HUMAN SERVICES DEPARTMENT

# Medicaid Management Information System Replacement (MMISR) Project

# SIPLT88 - Interface Management Plan

**NM HSD Deliverable Owner: John Oliver**

**Contractor Deliverable Owner: Dawn Gelle**

**Configuration Number v1.7**

**October 8, 2019**

TurningPoint

TurningPoint Global Solutions
Software Services Company™

Section 508 Compliant

# Table of Contents

# List of Tables



# List of Figures

# 1 Introduction

The definition of an interface is “an exchange of data, in a specified format, between two entities.” An entity could be (1) another government agency, (2) two systems within the same agency, or (3) an external business partner (for example, a provider). For the purposes of the Health and Human Services (HHS) 2020 initiative, an interface has a more narrow definition: “An exchange of data between the HHS 2020 enterprise and an external entity.”

This Interface Management Plan describes the approach to developing interfaces for legacy modules, Medicaid Management Information System Replacement (MMISR) contractors, and other State agencies, including – but not limited to – Income Support Division (ISD), Medical Assistance Division (MAD), Department of Health (DOH), data trading partners, and service providers that are external to the HHS 2020 enterprise. As well, some inter-system interfaces within the New Mexico (NM) Human Services Department (HSD) will become enterprise orchestrations, and therefore will not be managed as interfaces in the future. The System Integrator (SI) will develop interfaces in support of MMISR on an ongoing basis throughout the life of the project and integrate them into the HHS 2020 architecture. The SI team will execute interface management as follows:

- The SI team will collaborate with NM HSD to create an inventory of current interfaces.
- The SI team will collaborate with trading partners to define interface integration requirements including Interface Control Documents (ICDs), Service Level Agreements (SLAs), and responsibilities for error management.
- The SI team will develop plans with interface partners to migrate the interfaces from the legacy modules to the new HHS2020 architecture and conduct end-to-end testing as a part of a Work Package.

NM HSD currently maintains numerous interfaces with internal and external interface partners which represent siloed pipelines requiring a high degree of maintenance and customization. The SI team will provide oversight for, and design/develop interfaces for legacy modules, new MMISR vendors, and external data partners, to assist in replacing these legacy interfaces with a standards-based approach that enables interfaces and data extracts. This will be done through the Integration Platform (IP).

The approach to inventorying existing interfaces starts with the Interface Workgroup (IWG). The IWG will create an interface repository which will be the single source of all interfaces categorized by the source systems. This repository will be based on the information gathered from the sources, including – but not limited to – Omnicaid system documentation, CSES system documentation, DOH system(s) documentation, the NM HSD procurement library, Automated System Program and Eligibility Network (ASPEN) documentation, other external partners, and the Data Governance Council (DGC) library.

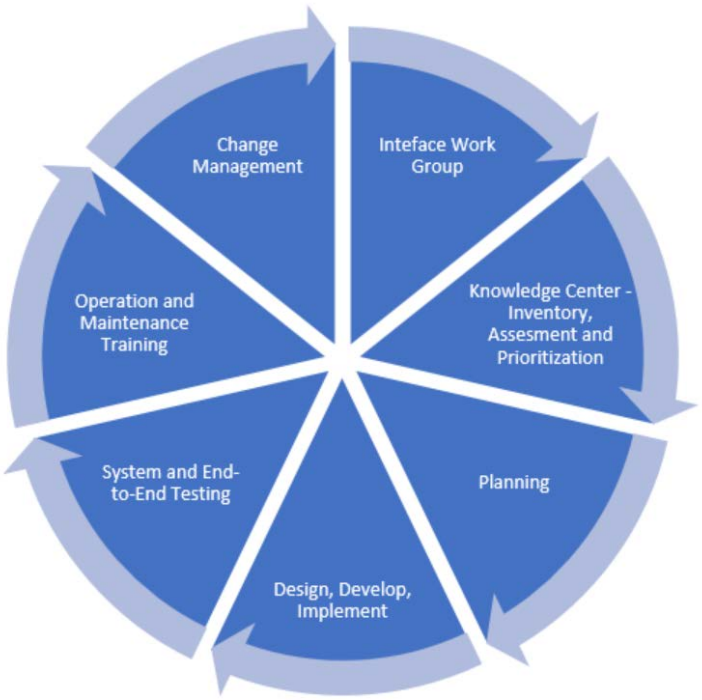
The SI Contractor and the IWG will perform a thorough assessment of the interfaces based on the information obtained in workflow Joint Application Requirements (JAR) sessions, IWG meetings, and additional documentation provided by the Subject Matter Experts (SMEs) participating in the IWG sessions. The outcome of the assessment will be captured, maintained, and reviewed by the members of the IWG, which maintains the interface inventory and is the “source of truth” in regards to interfaces for the HHS2020 MMISR project.

The assessment process will help the SI Contractor to propose the technical To-Be workflows based on the SI platform tools and methodologies. The SI Contractor will consider the Medicaid Information Technology Architecture (MITA) guidelines, such as reusability and loose coupling, among others. This process will help establish the end-to-end technical To-Be workflows.

The identified technical To-Be workflows are broken down into Integration Projects as trackable units of work. The process by which Integration Projects are conceived, created, and executed is detailed in Section 2.2 SDLC Execution for Interfaces. Each Integration Project is added to the Integration Project Backlog and executed in a combination of iterative and classic waterfall methods.

The implementation phase of the To-Be workflows includes coordination with appropriate stakeholders for effective integration testing of the workflows, and plan-associated logistics such as timing, environment, etc. Following integration and acceptance testing of the interfaces, the platform, workflows, adaptors, and processors will be ready to be rolled out to the higher environment. The following figure illustrates the Interface Management Lifecycle:

**Figure 1: Interface Management Lifecycle**



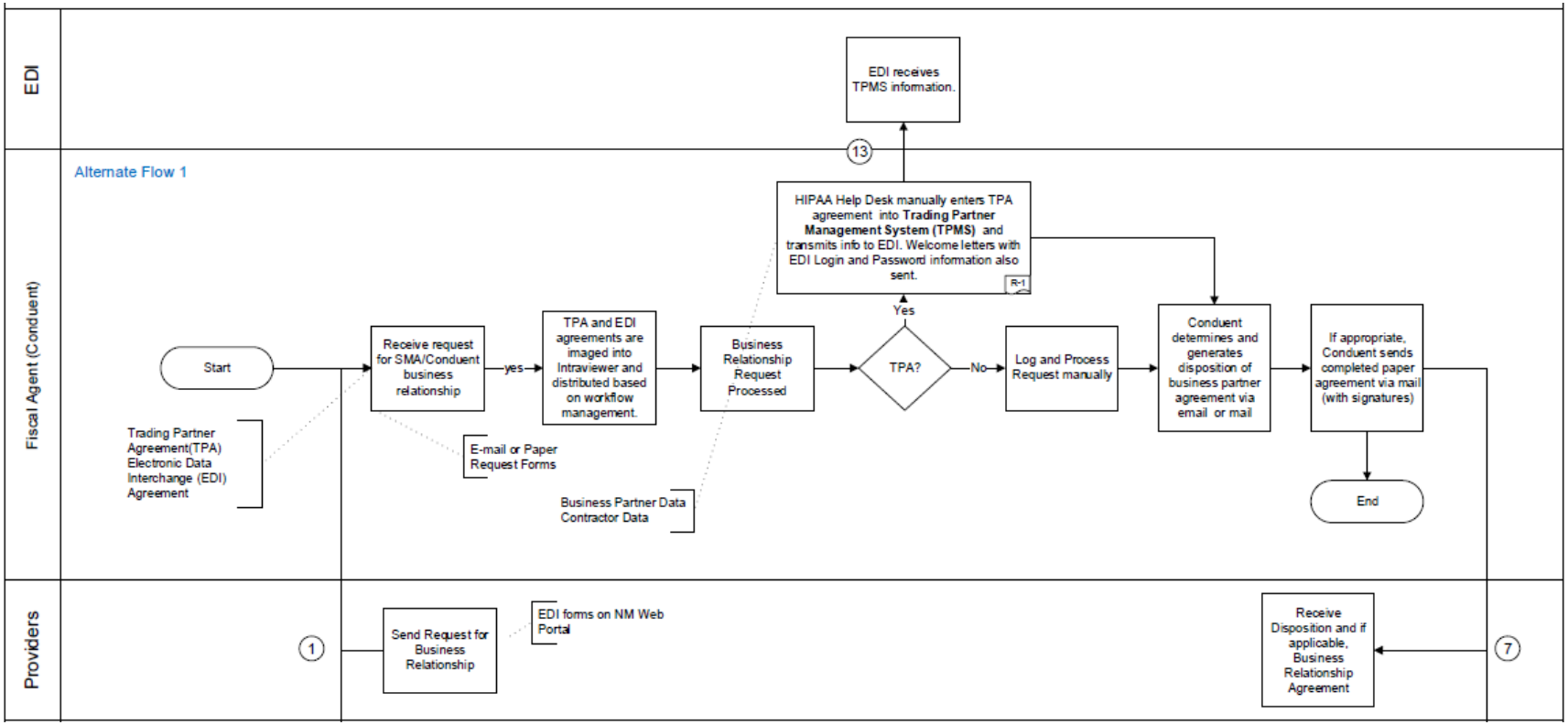
## 1.1 Interface Repository – Discovery and Inventory of Interfaces

The SI team, with NM HSD assistance, will perform a discovery process using NM HSD provided documentation. This discovery process will also help identify interfaces that have not yet been identified or documented. This process is tightly integrated and derives from enterprise workflow JAR/Joint Application Design (JAD) sessions. The SI team will also work with legacy system contractors to ensure that documentation provided is current. In the documentation, interfaces will be bucketed into categories; for example, interfaces required for a particular business process, such as Provider Management, will be identified, classified as incoming or outgoing, and categorized by method of transmission.

The outcome of this discovery and inventory process will be documented in a dedicated knowledge center established on SharePoint and will remain the single source of information for all external interfaces that are part of the HHS 2020 enterprise. The knowledge center will contain all the available information from the sources, including – but not limited to – the NM HSD procurement library and ASPEN documentation. The interfaces will be documented in the form of an Interface Control Document (ICD) Lite, an abridged version of a full Interface Control Document. This supports the format of the repository. A completed, unabridged, ICD occurs at the time of integration on the platform with a trading partner or external entity when additional details become available.

The As-Is JAD sessions captured MITA business process workflows which included key interface touchpoints. For example, the following figure shows a part of an As-Is workflow of the MITA business process area and business relationship management. This diagram has numbered labels at each of the interfacing systems' entry/exit point. Here, the number 1 is used to denote the interfaces between the providers and the NM HSD, and the Fiscal Agent for New Mexico Medicaid, Conduit. This diagram was created based on the knowledge obtained from the document sources listed earlier.

Figure 2: Establishing Business Relationship MITA Business Workflow



The SI Business Analyst (BA) team, along with HSD BA team, will perform this discovery process and create an initial catalog of interfaces for each of the labeled entry/exit points in the given MITA business workflows. The following figure shows a subset of interfaces identified for the given interaction among providers, NM HSD, and the Fiscal Agent for NM Medicaid. The column "Visio ID" helps to correlate the entry/exit point in the given workflow with the type of interface. For example, the entry point 1 in the diagram is broken down into several interfaces – namely 1.1, 1.2, and 1.3 – based on the nature of the interface, such as email, phone, and online modes of communication.

Figure 3: Interfaces Breakdown Based on the Visio Workflow

| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Description | Visio ID | File/ File Description | File Format (standards e.g ANSI X12, proprietary, paper form) | Frequency | Batch/Real Time/Manual | Electronic Formats (if applicable) | Data Source | Data Receiver |
| 2 | Provider initiates request to establish business relationship via email | 1.1 | Provider Business Relationship Request | email | | Manual | | Provider | State Medicaid Agency/Conduent |
| 3 | Provider initiates request to establish business relationship via paper | 1.2 | Provider Business Relationship Request | Paper | | Manual | | Provider | State Medicaid Agency/Conduent |
| 4 | Provider initiates request to establish business relationship via online (NM Portal - https://nmmedicaid.portal.conduent.com/webportal/enrollOnline) | 1.3 | Provider Business Relationship Request | EDI | | Real time | | Provider | State Medicaid Agency/Conduent |

## 1.2 Technical and business-related information is listed in Table 3: ICD Lite Template and validated with the IWG members.Interface Work Group

The IWG is tasked with defining, tracking, and ensuring all interfaces for the HHS 2020 program are successfully migrated from the current business silos into a coordinated, centralized structure supported by the SI. The IWG has several objectives that are listed below:

- Facilitate access to documentation from the Procurement Library and SharePoint, as well as any additional documentation.
- Facilitate access to SMEs from different departments that are the source of information for the respective departments.
- Assess, transform, and de-duplicate the interface list in preparation for the To-Be design. This activity is done in collaboration with the SI Contractor and NM HSD. The participating members of the IWG are from departments representing systems or business entities including – but not limited to – MAD, ISD, DOH, Behavioral Health Services Division (BHSD), Child Support Enforcement Division (CSED), Children, Youth, and Families Department (CYFD), Aging and Long-Term Services Department (ALTSD), and the Department of Workforce Solutions (DWS). These members are familiar with the desired HHS 2020 architecture and its objectives.

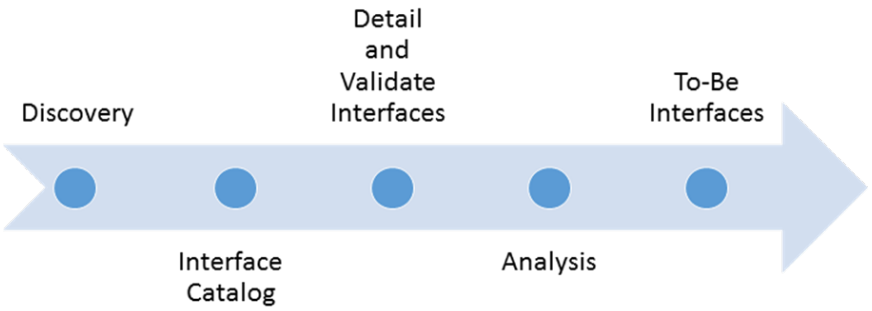
The following figure outlines the IWG activities, from deriving the materials developed during the workflow JARs/JADs, through interface cataloging, and finally to the well-documented and prioritized backlog of To-Be workflows. The following benefits are achieved from the activities performed by the IWG:

- Active interfaces are made available to all HHS 2020 modules, with proper role and privilege levels
- Interface controls are centralized
- Inactive and duplicate interfaces are removed
- A list of interfaces to automate and modernize the HHS 2020 enterprise is created

The success criteria of the IWG is defined and measured by the following criteria:

- To-Be MITA business interfaces compliant with the Centers for Medicaid and Medicare Services' (CMS) Seven Standards and Conditions, built on the SI platform's Enterprise Service Bus (ESB), spanning service orchestration, interfaces, legacy and new module integration, and Enterprise Shared Services (ESS)

Figure 4: IWG Vision


Discovery
Interface Catalog
Detail and Validate Interfaces
Analysis
To-Be Interfaces

## 1.3 Goals of Interface Management

The following sections outline the goals of interface management.

### 1.3.1 Implement Modular System Architecture

CMS' MITA framework establishes the Modularity Standard to ensure that Medicaid technology investments provide the flexibility and extensibility necessary to support today's program needs, while ensuring eligibility for Federal Financial Participation (FFP) funding. This condition requires the use of a modular, flexible approach to systems development, including the use of open interfaces and exposed Application Programming Interface (API), the separation of business rules from core programming, and the availability of business rules in both human and machine-readable formats.

The technical To-Be interfaces will be designed according to the MITA framework – which outlines a modular approach, significant reuse, and web service interoperability amongst MMISR modules.

### 1.3.2 Standards-Based Service Oriented Architecture and Governance Framework

The SI will deploy a Service Oriented Architecture (SOA) framework for HHS 2020 that supports a standards-based, loosely coupled, modular architecture for the MMISR initiative, which will also be used as the foundation for the HHS 2020 program. At the core of the SI solution is the IP, which enables vendor-neutral system-to-system interaction through a flexible, scalable solution.

