infrastructure and application performance before releases, upgrades, or changes
  - Determining if applications and infrastructure will support the expected level of users and transaction volumes
  - Testing application performance to plan for unexpected increases in usage volume
  - Identifying failover issues and application resiliency under load
- Improved user experience by confirming that the user experience remains unchanged and stable under stressful conditions, such as failures with architecture or dependent services
- Identifying bottlenecks, performance issues, and opportunities for tuning

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.

Our process will offer a continual feedback loop as we develop and implement the solution. Through incremental releases, users can provide feedback to the development and configuration teams and work collaboratively to validate we meet requirements before implementation. This approach will provide a smooth transition from development to deployment into a production environment.

In addition to the ORT, we will validate the functionality and usability of the Provider Services module using Model Office working sessions throughout the release phase by the DPHHS.

Prior to the formal sign-off of the Operational Readiness Checklist, we will conduct a walkthrough of the solution and the DPHHS and Optum-related operations to the Provider Services module. This will confirm that the solution is fully deployed and ready for the DPHHS to use.

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.

Optum uses a comprehensive suite of tools that will help the implementation of the Optum Provider Services solution. We exercise continuous release monitoring and control practices, enabled through the tools available to our development and configuration teams. Optum tracks and prioritizes all potential solution modifications (e.g., enhancements and defect fixes) to make appropriate release recommendations to the DPHHS.

Operational Readiness Verification

We developed a comprehensive checklist of activities to promote low-risk deployments and comprehensive Operational Readiness reviews. The checklists promote a controlled and repeatable release process. The following table describes the checklist in more detail.

Deployment Checklist	Description
Operational Readiness Verification	Hardware, software requirements, and design documentation, pre-production testing (including unit, integration, UAT, and Initial Operating Capability IOC), and validation, conducting necessary load and stress tests, and SLA compliance
Configuration Management	Rules configurations, code, database scripts, and other artifacts checked in/tagged for release, including executable and documentation artifacts - requirement specifications, user stories, architecture documents, object models, and scenario diagrams
User Guide and Training	Issue online guides and conduct online/classroom training to help clinician and technical staff use and operate the system; all necessary training completed prior to rollout
Customer Communication Plans and Change/Release approvals	Governs stakeholder communications, including Executive Management, Development and Operations Teams, end users, and change/release management committees with necessary approvals in place prior to release/deployment
Help Desk Communication and Training occur	Conduct training for Help Desk staff regarding the Provider Services module and issue help aids and scripts describing how to fix and escalate issues when they occur
Rollback Plans	Issue detailed plan for rolling back releases, if the rollout does not go as planned
Disaster Recovery and Business Resumption Plans	Detailed disaster recovery plan developed, tested, communicated, and accepted, including restoring access controls, databases, and other services
Post-deployment Validation/Approval for Operational Start	Conduct validation of system to verify deployment is complete and ready for operational use