The SI Contractor will collaborate with NM HSD to develop standards and governance processes for the Project Management Office (PMO), business, technology, and data areas of the program. The SI Contractor and NM HSD will disseminate enterprise standards and governance processes to all HHS 2020 module partners for successful integration into the SOA framework. This will be done through requirements and design reviews for new modules, education, and training about standards and enterprise services, and APIs for service consumption and provisioning to align with HHS 2020 standards. The governance process includes ongoing monitoring to ensure conformance with enterprise standards.

### 1.3.3 Business Process and Organizational Structure Re-Engineering

The HHS 2020 SI project is a business transformation initiative. Together with the deployment of the integration technology that enables the modular MMISR, the SI Contractor, NM HSD, and business owners from MAD, ISD, and CSED, and others will assist in re-designing business processes that leverage the SOA framework. Their strategic goals will include reusing services, while also de-duplicating and automating processes. The SI Contractor will take direction from the PMO and business owners to plan and implement interface business processes.

## 1.4 Interface Management Plan Maintenance and Update

The Interface Management Plan will be updated as design patterns and strategies evolve based on the needs of the integrating systems and technology upgrades.

### 1.4.1 Monthly Reporting

The Interface Management Report provides the monthly status of interface management activities. It will contain the following information:

- **Interface Table** – This is a table containing a list of all interfaces, with a link to the respective ICD.
- **Interface Status** – The above table will also have a column providing the prioritization status for a given interface. The statuses applicable are as follows:
  - Not yet prioritized
  - Prioritized but not yet started
  - Started
  - Completed
  - No longer needed in the new architecture
- **Interfaces Stage** – The above table would also have a column providing the stage of the lifecycle for a given interface. The stages applicable are as follows:
  - Requirements
  - Design
  - Development
  - Test
  - Rollout and Maintenance
- Activities and milestones for the previous and current months across interface work streams.
- Risks and issues across the interfaces work stream.

### 1.4.2 Relationship with Other Project Plans

The table below describes how the Interface Management Plan relates to other plan deliverables. The "Impact on Interfaces Management Plan" column highlights the relationship of the other plan to Interfaces work.

Table 1: Interface Management Plan – Related Deliverables

| Deliverable ID | Deliverable Name | Impact on Interfaces Management Plan |
|---|---|---|
| PMO1 | Project Management Plan (PMP) | As the over-arching project management guideline, this document provides a structured framework to enable the MMISR State-led PMO, SI Contractor and the module contractors to work in a coordinated manner to execute, monitor, and control the MMISR project and to achieve the project's critical success factors. |

| Deliverable ID | Deliverable Name | Impact on Interfaces Management Plan |
|---|---|---|
| PMO3 | Communications Management Plan | The Interfaces Team will adhere to the guidelines outlined in this plan in regards to communicating with external trading partners and agencies. |
| PMO4 | Communication Matrix | The Communication Matrix may need to be updated as each interface is worked to include any new audiences and the proposed delivery method. |
| PMO5 | Project Scheduling | The Interfaces Team will provide updates to the Integrated Master Schedule as each Integration Project is defined. |
| PMO9 | Service Orchestration Plan | Grouping interface-related services together into an executable module is defined in this plan. |
| PMO11 | Configuration Management Plan | The Interfaces Team will be a key user of the Configuration Management Plan and will abide by its guidelines. |
| PMO13 | Quality Management Plan (QMP) | The Interfaces Team will be a key user of the Quality Management Plan and will abide by its guidelines. |
| PMO14 | Test Management Plan (TMP) | The Interfaces Team will review the TMP to ensure the approach contains sufficient definition to handle testing interfaces. The interfaces team will use the testing methodologies prescribed in the TMP to promote interfaces through the review gates. The interfaces team will update the TMP with additional detail, if need be, at a later time to describe a plan for testing with trading partner, system or agency. |
| PMO15 | Requirements Management Plan | The Interfaces Workgroup will use the Requirements Management Plan as a guide for gathering requirements. Documenting the requirements will be stored in ICD documents and eventually in Jama and Jira. |
| PMO16 | Requirements Traceability Matrix (RTM) | Interface requirements will be added to Jama and Jira, and mapped appropriately to ensure traceability through the lifecycle process (requirements, design, development, and testing). |
| PMO37 | Configuration and Continuous Integration Services (CCIS) Plan | This plan provides guidance and direction for how module contractors and SI work together on delivering a fully integrated product. |

| Deliverable ID | Deliverable Name | Impact on Interfaces Management Plan |
|---|---|---|
| SECURITY1<br>SECURITY2 | Security Approach<br>System Security Plan | The Interfaces Team will be a key user of the Security plans and will abide by their guidelines. |
| SIPLT3 | Capacity Plan | All defined interfaces, including the quantity and frequency of the data exchanged, will be included in the plan to ensure that sufficient capacity exists in the infrastructure. |

# 2 Interfaces Work Stream Project Approach

HSD, vendors and the SI collaborate to support business process re-engineering across the HHS 2020 project, including interfaces. HSD business and technical leadership provide input, prioritization and decision-making to determine if an interface business process needs to change.

In a collaboration with the HHS 2020 team, the SI Contractor will lead the effort to decompose each interface into a technical To-Be solution with a breakdown of the technical services required to be developed to support the business workflow. The solution will be encapsulated and tracked within an Integration Project. Each Integration Project will be broken down into individual Work Packages that can be assigned to HHS 2020 vendors. These Work Packages are subsequently broken down into Work Items, which delineate the Software Development Life Cycle (SDLC) tasks involved in completing the Work Package.

As part of the execution, the following toolsets and libraries are utilized wherever applicable.

- Jama will be used to manage requirements
- X-Ray will manage test plans.
- Jira will be used for interfaces change management, backlog maintenance, and prioritization.
- Business Activity Monitoring (BAM) is the Oracle tool used for business related monitoring.
- Enterprise Manager Cloud Control (EMCC) is the Oracle tool for service-level monitoring and metrics.
- Memorandum of Understanding (MoU) will document partner business agreements.
- ICD documents provide technical specifications of each interface.

## 2.1 Planning

The SI Contractor will collaborate with NM HSD leadership to schedule each interface based on a jointly developed prioritization criteria. The planning will derive from the following sections of the CCIS Plan and tailored for the Interface management activities.

### 2.1.1 Adding to the Integration Project Backlog

Requests for new or modified interfaces will be added to the Integration Project Backlog. In defining the interface request, the team will first take into consideration To-Be requirements to identify the workflows affected.

The SI Contractor and NM HSD will discuss each workflow and the below set of prioritization factors to add interface-related Integration Projects to the Integration backlog once the To-Be business processes are identified. These factors will include:

1. **Module on boarding timeframe/schedule**: On boarding reflects the readiness of the module.
2. **Infrastructure readiness**: Validate the availability and readiness of the infrastructure to implement the interface. The main emphasis here is the integration testing environment where all of the systems participating in workflow execution can interact seamlessly for software testing.
3. **Interaction with stakeholders**: It is important to gather stakeholder feedback on the prioritization criteria for implementation.
4. **Prioritization**: This is based on MITA business process areas.
5. **Number of dependencies**: A workflow with fewer dependencies will be easier and faster to implement versus a workflow that has several dependencies.
6. **Implementation time**: The faster it is to implement a feature, the higher it could be on the priority list.

The SI Contractor's Implementation Manager coordinates stakeholder engagement in backlog grooming as well as their participation in related planning and requirements activities. The prioritized requirements follow an SDLC process for end-to-end implementation.

### 2.1.2 Integrated Work Breakdown Structure

Each interface project's Work Breakdown Structure (WBS) will be developed and managed in JIRA and tracked through the Kanban boards within the HSD Tools Ecosystem and will be integrated into the SI Project Plan, and incorporated into the Enterprise Project Schedule (EPS) as appropriate. The SI team will develop the WBS for the interfaces in collaboration with external interface partners, their system vendors, and HHS 2020 business owners to ensure coordination of activity among these stakeholders. As part of this process, the SI Contractor will create an inventory of current workflows representing NM HSD business processes that are referred to as As-Is workflows.

The interfaces' WBS involves development of technical To-Be workflows from As-Is workflows in coordination with the contractors responsible for new and legacy modules, ESS, and interfaces. Each technical To-Be workflow is broken down in order to identify the work responsibilities of different participating systems, as well as IP. The workflows can then be converted into logical tasks and assigned to vendors of each participating system. As a part of the WBS task, dependencies are identified as well. The interfaces WBS is fed into the integrated WBS to ensure all the tasks and dependencies are captured properly. As additional modules or related HHS 2020 initiatives are

implemented, the SI Contractor will review the approved HHS 2020 WBS to ensure that all appropriate changes or updates are incorporated.

Reference: Project Scheduling and CCIS Plan.

### 2.1.3 Integrated Master Schedule Management

To ensure enterprise-level visibility across stakeholders and projects and legacy and new module vendors, the SI Contractor will contribute tasks for implementing interfaces to the ePMO's Integrated HHS2020 Schedule by including new module contractors, legacy module contractors, interface trading partners, and other stakeholders that are integrating into MMISR.

An Integration Project will be defined for each Interface, which will then be broken down into individual Work Packages or services necessary for the Interface to be implemented.

As part of the schedule management approach, various tasks and dependencies for orchestration services will be identified in the orchestration services WBS. Other dependencies include availability of infrastructure, availability of integration environment, and services from the integrating partners.

The approach to maintaining the project schedule for interfaces is to track completion of the bundling of interface items identified by WBS within a Work Package. This Work Package is managed in Jira/Confluence and releases are scheduled and managed in the SI Project Plan. The SI Contractor team will work with the owners and vendors of systems and services included in that workflow to assign Jira items to convey the assigned tasks. The task management is tracked through Jira.

The following example will clarify this approach (Interface #1 consists of two tasks):

1. Task #1 is the creation of the service which selects the data to be sent.
2. Task #2 is the creation of the service which performs the actual transmission of the data to the external recipient.
3. Work Package #1 will be created for Task #1 as an SDLC work stream for the Data Services (DS) module contractor.
4. Work Package #2 will be created for Task #2 as an SDLC work stream for the SI Contractor.
5. Work Package #3 will be created by the SI Contractor to perform service orchestration.
6. Completion of Work Package #3 is dependent on completion of Work Package #1 and Work Package #2. It may also be dependent on other SI tasks, notably creation of the ESB and the System Migration Repository (SMR). Note that both Work Package #1 and #2 can be worked independently, but it is not until Work Package #3 is completed that Interface #1 can be considered complete and ready for production. This example defines the process for the initial implementation of an interface.

The CCIS Plan comes into use when an interface needs to change after its initial implementation. In that case, new Work Packages and tasks will be defined for any new processes, data, or data manipulation that is identified. These identified elements are then assigned to the various module contractors for development, testing, and orchestration.

Reference: Project Scheduling, Schedule Management Plan, Orchestration Management Plan, and CCIS Plan.

### 2.1.4 Enterprise Governance

Interfaces implementation will be compliant with business, information, and technical standards published by multiple governing bodies, including the Business Transformation Council (BTC), Data Governance Council (DGC), and Architecture Review Board (ARB).

The technical To-Be workflows will be identified on an ongoing basis throughout the life of the project, as opportunities for automation and re-use are identified through ongoing interface management. The technical To-Be workflows are primarily guided by the MITA business architecture, specifically for MAD interfaces (not for ISD or CSED interfaces). The technical To-Be workflows also incorporate processes that are not part of the MITA business architecture but are required to address the State's business needs.

To implement new business standards for To-Be design of processes and operations, the SI Contractor team will collaborate with the BTC to plan for the adoption of the new standards on an ongoing basis as new business workflows are defined. The SI Contractor's Functional/Business Manager will be the liaison from the SI Contractor to the BTC to bring into focus changes that impact the business. Additionally, they will evaluate changes across business units and plan for appropriate response to those changes.

Reference: PMO 12 – Governance Standards – Technical and Architectural.

### 2.1.5 Interface Implementation Process

HHS 2020 is a complex initiative that requires a well-defined process ensuring coordination among multiple stakeholders to successfully integrate the technologies, systems, data, and services into a unified solution. The SI Contractor will work with HSD to identify all the stakeholders responsible for the interfaces and strategize the communication and engagement mechanisms.

The SI will implement a communication protocol to convey information among HHS 2020 stakeholders and a process for onboarding stakeholders who are participating in integration activity. This will follow and elaborate upon the guidelines outlined in PMO 3 – Communication Plan.

The following table outlines the steps for interface implementation. Stakeholders for each step include HSD PMO, SI PMO, business owners, and all HHS 2020 system vendors.

Table 2: Process Steps for Interface Implementation

| Step | Title | Description |
|---|---|---|
| 1 | Backlog definitions | Identify Integration Projects including: Work Packages, As Is processes, To Be processes, workflows, services, initial prioritization of individual tasks and Work Packages. |

| Step | Title | Description |
|---|---|---|
| 2 | Release planning | Develop Rough Order of Magnitude (ROM)/Level of Effort (LoE) for prioritized Work Package and individual tasks for upcoming release based on ROM/LoE; Identify communication need for the release. |
| 3 | Backlog grooming | For a release, determine which Integration Projects and Work Packages will be completed. |
| 4 | Implementation | • Completion of individual tasks<br>• Coordination among actors of a workflow |
| 5 | Integration testing | Testing workflow implementation. |
| 6 | Acceptance | End-to-end User Acceptance Testing (UAT) |
| 7 | General availability | Go Live |

Reference: PMO 3 – Communications Management Plan; PMO 4 – Communication Matrix; PMO 17 – State Project Team Onboarding Plan; MODINT 1 – Vendor Onboarding Plan; PMO 37 –Configuration and Continuous Integration Services Management Plan CCIS Plan; and PMO 9 – Orchestration Management Plan.

### 2.1.6 Onboarding and MoU Process

NM HSD has established a Memorandum of Understanding (MoU) process with external state agencies, federal agencies, partners, and other commercial organizations. These MoUs define the nature of data exchange between NM HSD and the business relationship between partners. The MoUs will also reference technical information in some cases as supporting detail. The ICD covers the complete technical details and their relationship between entities. Both MoUs and ICDs may cross reference each other to form a complete view of business and technical relationship stipulations.

The SI Contractor and NM HSD will work with each unique business partner regarding the details of how to establish end points between partners. These tasks will be included in the WBS that follows the iterative waterfall SDLC found in both Module Integration and Continuous Integration plans.

New or existing MoUs between NM HSD and partners may need to be created/updated to reflect the IP design, development and implementation details.

## 2.2 SDLC Execution for Interfaces

SDLC implementation involves simultaneous execution of several interfaces in different stages of the lifecycle. This is done to maximize the reusability of environments, and to minimize the blockage of progress due to constraints like environment availability, SME and stakeholder's availability, and technical feasibility.

The SI project uses an iterative waterfall approach to the SDLC across all implementation, configuration, and integration activities. A waterfall SDLC process follows a linear sequence of well-defined activities for Planning, Requirements Analysis, Design, Development, Testing, Implementation, and O&M, which are further described in the Project Management Plan and will not be repeated here.

Reference: PMO 37 – Configuration and Continuous Integration Services Management Plan; PMO 1 – Project Management Plan; PMO21 – Implementation Plan, PMO 14 – Test Management Plan; and PMO 20 – Release Strategy.

## 2.3 Interface Requirements Management

This section details the requirement elicitation process for all the interfaces as per the PMO 15 – Requirements Management Plan. The requirements management approach follows the Requirements Traceability Matrix (RTM) framework explained in PMO 16 – Requirements Traceability Matrix to support bi-directional traceability among requirements, design, and testing. The requirements for interfaces work stream aligns with and derives from the enterprise level workflow elicited by the SI team through the JAR/JAD sessions. The JAR/JAD sessions are conducted and coordinated by SI team business analysts with the help of NM HSD stakeholders. The requirements also align with the data modelling efforts as the new models developed will influence some of the Application Programming Interface (API) interfaces entity models.

Common parameters applicable to any interface are captured as shown in Table 3 – the ICD Lite template. An ICD specifies the interface requirements the participating systems must meet, the concept of operations for the interface, the message structure and protocols that govern the interchange of data, and the communication paths along which the project team expects data to flow.

## Table 3: ICD Lite Template

1. Revision History
2. General Interface Information

**2.1 Interface Identification**

| | | |
|---|---|---|
| 1 | Interface Unique ID | |
| 2 | MAD Interface Catalog (Row) | |
| 3 | HSD Interface Catalog (Row) | |
| 4 | HSD Data Service Exchange (Row) | |
| 5 | Interface Name | |
| 6 | Interface Type (Internal/External) | |
| 7 | Direction of Data (relative to HSD) | |

**2.2 Interface Description / Purpose**

| | | |
|---|---|---|
| 1 | What / Why | |
| 2 | Trading Partner (Dept/Org/Entity) | |
| 3 | Trading Partner Contact Info (name, phone, email) | |
| 4 | Processing Steps (narrative) | |
| 5 | Trigger (condition) | |
| 6 | Exception / Error Handling | |
| 7 | Formatted Output (report or other) | |
| 8 | Automated (Batch or Real-Time) vs. Manual Intervention | |
| 9 | Technical POC Contact Info (name, phone, email) | |

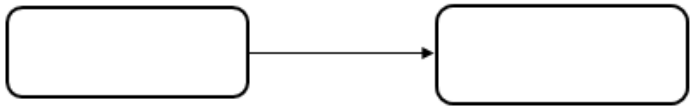
**2.3 Business Process**

| | | |
|---|---|---|
| 1 | MITA Business Area | |
| 2 | MITA Business Process | |
| 3 | JAD Date | |
| 4 | Visio interface reference number | |
| 5 | Other Reference Documents | |
| 6 | Business Owner/SME POC (Div / Dept / Org) | |
| 7 | Business POC Contact Info (name, phone, email) | |

**2.4 Data Flow Path**

| | | |
|---|---|---|
| 1 | Source System | |
| 2 | Source Application or Module | |
| 3 | Source Table | |
| 4 | Intermediate System | |
| 5 | Intermediate Application or Module | |
| 6 | Target System | |
| 7 | Target Application or Module | |
| 8 | Target Table | |

**2.5 Data Flow Diagram**



## 3. Detailed Interface Information

**3.1 Interface Data**

| | | |
|---|---|---|
| 1 | File Name | |
| 2 | File Type / Data Format (XML, CSV, EDI, Flat, other) | |
| 3 | File Structure (record types) | |
| 4 | Record Layout (data elements) | |

**3.2 Interface Rules and Controls**

| | | |
|---|---|---|
| 1 | Frequency / Schedule | |
| 2 | Transmission Protocol (FTP, TCPIP, other) | |
| 3 | Data Privacy Considerations (PHI, PII, FTI, other) | |
| 4 | Job Name | |

## 4. Business Feedback

**4.1 System Integration Considerations**

| | | |
|---|---|---|
| 1 | Current Pain Points | |
| 2 | Additional Notes | |

## 5. Other Information

**5.1 Record Layout**

**5.2 Source Table**

## 2.4 Interface Design Management

The interface work stream design is conducted according to the high-level design patterns explained in the System Design Document (SDD). Low-level ESB design patterns are detailed as part of the ESB Design documents and will be included in respective ICDs as appropriate, when additional details become available.

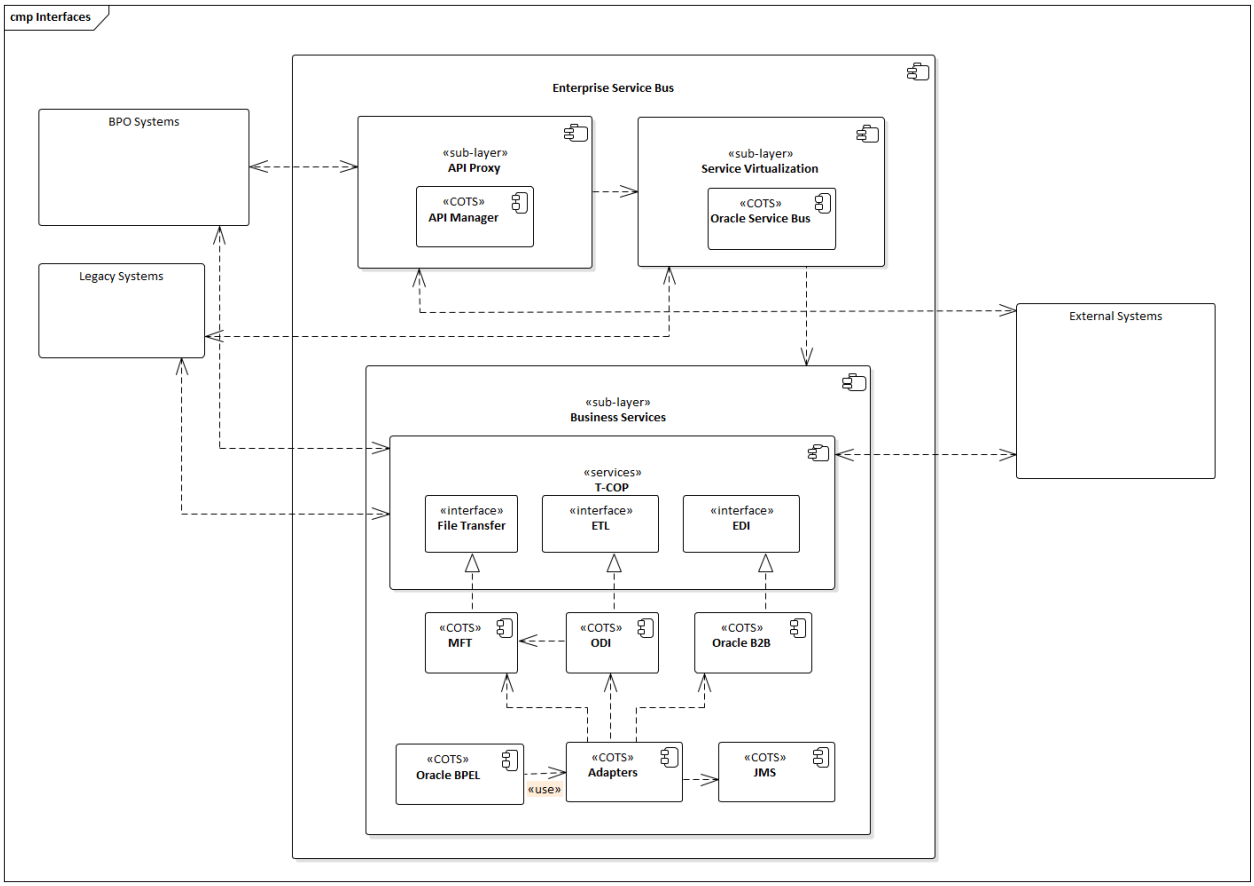
The SI solution will implement Interfaces using the Oracle Fusion Middleware Product stack, which includes SOA suite modules, database adaptors, Business-to-Business (B2B) adaptors, Oracle Data Integrator (ODI), Oracle Managed File Transfer (MFT), and other adaptors and connectors.

Traffic Cop (T-COP) is a framework that enables the business workflow engine, business process management, orchestration of services, execution of SI platform specific business logic and rules, EDI and bulk data processing, event handling and management of file transfers. It is implemented using Oracle Fusion Middleware components Oracle Business Process Execution Language (BPEL) and Oracle Business Process Management (BPM) which leverage other components of the platform namely Adapters, Managed File Transfer (MFT), ODI, B2B and BRE.

In addition, the interfaces leverage the security, auditing, diagnostics, transaction management, error, and exception handling features of the SI Contractor's ESB platform.

One primary interface pattern utilizes the conceptual framework of "services" being called and delivered through the use of APIs. Figure 5 below offers a generic representation of how either BPO systems or legacy module systems would join the IP and interface through the ESB to use the COTS products available in the IP.

Figure 5: Components of Interfaces Communication via ESB




## 2.4.1 File Transfer Interface

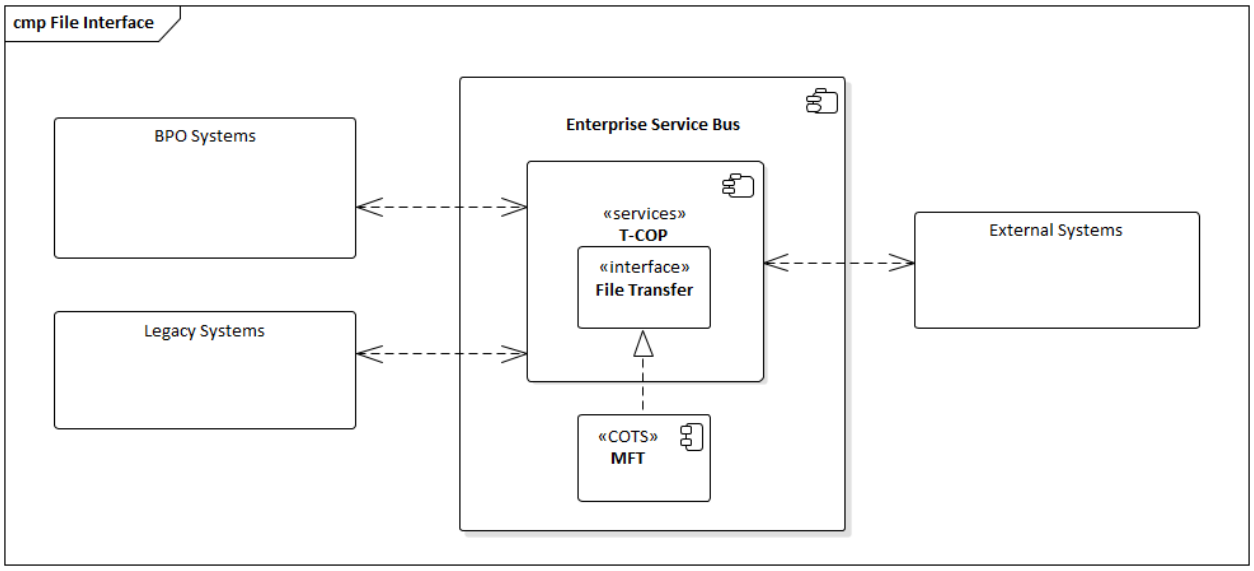
A second primary interface pattern uses the conceptual framework of secure file transfer protocols.

Oracle MFT is an integral part of the Oracle fusion middleware stack provided by the Integration Platform. Oracle MFT enables the MMISR vendors to communicate with external agencies using the following protocols:

- Secure File Transfer Protocol (SFTP)
- Secure Object Access Protocol (SOAP)/Representational State Transfer (REST) based web services

The MFT based ESB integration is explained in detail in the Section 7.2.5.3 of the SDD. This is a second primary interface

Figure 6: Example of File Transfer Interface



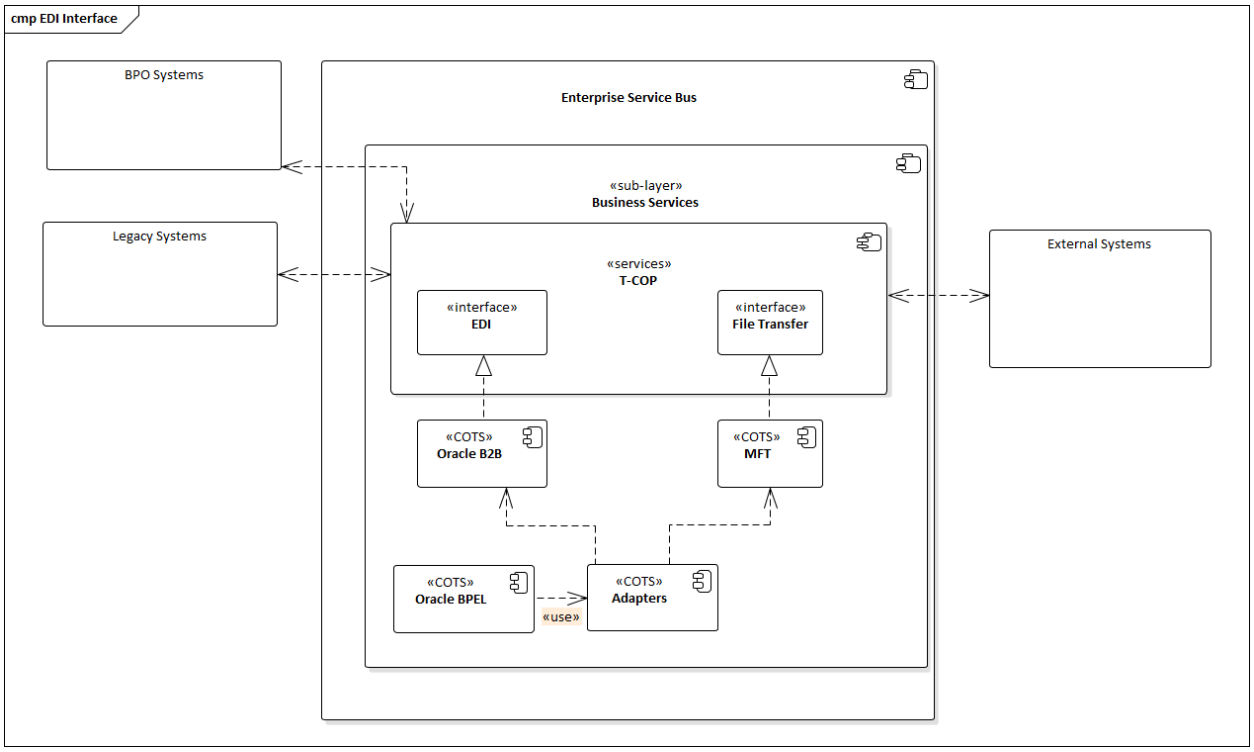

## 2.4.2 EDI Interface

Several interfaces of either design pattern (File transfer and Web services) in the HHS 2020 ecosystem use Electronic Data Interchange (EDI) file exchanges. The SI Platform's Oracle B2B enables exchanges of EDI messages between external trading partners and MMISR modules. Oracle B2B supports both the EDI for Administration, Commerce and Transport and X12 types of EDI. The integration platform acts as the transport and validation layer for EDI exchanges. The following two Workgroup for Electronic Data Interchange Strategic National Implementation Process (WEDI SNIP) types of the validation are supported by the Integration platform:

- Type 1: EDI Standard Integrity validation – Validate basic syntactical integrity of the EDI message.
- Type 2: Health Insurance Portability and Accountability Act (HIPAA) Implementation Guide Requirement validation – Validate HIPAA requirement-guide-specific syntax requirement by checking limits on repeat counts, used or not used qualifiers, code, elements, and segments.

WEDI SNIP Types 3 through 7 validations are performed by the respective MMISR module. The MMISR modules will configure their respective trading partner profiles on the SI Contractor-provided B2B platform, if needed. Some MMISR modules may bring their own EDI solutions and will not need to utilize the SI Contractor provided B2B platform; other module vendors may require the use of B2B to effectuate their EDI transactions if necessary to their business processes. The requirements for their validations are specified in the course of each vendor's implementation.

**Figure 7: Example of EDI Interface**




## 2.4.3 Interface Security

The SI platform handles the security for exchanges with external agencies. Each interface project will support the security requirements of message exchanges, i.e. conducting reliable messaging, including guaranteed message delivery (without duplicates) and support for non-deliverable messages within the HHS 2020 platform. Each interface project will not need to support the additional security requirements required for external interfaces communication.

For example, web services communication among HHS 2020 modules will only require one-way Secure Sockets Layer (SSL) authentication; however, the web services communication between the SI platform and the external agencies will be secured using two-way SSL.

The ESB platform security is detailed in Section 7.2.2 of the SDD.

Reference: SDD, Development Plan, Design Document – ESB and Orchestration Components of the Platform, and Design Document – Security.

Reference: SDD, Development Plan, Design Document – ESB and Orchestration Components of the Platform, and Design Document – Security.

# 2.5 Interface Implementation

## 2.5.1 Development of Interfaces

The development process of interfaces is derived from the specifications in the Development Plan. It outlines the logistics of working collaboratively with the other HHS 2020 stakeholders for the development of interfaces and how the process accounts for partial workflow implementations where services are not ready yet. It also describes how service catalogues are published and made available for the other stakeholders to integrate. These standards and tools are used during the development phase to ensure that the implementation of workflow orchestration adheres to the CMS Seven Standards and Conditions.

### 2.5.1.1 Identification of Development Task

The To-Be workflow design helps to identify services for implementation of workflows. An Integration Project is created based on To-Be workflow design. Work Packages are then identified and classified based on system owners and work streams. Individual tasks for IP that belong to an interface work stream identify the scope of development activity for a given iteration.

### 2.5.1.2 Development Methodology, Tools and Unit Testing

Once the identification of the development task is completed for a given iteration, developers are assigned the individual task related to the interface implementation. The LoEs of the individual task are taken into account to ensure uniform distribution of work in the interface work stream technical team.

Interface tasks development activity mainly involves service creation, application of business rules, and business SLA tracking. The SI Contractor uses the Commercial off-the-shelf (COTS) products to implement these features along with tools like Oracle SOA with Business Process Management (BPM) and Business Process Execution Language (BPEL), and Oracle Service Bus (OSB) for Service integration development. Oracle's Business Rules Engine (BRE) is used for business rules development. Technical SLA tracking is performed by Oracle EMCC and business SLA tracking is performed by Oracle BAM. These SLA trackers support regular data updates.

Oracle JDeveloper will be used to implement BPM workflow application. A developer can create a BPM application that consists of multiple BPM projects whereby each project represents a workflow. A project is not released for Systems Integration testing until it is completely coded and unit-tested. The JDeveloper provides integrated unit testing support for testing BPM projects. A test suite is created which consists of multiple test cases and can be triggered from the console. It is recommended to unit test the workflow before it is sent for peer review.

## 2.5.2 Integration with Orchestration Workflows

Service orchestration focuses on assembling vendor-developed services, interfaces, and enterprise shared services into a business workflow. All the services developed for a business workflow will likely require orchestration to be easily executed. The SI contractor will work with each MMISR module vendor to complete this orchestration.

### 2.5.3 Shared Services Utilization

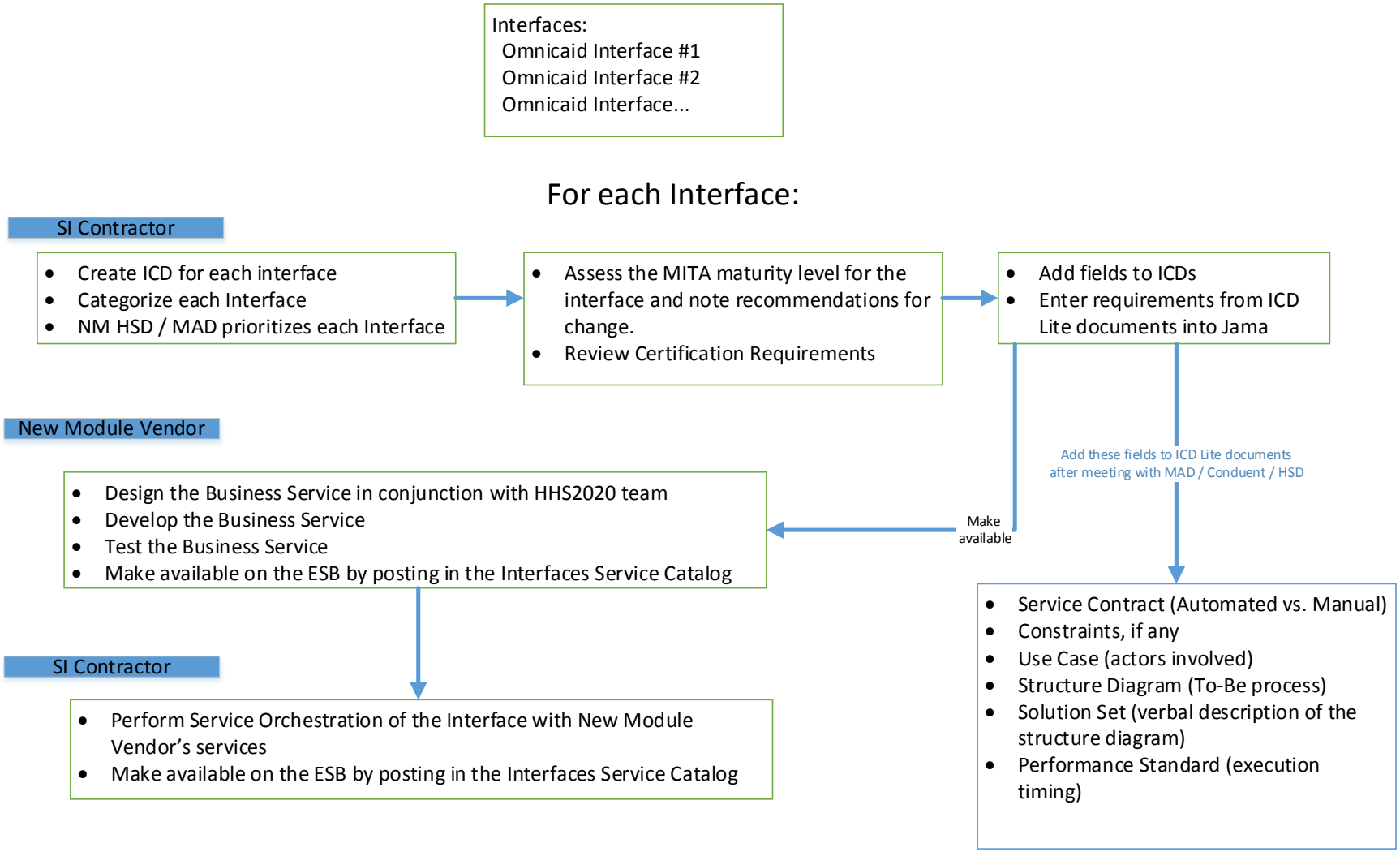
The interfaces work stream will utilize the Enterprise Shared Services as part of its implementation of functional Work Items. The enterprise shared services such as Master Data Management (MDM), Electronic Document Management (EDM), Address Standardized Verification and Validation (ASVV), and Customer Communication Management (CCM) engine will all be leveraged as part of the implementation of a BPEL workflow as deemed fit for requirements.

For example, as part of provider business relationship establishment, the address of the provider needs to be validated, standardized before being persisted into the Trading Partner Management System (TPMS). The operation of verifying and standardizing the address of the provider is invoked as an API to the ASVV API suite and the response will be used to proceed with the workflow.

### 2.5.4 Sample Scenario Describing Interfaces Management

The following is a sample scenario which models the activities associated with moving a set of interfaces from the currently existing Omnicaid system to the new SOA-based ESB architecture. Follow the arrows to understand the sequential steps involved in identifying and developing services for an interface.

**Figure 8: Interfaces Management Next Steps**



The steps above form the basis for Step 1 found in Table 2 – Stage-Wise Strategy for Interfaces (Section 2.1.4). An ICD will be completed for each interface to be converted in the MMISR project. The ICD provides the criteria for creating /processing the files as well as the transmission mechanism to the external agency who sends or receives the files. The SI Contractor will work with NM HSD to determine a relative priority for completing each interface into a logical progression. For example, it might make sense to group some interfaces together because they all deal with a specific agency and could enhance testing efforts.

The data in the ICD will be stored in Jama, becoming available to all contractors. This set of requirements becomes part of the Integration Backlog. After discussion and agreement with NM HSD, a new module contractor will be assigned several interfaces and begin development. Once completed, the new module contractor will notify the SI Contractor who will then perform orchestration of the newly created Interface service with other required services to create a "module" which would execute that interface on the ESB. A test cycle will be coordinated amongst the vendors to validate that the To-Be interface produces the same results as the As-Is interface.

Release Planning (Step 2 of Table 2 – Stage-Wise Strategy for Interfaces) helps to select the order for which interfaces will be worked soonest. Steps 3 through 7 of Table 2 round out the planning cycle for interfaces.

The SI Contractor will be working on the other services necessary for all interfaces to function on the ESB, i.e. the touchpoints for the interface.

A sample Project Plan below highlights the task flow for a single interface. The schedule will be repeated for all interfaces and will be added to the SI Integrated Project Plan Schedule as each new module contractor comes on board and offers their plan for each interface.

Joint planning among the new module contractors, NM HSD, and the SI Contractor will develop a plan for each release. Not all interfaces will be completed at the same time; thus, a logical grouping of interfaces will be incorporated into a release based on the length of time to complete the development SDLC, UAT testing with the SI Contractor, and the ultimate recipient of the interface. This "Backlog Grooming" activity, as noted in Table 2, Step 3, ensures that work is accomplished in an organized fashion for all parties involved (for example, that enough bandwidth exists for testing and working with NM HSD and its trading partners).

**Table 4: Sample Project Plan for Interface #1**

| Steps | Who |
|---|---|
| For each Interface: | |
| Complete the ICD, noting the criteria for creating the input/output file as well as the transmission mechanism | SI - Interfaces, HSD |
| Define the categories (CSV, EDI, etc. + Incoming/Outgoing, etc.); Touchpoints for ESB | SI - Technical |
| Update all ICDs with category and other info | SI - Interfaces |
| Discuss the MITA Maturity Level and note recommendations for change | SI - interfaces, HSD |
| Prioritize all interfaces | SI - interfaces, HSD |
| Load each Interface into Jama (priority, category, recommendations) | SI - Interfaces |
| Create an Integration Project for each interface and link to Jama | SI - Interfaces |
| | |
| Later, BTC selects Integration Projects (Interfaces) to be worked | BTC, HSD PMO |
| Joint effort to design service requirements for each Integration Project; Work Packages for each Contractor are created | SI - Interfaces, Module Contractors |
| A Level of Effort (LoE) and potential schedule is developed for each Work Package, yielding an overall Integration Project estimate and potential schedule | SI - Interfaces, Module Contractors |
| BTC reviews LoE and schedule to determine which Integration Projects can be completed for a release | BTC, HSD PMO |
| The composition of a release is set and the IMS is updated; BTC will review monthly to note progress and direct changes | BTC, HSD PMO |
| | |
| For each selected Integration Project (Interface): | |
| SI completes the Services for which they are responsible (API Touchpoints for ESB) | SI - Technical |
| | |
| Develop the service for Interface #1 - SDLC | |
| Design | Module Contractor #1 |

| | |
|---|---|
| Develop | Module Contractor #1 |
| Unit Test | Module Contractor #1 |
| Deliver to SI | Module Contractor #1 |
| | |
| Test the services for Interface #1 | |
| Load new services into Interface Services Catalog | SI - Technical |
| Perform Service Orchestration to combine services into a single module | SI - Technical |
| Verify that adequate / correct test data exists | Module Contractor #1 |
| Execute test for Interface #1 | SI - Interfaces, Module Contractor #1 |
| Verify test results | SI - Interfaces, Module Contractor #1 |
| Compare results with existing Interface #1 | SI - Interfaces, Module Contractor #1 |
| Document discrepancies; Identify who needs to fix | SI - Interfaces, Module Contractor #1 |
| Fix the service and test again | SI - Interfaces, Module Contractor # |
| Interface #1 is complete; Services can be run on ESB successfully | SI |

## 2.6 Interface Testing

Interface testing follows the Test Management Plan based on the CMS testing framework. Depending on the stage of testing, the integrating team will test the solution in isolation with mock mechanisms or integrate with other modules via the ESB and perform end-to-end testing of partial or complete workflows. The integrating test teams will produce test artifacts in the form of test cases and test plans. Test reports are generated out of X-ray based on the test executions as detailed in Section 2.7 of the TMP. The testing teams from the integrating modules and SI will produce the required reports for Test Readiness Review (TRR). The TRR assesses the test objectives, test methods and procedures, and the scope of tests. It confirms that test results from the completed test phase are complete and accurate. The test cases and test plans are associated to Jira issues and provides bi-directional traceability to the source requirements, as detailed in the RTM.

Figure 9: CMS Testing Categories


Predominantly, interface testing will validate all the file exchanges (EDI, ZIP, etc.) between NM HSD systems and external trading partners. Interface testing will also include validation of web services transactions that will be executed when exchanging data between NM HSD system(s) and external interfaces in real-time.

File transfer testing involves verifying and simulating the Oracle MFT configuration in lower environments, with or without Oracle B2B integration depending on the type of interface. Web services testing are tested in isolation using SoapUI, an API testing tool and as part of SOA BPEL composite.

The SoapUI tool offers the ability to mock any external service that needs to be tested by the platform. A mock service is a static emulation of an API. As a result, web services could be tested independently from any other external service.

### 2.6.1 Interfaces – Development Testing

The development testing encompasses infrastructure, unit, and Unit Integration Testing (UIT), and is carried out in the development environment. Each module contractor in a participating workflow will test their infrastructure in isolation. The report generation, file transfer configuration, and web service development are all tested in isolation as part of the unit testing. When at least two modules are ready to integrate, unit integration testing is performed just between those two modules.

Unit testing is the process by which individual units of source code and sets of one or more computer program modules are tested. Together with associated control data, usage procedures, and operating procedures unit testing determines whether the resulting code is fit for use.

For further details on the actors and process of the sub-phases of Development Testing phase refer to Section 4 of the TMP.

### 2.6.2 Interfaces – Validation Testing

Validation testing consists of a set of test functions performed within the QAT and SIT environments. The interfaces work stream relies on the integration testing and system testing of this phase to collaborate with all participating modules to perform integration and system testing respectively. Integration testing focuses on the integration of the individual system with one or more interfaces. System testing focuses on end-to-end functional validation with real interfaces using pre-defined integration test cases and test data. In addition, security testing is performed in this phase to ensure the entire integration is free of security vulnerabilities. The testing team, along with the trading partners and business owners, will run the test plan and identify and report on defects during test execution. These defects will be reported to the development team for resolution. When defect fixes are deployed and tested, regression testing will also be performed to ensure that the new code has no undesired consequence on the interface workflow.

Before entering the system testing phase in the SIT environment, the testing teams gets approval of the Test Readiness Review 1 (TRR1) report so that the applications can be promoted to the implementation testing phase.

For further details on the actors and process of the sub-phases of Validation Testing phase, refer to Section 5 of the TMP.

### 2.6.3 Interfaces – Implementation Testing

Implementation testing is performed on the UAT and production-like environments. The focus of this phase is the non-functional attributes of the solution such as security and performance. As the testing is conducted performance and security benchmarks are measured and set here. One of the objectives of this phase is to ensure that the application conforms to the System Security Plan (SSP). Security testing is used to verify and validate that the processes, business application, software platform, and infrastructure comply with the MARS-E security controls. Performance testing involves load and stress testing of the business application to ensure that the application and the underlying platform are capable of handling the surge in requests in the production environment.

Before entering the Agency Acceptance Testing (AAT) phase, the testing teams get approval from NM HSD of the Test Readiness Review 2 (TRR2) report so that the applications can be promoted to the production phase. AAT is the phase in which the identified acceptance test cases are executed and validated by NM HSD. The results of the AAT are presented to NM HSD in the form of AAT Summary Reports.

For further details on the actors and process of the sub-phases of Implementation Testing phase, refer to Section 6 of the Testing Management Plan.

### 2.6.4 Interfaces – Operational Testing

Operational testing confirms that the HHS 2020 enterprise solution is operational in accordance with architectural and technical requirements in the production environment. The objective of the operational phase is to verify the operational integrity, effectiveness, and resilience of the HHS 2020 enterprise solution in the production environment. The critical element of operational testing with respect to interfaces is monitoring and reliability testing. As part of the monitoring and reliability testing, the participating teams will ensure operational availability of the HHS 2020 enterprise solution and infrastructure by continuous monitoring of performance, incidents, and capacity utilization. In addition, operational contingency testing is performed on the production environment to ensure that the HHS 2020 business applications adhere to the Disaster Recovery Plan (DRP).

For further details on the actors and process of the sub-phases of Operational Testing phase, refer to Section 7 of the TMP.

### 2.6.5 Interfaces – Testing Patterns

Various testing patterns required to test the interfaces are identified and described as part of SIPLT 40 – System Test Plan (STP) – ESB and Orchestration Components of the Platform.

## 2.7 Operation and Maintenance

Once the solution is in production and operational, the daily operations require system monitoring to ensure that system is running without any issues and errors are monitored and propagated to ensure proper handling of those errors. The daily operation involves monitoring of systems to identify bottlenecks in advance. Automated alert generation scripts are put in place to generate an alert in case the thresholds are crossed.

The solution provides high availability to minimize service outages. In case a service outage does happen, the Operations team needs to coordinate to ensure all the participating systems are notified. The service resumption procedure ensures that backlog messages do not choke the system.

There are planned service outages for maintenance needs that are coordinated among the operation team. A Standard Operating Procedure (SOP) is established to address the notifications to all the relevant stakeholders and define action to be taken by each of the stakeholders in case of planned service outage.

Reference: PMO 20 – Release Strategy and PMO 1 – Project Management Plan.

## 2.8 MITA Strategy

The MITA strategy describes the SI approach to ensuring that the Interface Management Plan aligns with MITA and supports the NM MITA Roadmap for enhancing the MMIS such that the capabilities reach MITA Maturity Level 4, where possible.

This section contains the following information as it pertains to Interface Management:

- MITA Goals
- Advancement of MITA Maturity
- Approach to MITA Maturity

The information gathered on MITA Strategy feeds into the MMIS Certification activities. The end results can be used by the State in subsequent MITA State Self-Assessments.

As an integral part of the MITA Strategy, adherence to the MITA Seven Conditions and Standards will be included in the evaluation of the advancement of the MITA Maturity. Detailed information on the SI Contractor's MITA Strategy can be found in the CCIS Plan.

### 2.8.1 MITA Goals/Advancement of MITA Maturity

Based on the current MITA State Self-Assessment (SSA), the current business, information and technical architectures are at a MITA Maturity Level of 1 or 2. The goal is to advance the MITA Maturity for the MMISR to Maturity Level 4.

In addition, adherence to the Seven Conditions and Standards will be included in the evaluation of the advancement of the MITA Maturity.

The resulting MITA goals are integral to the Certification activities of the MMISR.

### 2.8.2 Approach to the Advancement of MITA Maturity

The SI Certification Team identifies MITA Capabilities from the information architecture, technical architecture, and business architecture that are applicable to interfaces. This includes identification of the CMS Seven Conditions and Standards that apply. These identified capabilities are documented as part of the design and testing of the MMISR and its interfaces.

This information will be reviewed by CMS as part of the MMIS Certification during formal Medicaid Enterprise Certification Life Cycle (MECL) reviews, as identified in the MMIS Certification section of this deliverable.

# 3 CMS Certification

This section documents the approach to CMS Certification related to this deliverable. The documented processes are followed, and the changes will be documented and tracked throughout the entire project life cycle. This deliverable will be reviewed by CMS during the following MECL reviews:

- R2, Operational Milestone Review
- R3, CMS Certification Final Review

This deliverable may also be reviewed by CMS during informal reviews, including Consults and Gate Reviews.

Appendix D: MECT Checklist and Programmatic Critical Success Factors (CSFs) contains the MECT and Critical Success Factor items that are attributable this deliverable.

The Certification Process Guide contains detailed information regarding the CMS Certification approach.

**Critical Success Factors (CSFs)**

The MECL incorporates CSFs into the certification process. There are two types of CSFs—programmatic and functional. Programmatic CSFs identify activities the state PMO will need to perform in managing its MMIS project. They are found in the Programmatic Tab of the Independent Verification and Validation (IV&V) Progress Report Template, which the IV&V contractor fills out as part of the regular progress reports.

MMIS functional CSFs report the status of the business CSFs with a focus on those that are not met. Should a business improvement require interface management then those requirements will be introduced into the MMIS project.

# 4 Applicable Standards

Interface design, development and implementation supports the IP meeting all applicable standards as outlined in PMO 12 – Governance Standards – Technical and Architectural.

# 5 Assumptions / Constraints / Risks

## 5.1 Assumptions

This section describes an initial set of assumptions which may be updated over time.

1. MMISR resources are available to engage in this work stream.
2. External interface partners and associated vendors are available to support interface projects.
3. All interfaces will be identified, prioritized, and selected for implementation with NM HSD concurrence and approval.
4. Interfaces will use “out-of-the-box” connectors to connect and exchange data with interface partners. If custom implementation is required, it will be implemented upon approval of design after discussion with NM HSD.
5. The SI Contractor has an oversight role on New Module only interfaces; the new module contractors need to follow the processes laid out in the Interface Management Plan and Service Orchestration Plan.
6. The current inventory of interfaces is documented in the NM HSD procurement library, ASPEN documentation, and the DGC library.
7. In order to meet MITA goals, NM HSD will decide if the As-Is interface mechanism changes or remains the same. The SI Contractor will only make recommendations.
8. Interface rollout prioritization will be based on the new module rollout schedule.

## 5.2 Constraints

There are no constraints that are specific to Interfaces.

## 5.3 Risks

This section describes an initial set of risks, which will be updated and managed per the Risk Management Plan.

The interfaces work stream involves several risks, most importantly due to the interoperability factor of integrating with multiple external partners and agencies that are operating outside of the HHS 2020 ecosystem and have individual standards and platforms.

1. **Technology Risks** – Each of the interfacing partners and agencies are constrained by their native technology stack which will partially or completely restrict interfacing with them. This risk will prevent consolidation of the interfaces with a handful of protocols, toolsets, and frameworks.
2. **Budgetary Risks** – While the Integration Platform is standards driven and can integrate with any external partners supporting these standards, there is a risk of that some partners may require legacy or custom protocols, thereby increasing the budgetary requirements for the interfaces work stream.
3. **Quality Risks** – It is possible that the legacy interfaces may not be adequately documented, in which case as new modules take over the interfaces there may be issues with the message interaction and the data in the messages.
4. **Testing Risks** – Interface partners may not be able to provide a testing/integration environment, leading to an inability to test the integration thoroughly before promoting to the Production.
5. **Schedule Risks** – The interfaces work stream activities are directly dependent on the rollout of the SI platform and the new modules.
6. **Security Risks** – Though the Integration Platform recommends security standards, protocols, and practices, some of the interface partners may not be able to support the standards and instead support only a predecessor/deprecated version of them. For example, some interface partners will only be supporting SSL, while the preferred standard for the Integration Platform is the successor of SSL, TLS (Transport Layer Security). Deprecated versions of protocols will lead to security risks like Man-In-the-Middle-Attack (MITM).

Reference: PMO 7 – Risk Management Plan

# 6 Requirements Traceability

Interface projects manage requirement discovery, documentation, and traceability as prescribed in PMO 15 – Requirements Management Plan and PMO 16 – Requirements Traceability Matrix.

# 7 Appendices

## 7.1 Appendix A: Interfaces Use Cases

The use cases described here are replacements for the provider interfaces currently operated out of the Omnicaid system. This section outlines the design of the Oracle Fusion Middleware (MW) elements that will be used to, repeatedly, implement an interface to the HHS 2020 enterprise. These external interfaces are built on top of the existing Oracle Fusion MW based ESB framework.

As these interfaces are exposed to the public internet for third-parties to consume, they have added levels of security. The toolset of API Manager, OSB, MFT, and SOA are used to transact with external entities. Among the Oracle Fusion MW components, Oracle MFT will be the external partner facing tool for all file transfer use cases. Oracle API Manager and Oracle OSB will be the external partner facing tools for web services based use cases. All the components used for external communication are depicted in Figure 5: Components of Interfaces Communication via ESB.

The following sections define the significant interfaces of specific tools and their usage, followed by two use cases, where these tools are utilized to provide external interface service for the Provider domain.

### 7.1.1 Interfaces Using Oracle Fusion MW Components

This subsection describes how each of the Oracle Fusion MW components are utilized in the external interface design. Ancillary components like Oracle Business Activity Monitoring (BAM), Enterprise Manager Cloud Control (EMCC), are not described here; more details about them can be found in the SDD and other ESB design documents.

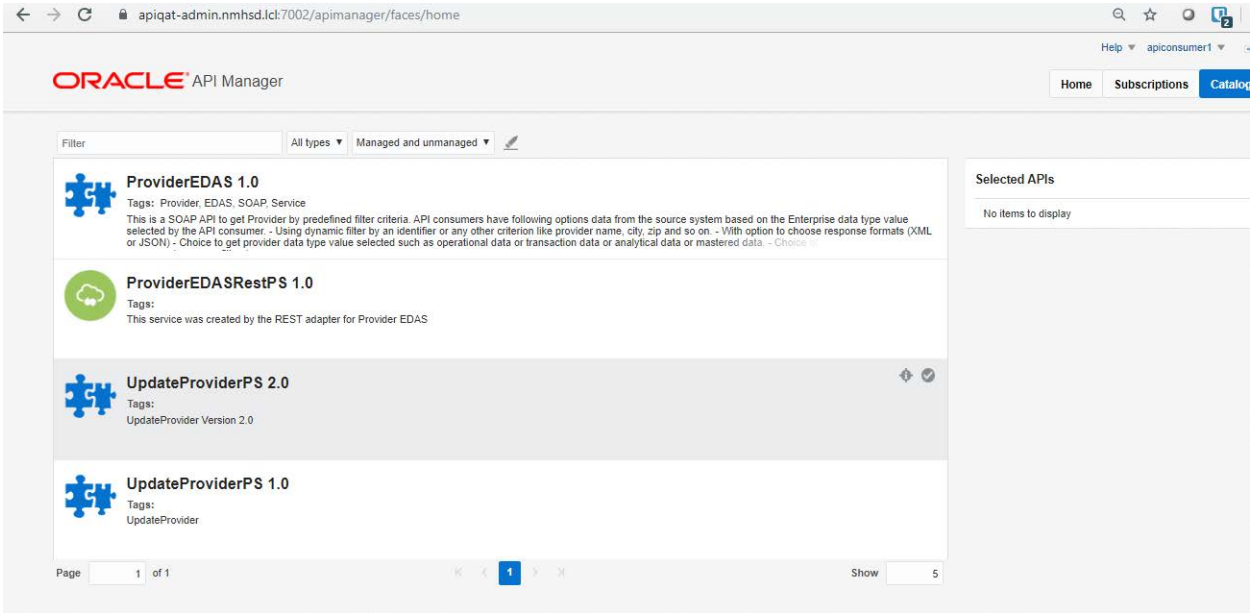
**Publishing External Web Services via API Manager**

The API Manager is installed in conjunction with the OSB, with which developers can create Web Services Description Language-based (WSDL) SOAP proxy services as well as Web Application Description Language-based (WADL) REST proxy services to be published as APIs, as shown in the example below. To access API Manager, any consumer needs to have a valid credential.

These two components (API Manager and OSB) service the incoming and outgoing web services (SOAP or REST) from and to any external partners of the SI platform. The web services published on API Manager are visible internally to HHS 2020 modules and also to the external entities like CMS. A consumer can view the API metadata, such as payload structure (WSDL or WADL) and business description. However, to invoke these APIs, the internal and external partners need to have an entitlement key generated per API and place it in the request headers. APIs which are available only by subscription are called Managed APIs. Unmanaged APIs, on the other hand, does not require subscription keys. In addition to these subscription keys, each API will have a corresponding security policy, with which the validations will be performed.

Here, the Provider Enterprise Data as Service incoming endpoint is published as both SOAP and REST web services for any partner to subscribe to and consume. The payload, in this case, is the header and body content of the web service call is two-way SSL encrypted as noted in the Subsection 3.4.3 Interfaces Security. The two-way SSL ensures both the external partner and SI platform engage in a mutual authentication and validate each other.

Figure 10: Oracle API Manager – API Catalog



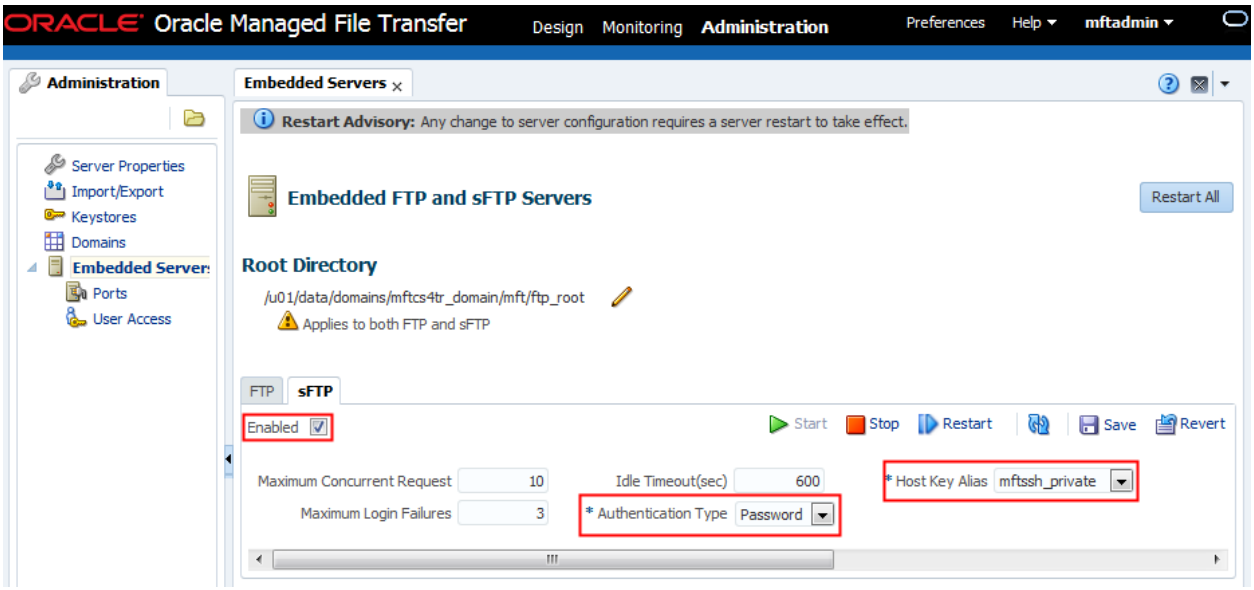

The Oracle API manager security service is integrated with the Oracle IDM solution, which provides integration with users and groups for API access.

**Publishing Files on SFTP Server with Oracle MFT**

In the case of external file-based transfers defined in Subsection 3.4.1, SFTP servers are established on top of the Oracle MFT component. Once the SFTP server is established and published to external parties, the same can be used to transfer and receive files of any type and size. The embedded SFTP servers use the Advanced Encryption Standard (AES) as the standard symmetric encryption algorithm to secure the file-based transactions. This is done to ensure that even when some unauthorized users manages to breach, the file contents remain intact as it cannot be read or modified without encryption keys.

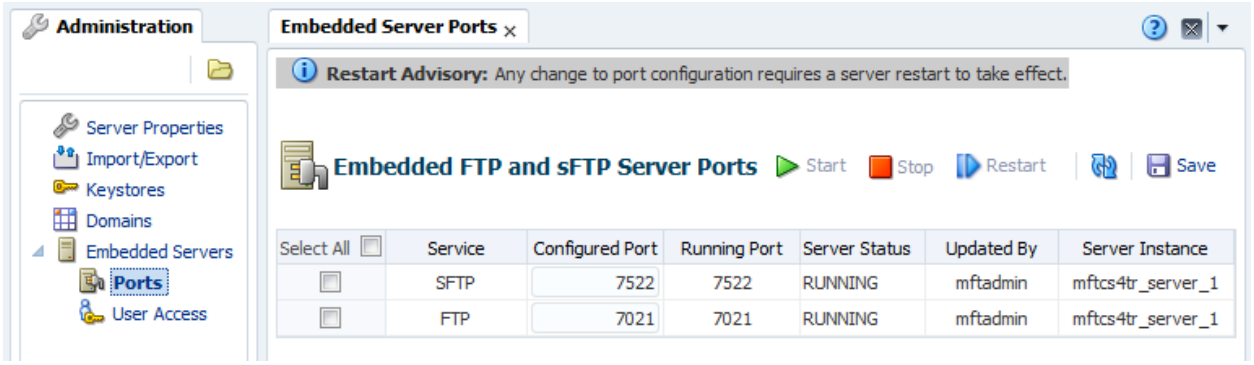
The following image depicts the creation of embedded SFTP server on an Oracle MFT instance. Compared to a standalone SFTP server, the embedded servers offer additional benefits like integration with rest of Oracle Fusion MW toolsets like BAM, EMCC. These integrations provide technical and business visibility into the file transfer process and corresponding interfaces. The files are encrypted, and password-protected to ensure only intended recipients are able to open and read the contents of the file.

Figure 11: Oracle MFT – Create Embedded SFTP Server




Once these embedded SFTP servers are created, respective inbound and outbound folders are created per interface partners to ensure compartmentalized access control.

Figure 11: Oracle MFT Embedded Servers



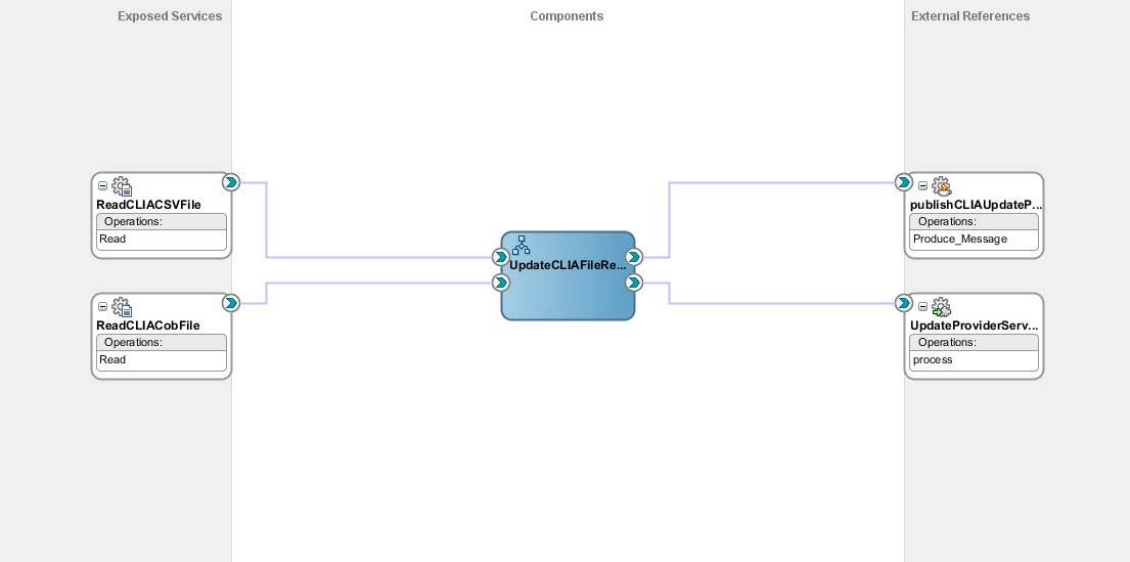

The SFTP is a method that allows a file transfer using the Secure Shell (SSH) protocol. SFTP encrypts the data using modern methods and protects the integrity of data.

**Orchestrating Workflows via SOA Suite**

Post entry of data inside the Oracle Fusion MW components, the core business validation, and processing occurs in the BPEL layer. At this point, both internal workflows and external interfaces driven workflows are handled by the same Oracle components as the OSB and SOA Suite.

The following figure depicts services designed and exposed via Oracle BPEL Process Manager. The SOA Suite also integrates with Oracle Business Rules for making runtime business decisions in the workflow. Similar to other Oracle tools, the SOA Suite also integrates with BAM and EMCC to provide business and technical metrics respectively.

Figure 12: Oracle SOA Suite – BPEL Workflows




## 7.1.2 Update Provider via ESB

At present, the Omnicaid system receives files and updates the provider database. In the Oracle Fusion MW enabled ESB platform, the Oracle system components like API Manager, OSB, and SOA/BPEL are utilized. This use case shows the workflow originating from an external partner, CMS, to make an update to a Provider entity via the API interface exposed through API Manager and built on OSB and SOA/BPEL. The request payload (XML) will be persisted in the Oracle RAC database for auditing purposes in non-production environments. The duration of storage is dependent on the retention policy guidelines. In the production environment, the entire payload will not be persisted, however, key information related to the API are persisted for generating business metrics.

The endpoints for Provider Update or any other business workflow are created for reusability. Re-usability provides the following benefits:

- Avoids service proliferation
- Ease of maintenance, both at application and testing level.

However, if the business workflow demands a separate endpoint, it needs to be custom created for the given interface.

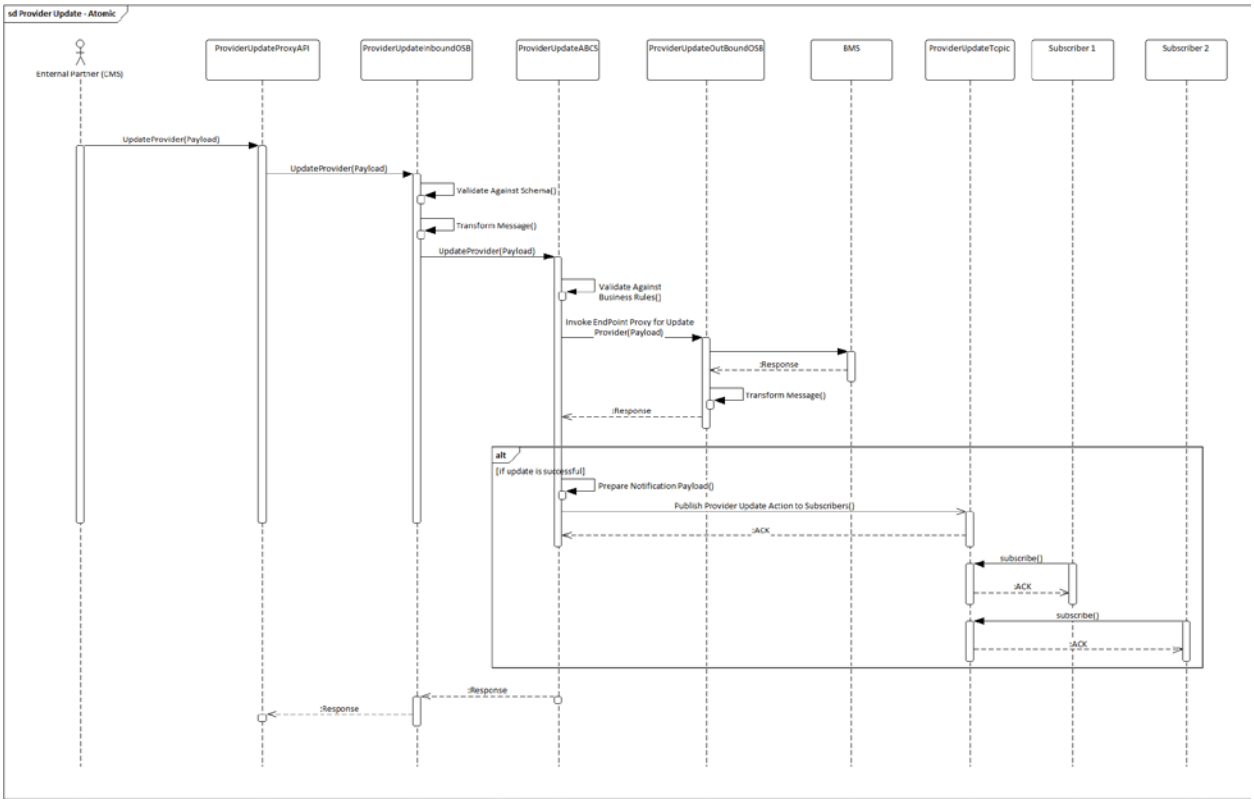
Subcomponents of the Update Provider service on ESB include the following:

- **ProviderUpdateProxyAPI** – The proxy service is exposed on the API Manager component of the Oracle Fusion MW and will be the single point of entry for any update of provider information across HHS 2020. API Manager serves as the entry point for all API invocation. The subsequent business logic and validations are built in the OSB and BPEL components.
- **ProviderUpdateInboundOSB** – The OSB service is the second layer in this API and provides syntactic and semantic validation of the API.
- **ProviderUpdateABCS** - The role of the Application Business Connector Services (ABCS) is to expose the HHS 2020 business functions provided by the participating module in a

representation that is agreeable to a service Interface. In the SI platform's canonical integration style, the common service interface is the one exposed by ESB. It can also serve as a glue to allow the participating application to invoke the EBSs.

- **ProviderUpdateOutboundOSB** – Requests originating with the ESB and terminating in any of the external module, Benefits Management System (BMS) in this case, will use the this service to route the API call.
- **ProviderService - BMS** – This subcomponent is the core business module exposing all operations related to the provider. BMS module is the authoritative source of provider information across the enterprise.
- **ProviderUpdateTopic** – This subcomponent is a sub workflow to ensure that any parties interested in learning and consuming the update to the provider object, can consume through this JMS (Java Messaging Service) Topic.

**Figure 13: Update Provider Entity - Sequence of Request and Response**




## 7.1.3 Get Provider via ESB

The Get Provider APIs act as the central point for any internal or external consumer to retrieve information about the Get Provider Service. The ESB will provide the option for internal or external consumers to retrieve provider data through the Get Provider Service. This use case shows the workflow originating from an external partner, CMS, to retrieve a Provider entity via the API interface.

The Get Provider Service will have the following options:

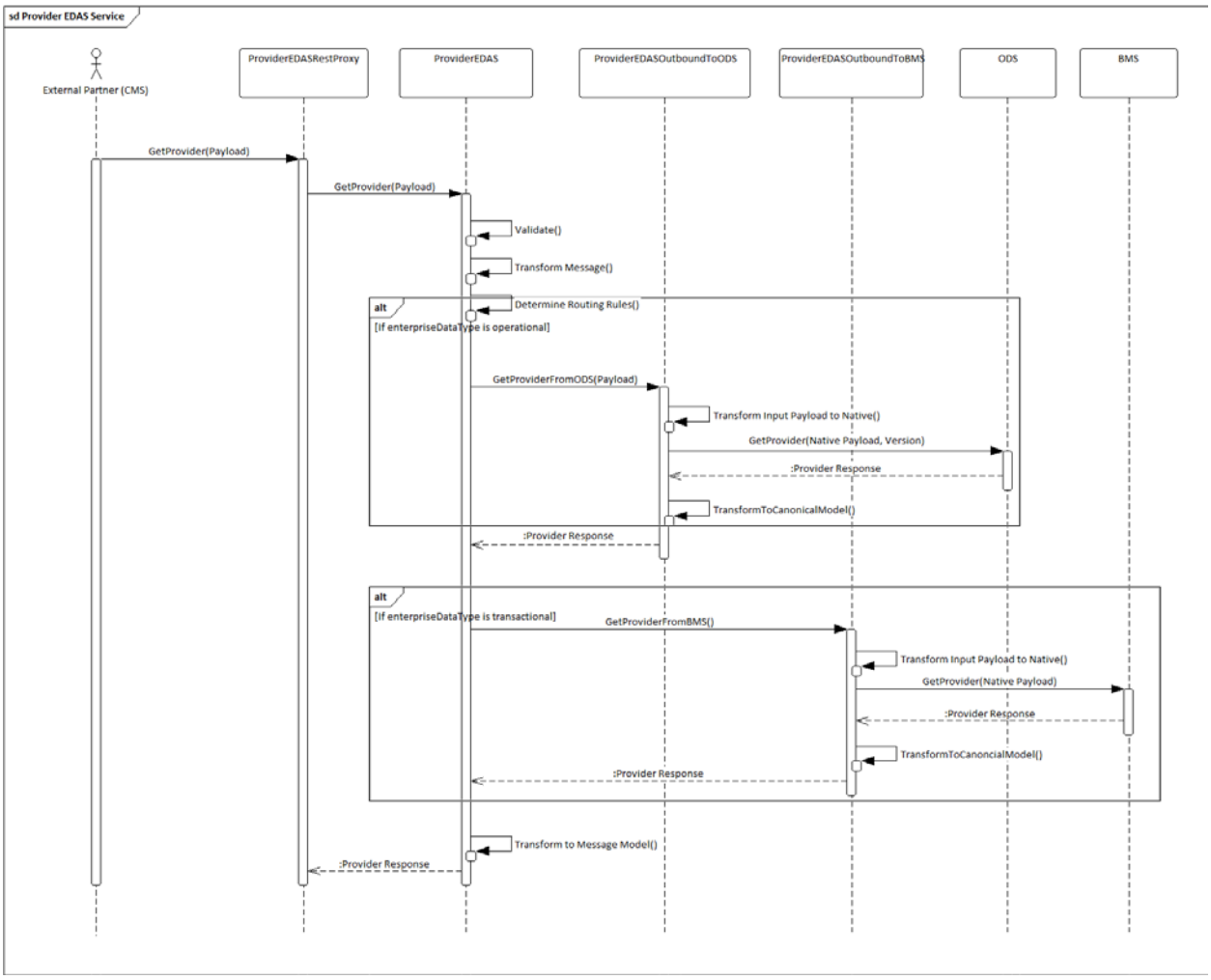
- Dynamic Search Filters
    - Filter criteria from a predefined list of elements listed below:
        - Provider Network identifier
        - Provider Type
        - Specialty
        - First Name
        - Last Name
        - Organization Name
        - Address Type
        - City
        - State
        - Zip
        - Country Code
    - The criteria shall be in key=value where the key is the field name to filter the records (city=Santa Fe).
    - The client must supply at least one key-value pair.
    - The multiple key-value pairs are joined by AND expression.
    - If the key-value passed in the request is not part of the enumeration, the request will be rejected with a message.
- Dynamic Response Formats for REST Services (XML or JSON)
    - The client has the option to request the response in XML or in JSON by providing the mime type in Accept header in the HTTP request.
    - The following is the syntax of the header.
    - Accept: <MIME_type>/<MIME_subtype> [application/json, application/xml].
    - If the header is not found in the request, the service will consider the JSON as default.
- Variable Response Sets
    - The caller will have the ability to filter the response by sub-entity names. Example: responseSet=Basic, ProviderNpi, ProviderAddress, ProviderSpeciality, ProviderTaxonomies, ProviderAffiliations.
    - Where basic is the provider entity alone (main entity). Rest of the values are the sub-entities of the provider domain.
- Dynamic Section of the Data Source Based on Input from the Caller
    - The caller will have the option to select the source from where data will be fetched. This depends on the type of information required by the consumer. Source options are source module (BMS) for the most current data, Operational Data Store for transactional data, MDM for master data, and DS for any reports.
      If no value is provided, ESB will consider the source module as the default source.

Subcomponents of the Get Provider Service on ESB include the following:

- **ProviderEDASRestProxy** – The proxy service is exposed on the API Manager component of the Oracle Fusion MW and will be the single point of entry for any read or get operation of provider information across HHS 2020.
- **ProviderEDAS** – Provider Enterprise Data as Service (EDAS) is the centralized API hosted on the ESB platform for retrieval of provider information in both atomic and batch fashion. Depending on the consumer's interest, the EDAS will respond with analytical or mastered or transactional data of the provider(s).

- **ProviderServiceODS** – The source of all transactional data of providers are exposed via this service.
- **ProviderServiceBMS** – The source of all operational data of providers are exposed via this service.

Figure 14: Get Provider Entity - Sequence of Request and Response




## 7.2 Appendix B: Deliverable Record of Changes

Table 5: Record of Changes

| Version Number | Date | Author / Owner | Description of Change |
|---|---|---|---|
| V0.1 | 4/8/18 | Hans Bhatia | Initial Draft |
| V0.2 | 5/14/18 | Hans Bhatia | Revised Draft |

| Version Number | Date | Author / Owner | Description of Change |
|---|---|---|---|
| V0.3 | 5/22/18 | Hans Bhatia | Revised Draft to align with PMO37 and based on HSD comments |
| V0.4 | 2/07/19 | Tom Costa | Rewrite based on consultation with team and HSD |
| V0.5 | 2/10/19 | Tom Costa | Rewrite based on consultation with team and HSD |
| V1.0 | 3/6/19 | Tom Costa | Rewrite based on consultation with team and HSD |
| V1.0 | 3/28/19 | Tom Costa | Re-delivered Final-Draft after modification due to expected contract modifications regarding SI responsibilities. |
| V1.0 | 4/29/19 | Tom Costa | Re-delivered Final-Draft after responding to all HSD comments. |
| V1.1 | 7/18/19 | Henry Huston | Re-reviewed Final-Draft to ensure alignment with PMO9 and PMO37. |
| V1.2 | 8/1/19 | Dawn Gelle | Small edits for clarification. |
| V1.3 | 8/26/19 | Henry Huston Dawn Gelle | Revised to address HSD comments. |
| V1.4 | 8/29/19 | Dawn Gelle | Re-review of all HSD comments to ensure completeness. |
| V1.5 | 9/5/19 | Pradeep Thopae | Inclusion of Use Case examples. |
| V1.6 | 9/20/19 | Linda Perrett/Dawn Gelle | Update of Use Case examples and QC of updates. |
| V1.7 | 10/7/19 | Pradeep Thopae/Dawn Gelle | Updated use cases, completed comments from 9/25/19 comment review meeting, verified MECT table. |
| V1.8 | 10/14/19 | Pradeep Thopae | Updated use cases. |

Changes to the SIPLT 88 – Interface Management Plan deliverable after initial approval will follow the process documented in PMO 10 – Change Control Management Plan.

## 7.3 Appendix C: Acronyms

The table below represents the common acronyms utilized for the HHS 2020 procurements. This list is subject to change over the course of the procurement process.

Table 6: List of Acronyms

| Acronym | Definition |
|---|---|
| AAT | Agency Acceptance Testing |
| ABCS | Application Business Connector Services |
| AES | Advanced Encryption Standard |
| ALTSD | Aging and Long-Term Services Department |
| ANSI | American National Standards Institute |
| API | Application Programming Interface |
| ARB | Architecture Review Board |
| ASPEN | Automated System Program and Eligibility Network |
| B2B | Business-to-Business |
| BA | Business Analyst |
| BAM | Business Activity Monitoring |
| BHSD | Behavioral Health Services Division |
| BPEL | Business Process Execution Language |
| BPM | Business Process Management |
| BPO | Business Process Outsourcing |
| BRE | Business Rules Engine |
| BTC | Business Transformation Council |
| CCIS | Configuration and Continuous Integration Services |
| CCM | Customer Communication Management |
| CMMI | Capability Maturity Model Integration |
| CMS | Centers for Medicaid and Medicare Services |
| COTS | Commercial off-the-shelf |
| CR | Change Request |
| CSED | Child Support Enforcement Division |
| CSF | Critical Success Factor |
| CYFD | Children, Youth, and Families Department |
| DGC | Data Governance Council |
| DOH | Department of Health |
| DRP | Disaster Recovery Plan |
| DS | Data Services |
| DWS | Department of Workforce Solutions |
| EDAS | Enterprise Data as Service |
| EDI | Electronic Data Interchange |
| EDIFACT | Electronic Data Interchange for Administration, Commerce and Transport |
| EDM | Electronic Document Management |
| EMCC | Enterprise Manager Cloud Control |
| ESB | Enterprise Service Bus |

| Acronym | Definition |
|---|---|
| ESS | Enterprise Shared Services |
| ETL | Extract Transform and Load |
| FHIM | Federal Health Information Model |
| FISMA | Federal Information Security Management Act |
| FK | Foreign Key |
| FPLS | Federal Parent Locator Service |
| FTI | Financial Transaction Information |
| HHS | Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act |
| HL7 | Health Level 7 |
| HSD | Human Services Department |
| HTTPS | Hypertext Transfer Protocol Secure |
| ICD | Interface Control Document |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IMS | Integrated Master Schedule |
| IP | Integration Platform |
| ISD | Income Support Division |
| ISO | International Organization for Standardization |
| IV&V | Independent Verification and Validation |
| IWG | Interface Workgroup |
| JAD | Joint Application Design |
| JAR | Joint Application Requirements |
| JSON | JavaScript Object Notation |
| LDAP | Lightweight Directory Access Protocol |
| LoE | Level of Effort |
| MAD | Medical Assistance Division |
| MITM | Man-in-the-middle (attack) |
| MDM | Master Data Management |
| MECL | Medicaid Enterprise Certification Life Cycle |
| MECT | Medicaid Enterprise Certification Toolkit |
| MFT | Managed File Transfer |
| MITA | Medicaid Information Technology Architecture |
| MMISR | Medicaid Management Information System Replacement |
| MoU | Memorandum of Understanding |
| MW | Middleware |
| NIEM | National Information Exchange Model |
| NM | New Mexico |
| O&M | Operations and Maintenance |
| ODI | Oracle Data Integrator |
| OSB | Oracle Service Bus |
| PCI | Payment Card Industry |
| PHI | Personal Health Information |
| PII | Personally Identifiable Information |

| Acronym | Definition |
|---|---|
| PK | Primary Key |
| PL | Procedural Language |
| PMBOK | Project Management Body of Knowledge |
| PMO | Project Management Office |
| POC | Point of Contact |
| PPQA | Product and Process Quality Assurance |
| REST | Representational State Transfer |
| ROM | Rough Order of Magnitude |
| RTM | Requirements Traceability Matrix |
| SAMHSA | Substance Abuse and Mental Health Services Administration |
| SAML | Security Assertion Markup Language |
| SDD | System Design Document |
| SDLC | Software (or System) Development Life Cycle |
| SFTP | Secure File Transfer Protocol |
| SI | System Integrator |
| SLA | Service Level Agreement |
| SMA | State Medicaid Agency |
| SME | Subject Matter Expert |
| SMR | System Migration Repository |
| SOA | Service-Oriented Architecture |
| SOAP | Simple Object Access Protocol |
| SOP | Standard Operating Procedure |
| SQL | Structured Query Language |
| SRC | System Review Criteria |
| SSA | State Self-Assessment |
| SSL | Secure Sockets Layer |
| SSP | System Security Plan |
| STP | System Test Plan |
| TCP | Transmission Control Protocol |
| TMP | Test Management Plan |
| TPMS | Trading Partner Management System |
| TRR | Test Readiness Review |
| UAT | User Acceptance Testing |
| UIT | Unit Integration Testing |
| WADL | Web Application Description Language |
| WBS | Work Breakdown Structure |
| WSDL | Web Services Definition Language |
| XML | eXtensible Markup Language |
| XSD | XML Schema Definition |

| | |
|---|---|
| PMO | Project Management Office |
| POC | Point of Contact |
| PPQA | Product and Process Quality Assurance |
| REST | Representational State Transfer |
| ROM | Rough Order of Magnitude |
| RTM | Requirements Traceability Matrix |
| SAMHSA | Substance Abuse and Mental Health Services Administration |
| SAML | Security Assertion Markup Language |
| SDD | System Design Document |
| SDLC | Software (or System) Development Life Cycle |
| SFTP | Secure File Transfer Protocol |
| SI | System Integrator |
| SLA | Service Level Agreement |
| SMA | State Medicaid Agency |
| SME | Subject Matter Expert |
| SMR | System Migration Repository |
| SOA | Service-Oriented Architecture |
| SOAP | Simple Object Access Protocol |
| SOP | Standard Operating Procedure |
| SQL | Structured Query Language |
| SRC | System Review Criteria |
| SSA | State Self-Assessment |
| SSP | System Security Plan |
| STP | System Test Plan |
| TCP | Transmission Control Protocol |
| TMP | Test Management Plan |
| TPMS | Trading Partner Management System |
| TRR | Test Readiness Review |
| UAT | User Acceptance Testing |
| UIT | Unit Integration Testing |
| WBS | Work Breakdown Structure |
| WSDL | Web Services Definition Language |
| XML | eXtensible Markup Language |
| XSD | XML Schema Definition |

## 7.4 Appendix D: Glossary

A glossary of project-specific terminology is maintained on the SI Contractor SharePoint site which can be found:

***REDACTED DUE TO SECURITY CONCERNS***

## 7.5 Appendix E: MECT Checklist and Programmatic CSF

This section provides a table with items from the Medicaid Enterprise Certification Toolkit (MECT) Checklist attributable to this deliverable.

Table 7: MECT Checklist

| Checklist ID | Requirement Text / System Review Criteria (SRC) | MITA Business Area Module Checklist Set | Business Process | CMS Guidance |
|---|---|---|---|---|
| CM.CM23.1 | The system receives and processes PCP registry data from MCOs. | Care Management | Benefit Management Services | N/A |
| CO.CM23.1 | The system receives MCO contract information from contract data store (e.g. address, covered services, rates). | Care Management | Manage Contractor Information | N/A |
| EE.CM23.1 | The system receives and processes eligibility data from state's eligibility source system. | Care Management | - | N/A |
| EE.CM23.2 | SMA receives and processes provider eligibility data from MMIS or data repository for PCP program. | Care Management | - | N/A |
| OM.CL3.8 | SMA provides prompt response to inquiries regarding the status of any claim through a variety of appropriate technologies, and tracks and monitors responses to the inquiries. Processes electronic claim status request and response | FFS Claims and Adjudication | Process Claims | N/A |

| | | | | |
|---|---|---|---|---|
| | transactions (ASC X12N 276/277) required by 45 CFR Part 162. | | | |
| CM.CM7.3 | SMA receives, stores, and transmits data for external independent reviews for quality and timeliness of care, health outcomes and access to services. | Care Management | | - |
| CM.CL7.3 | The system supports receiving, processing and sending electronic health care service review, request for review, and response transactions required by 45 CFR part 162, as follows:<br><br>• retail pharmacy drug referral certification and authorization<br><br>• dental, professional and institutional referral certification and authorization (ASC X12N 278) optionally, supports web or internet submissions or prior authorization requests. | FFS Claims and Adjudication | CM07 Authorize Referral | N/A |
| IA.DMS.5 | The system refreshes or replaces all historical claim data, recipient enrollment, provider enrollment, and other primary reference data on a scheduled basis. | Information Architecture | IA Component Name: Data Management Strategy (DMS) | This criterion does not apply to E&E. For R1, evidence could include acquisition documents, requirements, a ConOps that explains how this will be implemented, service level agreements (SLAs), or other planning documents that |

| | | | | |
|---|---|---|---|---|
| | | | | demonstrate plans to adopt statewide standards. For R2 and R3, evidence could be a log of actual updates and SLAs. For R3, evidence should show that the SLAs have been enforced back to go-live. For R2 (if not a desk review) and R3, the state should be prepared to demonstrate this capability. Enterprise: All modules update primary reference data regularly. Module: The module demonstrates that it supports regular data updates. |
| IA.DS.1 | The system of interest supports system transmission and receipt of all current version x12N and NCPDP eligibility verification transactions. | Information Architecture | IA Component Name: Data Standards (DS) | This criterion does not apply to E&E. This criterion applies to modules that generate or transform data related to x12N or NCPDP eligibility verification transactions. For R1, evidence could include acquisition documents, requirements, a ConOps that explains how this will be implemented, or other planning documents that demonstrate plans to implement this functionality. For R2 and R3, evidence could include screenshots showing transmission and receipt of these types of verification transactions. For R3, evidence should demonstrate functionality back to go-live. For R2 (if not a desk review) and R3, the state should be prepared to demonstrate |

| | | | | |
|---|---|---|---|---|
| | | | | and discuss these transactions. |
| IA.DS.10 | The system of interest, at a minimum, supports transfer of data from MMIS and to other entities (e.g., claims history, recipient enrollment, provider enrollment, and primary reference data information (e.g. diagnosis, procedure, national drug code [NDC], and pricing). | Information Architecture | IA Component Name: Data Standards (DS) | This criterion does not apply to E&E. For R1, evidence could include acquisition documents, requirements, a ConOps that explains how this will be implemented, or other planning documents that demonstrate plans to operationalize this functionality. For R2 and R3, evidence could include screenshots showing transfer of the data types listed in the criteria. Screenshots should show transfer between MMIS and entities shown on the state's context diagram. For R3, evidence should show this functionality operational at go-live. For R2 (if not a desk review) and R3, the state should be prepared to demonstrate and discuss these transfers. Modules: Applies to modules involved in any aspect of transferring data to other entities. |
| IA.DS.11 | The system of interest supports consumption of data in multiple formats from many sources, such as vital statistics, MCO encounter data, benefit manager encounter data (pharmacy, dental, mental health), waiver program data, and census bureau. | Information Architecture | IA Component Name: Data Standards (DS) | This criterion does not apply to E&E. Enterprise: For R1, evidence could include acquisition documents, requirements, a ConOps that explains how this will be implemented, or other planning documents that demonstrate plans to operationalize this functionality. For R2 and R3, evidence could include screenshots showing incorporation of data that |

| | | | | |
|---|---|---|---|---|
| | | | | use various formats. Screenshots should show pharmacy, dental, encounter data, etc. For R3, evidence should show this functionality operational at go-live. For R2 (if not a desk review) and R3, the state should be prepared to demonstrate and discuss receipt of these data. Modules: Evidence could include test reports and screenshots showing that the module(s) accepts data in multiple formats from various sources, relevant to the scope of the module's intended functionality. |
| IA.DS.15 | The system of interest interfaces with the National Plan and Provider Enumerator System (NPPES) to verify the NPI of provider applicants. | Information Architecture | IA Component Name: Data Standards (DS) | This criterion does not apply to E&E. For R1, evidence could include acquisition documents, requirements, a ConOps that explains how this will be implemented, or other planning documents that demonstrate plans to interface with the NPPES . For R2 and R3, evidence could include a context diagram and description showing how the module interacts with the NPPES, along with example transactions, if applicable. This criterion applies to modules that should interface with the NPPES. |
| IA.DS.5 | The system of interest supports the sending and receiving of electronic claims transactions, containing valid | Information Architecture | IA Component Name: Data Standards (DS) | This criterion does not apply to E&E. Enterprise: The MMIS is able to send and receive NCPDP and X12N 837D transactions across the relevant modules. Modules: This |

| | | | | |
|---|---|---|---|---|
| | codes, required by 45 CFR Parts 160 and 162, as follows:<br><br>• Retail pharmacy drug claims (NCPDP)<br><br>• Dental health care claims (X12N 837D) | | | criterion applies only to modules that support send/receive functionality for NCPDP and X12N 837D claims transactions. For R1, evidence could include acquisition documents, requirements, a ConOps, or other planning documents that demonstrate intent to implement this functionality. For R2 and R3, evidence could include screenshots showing the successful import of data from a pharmacy drug claim and from a dental health claim along with example transactions sent from the module(s). For R3, evidence should show compliance back to go-live. For R2 (if not a desk review) and R3, the state should be prepared to give a demonstration. |
| IA.DS.6 | The system of interest provides secure, HIPAA-compliant software and documentation for use by providers to submit electronic claims. | Information Architecture | IA Component Name: Data Standards (DS) | This criterion does not apply to E&E. Enterprise and modules: Comply with all HIPAA regulations. Modules that provide interfaces to providers or receive information from them must demonstrate that the modules are secure and HIPAA compliant. For R1, evidence could include acquisition documents, requirements, ConOps, or other planning documents that demonstrate intent to implement HIPAA requirements. For R2 and R3, evidence should show screenshots or other documentation showing |

| | | | | |
|---|---|---|---|---|
| | | | | successful submission of electronic transmission of all claim types. For R3, the evidence should show functionality back to go-live. For R2 (if not a desk review) and R3, the state should be prepared to give a demonstration and discuss. |
| IA.DS.9 | The system of interest complies with the SMA's standardized structure and vocabulary data for automated electronic intrastate interchanges and interoperability. | Information Architecture | IA Component Name: Data Standards (DS) | Enterprise: Has standardized structure and vocabulary data standards. Show how they are being used by the modules. Module: Show use of the SMA 's documented standards for interoperability. For R1, evidence could be state's interoperability standards in the ConOps or other planning documentation. For R2 and R3, evidence can include test reports showing that system/module uses the state's defined interoperability standards. |
| CM.R1.14 | The system has regularly scheduled data exchanges (including Medicaid children records) with statewide automated immunization registry and regularly sends information to a statewide immunization registry through the interface:<br><br>• Medicaid identifier<br>• Demographic information<br>• Current Procedural | Registries | CM04 Manage Registry | N/A |

| | | | | |
|---|---|---|---|---|
| | Terminology (CPT)/billing procedure code<br>• Identify rendering service provider<br>• Reminder/recall notice dates.<br>• Medicaid claims for children receiving immunizations. | | | |
| CM.R6.1 | If a separate state wide registry exists, SMA exchanges data with this registry on at least a weekly basis. | Registries | CM04 Manage Registry | N/A |
| CM.R6.2 | To the extent possible, provides for interfaces with other systems within the State, such as:<br>a. Child Welfare (SACWIS)<br>b. Women, Infants and Children (WIC)<br>c. Early Periodic Screening, Diagnosis and Treatment (EPSDT) Program<br>d. Bureau of Vital and Health Statistics<br>e. Children's Health Insurance Program (S-CHIP)<br>f. Public Health Clinics<br>g. Health Information Systems (HIS)<br>h. Vaccine Management System (VACMAN) (CDC)<br>i. Other. | Registries | CM04 Manage Registry | N/A |
| CM.R7.3 | The system selects and sends data to the registry at least on a weekly basis. | Registries | CM04 Manage Registry | N/A |

| | | | | |
|---|---|---|---|---|
| S&C.IC.3 | The system conforms to ASC X12 Technical Reports Type 3 (TR3), Version 005010 is mandated by 1/1/2012. | Information Architecture | S&C: Interoperability Condition | For R1, evidence could include acquisition documents, a ConOps, test plans, or other planning documents that demonstrate plans to incorporate this capability. For R2 and R3, evidence can include transaction data. Module: This only applies to modules that are related to TR3 types—they must support ASC X12. For modules interfacing with the Federal Data Services Hub (FDSH), X12 use is satisfied through adherence to the FDSH BSDs. |
| S&C.IC.4 | The system uses the Clinical Modification (ICD–10 CM) for diagnosis coding (including the Official ICD–10 CM Guidelines for Coding and Reporting), and, the Procedure Coding System (ICD–10 PCS) for inpatient hospital procedure coding (including the Official ICD–10 PCS Guidelines for Coding and Reporting). | Standards and Conditions | S&C: Interoperability Condition | HIPAA-covered entities were authorized to process and adjudicate claims using ICD-9 code sets up to and including 9/30/2015. On 10/1/2015, HIPAA-covered entities are authorized to process and adjudicate claims using the ICD-10 code set. This criterion does not apply to E&E. For R1, evidence could include acquisition documents, requirements, or a ConOps that prove the plan to use ICD-10. For R2 and R3, evidence could include screenshots that show the use of ICD-10 along with test reports and demonstration of its use and the ability to access old claims that use ICD-9. For R3, evidence should demonstrate ICD-10 usage back to either go-live or to 9/30/2015. For R2 (if not a desk review) and R3, the state should |

| | | | | |
|---|---|---|---|---|
| | | | | be prepared to discuss. Module: For modules that use ICD codes, the module can support the import of legacy (ICD-9) data by using an ICD-9/ICD 10 mapping function provided by the state. |
| S&C.IC.6 | The architecture adopted preserves the ability to efficiently, effectively, and appropriately exchange data with other participants in the health and human services enterprise. | Standards and Conditions | S&C: Interoperability Condition | This criterion speaks to integration with programs like SNAP, TANF, etc. Enterprise: The state should have an architecture that supports this capability. Module: This applies only to modules involved in data exchange with human services systems. These should be able to support the state's data exchange goals. For R1, evidence should include a high-level system context diagram that shows the system as a whole, illustrating input and output interfaces from/to external systems. Where possible, these interfaces should be accompanied by high-level data content descriptions. For R2 and R3, evidence could include screenshots that demonstrate successful data exchange between the module and key external systems. For R2 (if not a desk review) and R3, the state should be prepared to demonstrate and discuss the data exchange between other state health and human services enterprises. |

| | | | | |
|---|---|---|---|---|
| S&C.ISC.6 | The system of interest complies with standards and protocols adopted by the Secretary under sections 1104 and 1561 of the Affordable Care Act. | Standards and Conditions | S&C: Industry Standards Condition | This criterion speaks to health information enrollment standards and protocols to promote the interoperability of systems for the enrollment of individuals in federal and state health and human services programs as well as the adoption of uniform standards and operating rules for the electronic transactions that occur between providers and health plans that are governed under HIPAA. Establishes a process to regularly update the standards and operating rules for electronic transactions and requires health plans to either certify compliance or face financial penalties. The goal of this section is to make the health system more efficient by reducing the clerical burden on providers, patients, and health plans. For R1, evidence could include acquisition documents, requirements, or a ConOps that explains how the state plans to adopt standards. For R2 and R3, evidence could include test reports of successful data exchange between modules and/or external systems. **Enterprise:** The state should have an architecture that supports this capability. **Module:** This applies only to modules involved in data exchange with human services systems. These |

| | | | | |
|---|---|---|---|---|
| | | | | should be able to support the state's data exchange goals. |
| S&C.MS.2 | Open standards between key interfaces have been considered for all and chosen where feasible. | Standards and Conditions | S&C: Modularity Standard | Evidence could include acquisition documents and designs that stipulate the use of open standards for interfaces (R1), detailed designs that include interoperability standards adopted by the state and test reports showing successful integration between modules (R2, R3). For R2 (if not a desk review) and R3, the state should be prepared to demonstrate and discuss the open standards and interfaces. **Enterprise:** During acquisition planning the state needs to ensure that the modules that it acquires will interface properly with each other by using open interfaces and not proprietary ones. **Module:** Show that the module uses the open standards adopted by the state. |
| TA.CM.4 | The system of interest uses technology-neutral interfaces that localize and minimize impact of new technology insertion. | Integration and Utility | Technical Service Classification: Configuration Management | This criterion addresses the use of modern principles and protocols implemented through open web services, APIs, or batch type interfaces. For R1, evidence could include acquisition documents, requirements, a ConOps that explains how this will be implemented, or other planning documents that demonstrate plans to incorporate this capability. For R2 (if not a desk review) and R3, evidence |

| | | | | |
|---|---|---|---|---|
| | | | | could include test reports regarding the open web services or APIs. For R2 and R3, the state should be prepared to give a demonstration of this capability. Module: Demonstrate the use of APIs or other minimally impactful interfaces. |
| TA.PM.5 | The system of interest's transactions execute in a reasonable amount of time. | Access and Delivery | Technical Service Classification: Performance Measurement | This criterion speaks to the need to conduct good capacity management practices. The state and its contractors should anticipate capacity needs and design and manage to meet current and future needs. Evidence can include plans to perform capacity management processes (R1) and performance testing and capacity monitoring reports (R2, R3). For R2 (if not a desk review) and R3, the state should be prepared to discuss. Enterprise: The state has defined acceptable transaction times for various transaction types, understands and documents which modules are involved in which transactions, defines performance requirements and determines capacity needs against those requirements, acquires necessary capacity, monitors system performance, and periodically plans capacity modifications according to future needs. |

| | | | | |
|---|---|---|---|---|
| TA.SOA.4 | The SMA conducts system coordination between intrastate agencies and some external entities. | Intermediary and Interface | Technical Service Classification: Service Oriented Architecture | This criterion means that the system interfaces or integrates with at least some external or intrastate agencies. For R1, evidence could include a list of external agencies the system coordinates and by what methods in the ConOps and ICD documents. For R2 and R3, evidence could include meeting minutes or change control board documents showing how the state coordinates between interstate or external agencies. For R3, this evidence should date back to go-live. For R2 (if not a desk review) and R3, the state should be prepared to discuss. Enterprise: State should ensure that stakeholder and technical coordination is happening across all relevant modules and the external entities. Module: **Applies only to modules that interface with external/intrastate entities.** |
| TA.SP.12 | The SMA adopts CAQH CORE Phase I, II and III as stipulated in 45 CFR 162 (Operating Rules for HIPAA Transactions) | Information Architecture | Technical Service Classification: Security and Privacy | This criterion does not apply to E&E. Enterprise: Ensure that this criterion applies across all relevant modules. Modules: Applies to modules that perform HIPAA transactions. For R1, evidence could include state policy, acquisition documents, a ConOps, test plans, or other planning documents that demonstrate plans to incorporate this capability. |

| | | | | |
|---|---|---|---|---|
| | | | | For R2 and R3, evidence should include screenshots showing the elements of compliance to CAQH CORE requirements. For R3, the evidence should show compliance back to go-live. For R2 (if not a desk review) and R3, the state should be prepared to demonstrate this functionality. |
| TA.SP.16 | The system of interest supports ANSI X12N 820 Premium Payment transaction as required by HIPAA. | Information Architecture | Technical Service Classification: Security and Privacy | This criterion does not apply to E&E. Enterprise: Ensure that this criterion applies across all relevant modules. Modules: Applies to modules that perform X12N 820 transactions. For R1, evidence could include state policy, acquisition documents, a ConOps, test plans, or other planning documents that demonstrate plans to incorporate this capability. For R2 and R3, evidence should include screenshots showing the elements of compliance to CAQH CORE requirements. For R3, the evidence should show compliance back to go-live. For R2 (if not a desk review) and R3, the state should be prepared to demonstrate this functionality. |
| TA.SP.17 | The system of interest supports all ANSI X12N transactions as required by HIPAA. | Information Architecture | Technical Service Classification: Security and Privacy | This criterion does not apply to E&E. For R1, evidence could include state policy, acquisition documents, a ConOps, test plans, or other planning documents that demonstrate plans to incorporate this capability. |

| | | | | |
|---|---|---|---|---|
| | | | | For R2 and R3, evidence should include screenshots showing ANSI X12N transactions. For R3, the evidence should show compliance back to go-live. For R2 (if not a desk review) and R3, the state should be prepared to demonstrate this functionality. Enterprise: Ensure that this criterion applies across all relevant modules. Modules: Applies to modules that perform X12N transactions. |
| TA.SP.72 | Sensitive data in transit that requires confidentiality protection are encrypted when traversing entity boundaries. For data in transit where the only concern is the protection of integrity, hashing techniques and message authentication codes are used instead of encryption.* | Access and Delivery | Technical Service Classification: Security and Privacy | For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. For R1, evidence could include acquisition documents, technical controls documentation, a ConOps, or other documents that demonstrate intention to use FIPS 140-2 validated or compliant encryption technology across system boundaries. For R2 and R3, evidence could include (1) screenshots of the encryption technology being used and (2) a diagram showing interfaces with external systems/modules and where excrypted data is being transmitted/received across those boundaries. For R3, evidence should show that an approved encryption algorithm has been used since go-live. |

| | | | | |
|---|---|---|---|---|
| | | | | For R2 (if not a desk review) and R3, the state should be prepared to discuss its encryption and hashing use. Enterprise: The state must ensure that its business partners and downstream entities are complying with the state's policies in a consistent and effective manner. The state should provide audit reports to that effect. Module: This applies to modules that process, store, manage, disclose, and use ePHI/PII. |
| TA.DAM.2 | The system of interest conducts information exchange (internally and externally) using MITA Framework, industry standards, and other nationally recognized standards. | Integration and Utility | Technical Service Classification: Data Access & Management | For R1, evidence could include a statement in the ConOps as to which standards the state will use. For R2 and R3, evidence could include screenshots and test reports of successful information exchange using the standards. For R3, the evidence should show **compliance back to go-live.** For R2 (if not a desk review) and R3, the state should be prepared to give a demonstration. State and modules: Evidence should show how the solution uses nationally recognized standards adopted by the state. |
| TA.DAM.3 | The system of interest develops data models that include mapping of information exchange with external organizations. | Integration and Utility | Technical Service Classification: Data Access & Management | For R1, evidence should include a high-level system context diagram that shows the system as a whole, illustrating input and output interfaces from/to external systems. Where possible, these interfaces should be |

| | | | | |
|---|---|---|---|---|
| | | | | accompanied by high-level data content descriptions. For R2 and R3, evidence should include **copies of data models**. For R2 (if not a desk review) and R3, the state should be prepared to **discuss the data models, what data is exchanged with what external systems, and how that data is managed.** Enterprise: The state's data models cover MMIS / E&E enterprise. Modules: The module has identified **which data can be shared externally and enables the sharing of that data**. |
| TA.DC.9 | The system of interest uses standards (e.g. XML or JSON in a RESTful environment) for message format to ensure interoperability. | Intermediary and Interface | Technical Service Classification: Data Connectivity | This criterion applies across the enterprise and for individual modules. For R1, evidence could include acquisition documents, requirements, a ConOps that explains how this will be implemented, or other planning documents that demonstrate plans to incorporate this capability. For R2 and R3, evidence could include samples of messaging (XML or JSON in a RESTful environment). For R3, the evidence should show functionality at go-live. For R2 (if not a desk review) and R3, the state should be prepared to demonstrate this capability. |
| TA.DC.10 | The system of interest securely conducts electronic information exchange within the agency and with | Intermediary and Interface | Technical Service Classification: Data Connectivity | For R1, evidence could include acquisition documents, requirements, a ConOps that explains how this will be implemented, or other |

| | | | | |
|---|---|---|---|---|
| | multiple intrastate agencies via an information hub. | | | planning documents that demonstrate plans to incorporate this capability. For R2 and R3, evidence could include screenshots showing successful exchange of data with an information hub. For R2 (if not a desk review) and R3, the state should be prepared to give a demonstration of this capability and describe the maturity of the security involved. Enterprise: The state should ensure modules and other state systems are exchanging information properly. Module: Should have capability to send/receive data through the enterprise from other state systems. |
| TA.SE.3 | The system of interest documents all interfaces in an Interface Control Document (ICD), along with how those interfaces are maintained. | Intermediary and Interface | Technical Service Classification: System Extensibility | Evidence should include a ConOps, ICD, or System Design Document (R1, R2, R3). For R2 (if not a desk review) and R3, the state should be prepared to discuss how the interfaces are maintained. Enterprise: The state should ensure that all system interfaces between modules with external entities are defined and maintained. Module: Define capabilities for interfacing with other modules or external entities, identify what modules/capabilities it should interface with, and how it will do so. |
| TA.SOA.2 | The system of interest conducts reliable messaging, | Intermediary and Interface | Technical Service Classification: | For R1, evidence could include acquisition documents, requirements, |

| | | | | |
|---|---|---|---|---|
| | including guaranteed message delivery (without duplicates) and support for non-deliverable messages. | | Service Oriented Architecture | a ConOps that explains how this will be implemented, or other planning documents that demonstrate plans to incorporate this capability. For R2 and R3, evidence could include enterprise system diagrams like those found in a System Design Document that explain how the state guarantees message delivery. For R3, the evidence should show compliance back to go-live. For R2 (if not a desk review) and R3, the state should be prepared to demonstrate this capability. Module: This criterion applies to any modules responsible for messaging. |
| TA.SE.2 | The system of interest uses RESTful and/or SOAP-based web services for seamless coordination and integration with other U.S. Department of Health & Human Services (HHS) applications and intrastate agencies, including the Health Insurance Exchange (HIX). | Intermediary and Interface | Technical Service Classification: System Extensibility | For R1, evidence could include acquisition documents, requirements, a ConOps that explains how this will be implemented, or other planning documents that demonstrate plans to incorporate this capability. For R2 and R3, evidence could include enterprise system diagrams like those found in a System Design Document that explain how integration with the other systems are achieved. For R2 (if not a desk review) and R3, the state should be prepared to discuss. Module: This criterion applies to modules that must integrate with the Department of Health and |

| | | | | |
|---|---|---|---|---|
| | | | | Human Services and intrastate agencies. |

**Critical Success Factors**

The table below provides the Programmatic Critical Success Factors:

Table 8: CSFs

| Checklist ID | Requirement Text / System Review Criteria (SRC) | MITA Business Area Module Checklist Set | Business Process | CMS Guidance |
|---|---|---|---|---|
| N/A | N/A | N/A | N/A | N/A |