



# **State of Tennessee**

**Division of Health Care Finance and Administration**

## **Tennessee Technical Advisory Services (TN TAS)**

### **Interface / Integration Management Plan**

Version: 1.0

Submitted Date: March 31, 2016

## TABLE OF CONTENTS

<b>1. Executive Summary .....</b>	<b>6</b>
<b>2. Introduction.....</b>	<b>8</b>
2.1. Purpose .....	8
2.2. Objective.....	8
2.3. Scope.....	9
2.4. Assumptions, Risks, and Constraints.....	9
2.5. Referenced Documents.....	10
<b>3. Interface/Integration Management Plan Vision .....</b>	<b>12</b>
3.1. Vision and Concept Overview .....	12
3.2. Interface/Integration Management Master Plan .....	13
3.3. Integration Strategy .....	13
3.4. Interface Release Plan .....	18
3.5. Interface Management Life Cycle.....	18
<b>4. Governance.....</b>	<b>20</b>
4.1. Governance Bodies .....	20
4.2. Integration Principles .....	21
4.3. Interoperability Standards .....	22
4.4. Integration Patterns .....	22
<b>5. Interface/Integration Framework and Methodology.....</b>	<b>24</b>
5.1. Identify Phase.....	24
5.2. Define Phase .....	25
5.3. Design Phase .....	28
5.4. Implementation Phase.....	31
5.5. Operate and Maintain Phase.....	31
5.6. Decommission Phase.....	32
<b>6. Operational Interface/Integration Plan Management.....</b>	<b>33</b>
6.1. Change Management.....	33
6.2. Communication Management .....	33
6.3. Roles and Responsibilities .....	34
6.4. Additional Roles for Consideration .....	39
<b>Appendix A: Definitions, Acronyms and Abbreviations.....</b>	<b>41</b>

**Appendix B: SDLC RACI Chart Role Definition ..... 45**

**Appendix C: Framework Specification ..... 47**

    Appendix C.1: Data Sharing Agreement Document..... 48

    Appendix C.2: Business Impact Analysis Document ..... 55

    Appendix C.3: Interface Control Document..... 61

**Appendix D: Interface/Integration Acceptance Criteria and Metrics ..... 79**

## TABLE OF FIGURES

Figure 1: Interface/Integration Management Context .....	13
Figure 2: Integration Strategy Components .....	14
Figure 3: Management of Interfaces during their life cycle in a System Landscape © 2011 IEEE .....	19
<i>Figure 4: TEDS Interface Management Life Cycle</i> .....	19
Figure 5: EDI Trading Partner Request Flow .....	23
Figure 6: Interface Management Life Cycle Alignment to the MMP SDLC .....	24

## TABLE OF TABLES

Table 1: Referenced Documents .....	10
Table 2: Integration Approach for MMP .....	15
Table 3: Interface Life Cycle Roles and Responsibilities .....	34
Table 4: Definitions, Acronyms and Abbreviations .....	41
Table 5: RACI Participants Definition .....	45

# 1. Executive Summary

This Management Plan is to be used as a guide by the SI Contractor for developing an Interface/Integration Management Master Plan for each project within the Medicaid Modernization Program (MMP), most currently, the Tennessee Eligibility Determination System (TEDS). As such, this document will provide a framework for the management of interface/integration activities for the Eligibility Modernization Project (EMP) throughout the Life Cycle of an Interface.

The Interface/Integration Management Master Plan will outline and describe the general integration strategy, approaches, and standards established for the project. These guidelines are to then be applied to each individual interface that is to be implemented and/or managed. While this plan will be created at the project level, it is expected that each interface being implemented by the EMP will be specified and planned for as part of an Interface Release Plan that is aligned to the overarching Release Strategy of the project.

This document will outline the framework, methodology, operational enablement, and governance mechanisms required for the management of interfaces/integration for MMP projects, specifically EMP.

## **Interface/Integration Management Plan Vision**

The Interface/Integration Management Master Plan must be developed by the SI Contractor for the integration of TEDS with other systems within Health Care Finance and Administration (HCFA), other State Agencies, and the Federal Data Hub.

This plan should clearly articulate the integration strategy, target integration architecture, and integration roadmap for EMP. The integration strategy will include the approach, principles, and standards that the project should align and adhere to in the design and deployment of an interface.

An Interface Release Plan for each release of the project will also be defined by the SI Contractor as an update to the Interface/Integration Master Plan.

## **Framework and Methodology**

The framework and methodology for the management of interfaces has been established and defined in alignment with both the Interface Management Life cycle and MMP System Development Life Cycle (SDLC).

In order to manage an interface release, the methodology has been broken down into seven critical phases. Starting with the Identify Phase of the Life Cycle where interface/integration needs are identified for the project. Each subsequent phase builds upon these needs and priorities. Associated artifacts must be defined by the SI Contractor within the Interface/Integration Master Plan, each interface within this master plan must also be defined as part of the Interface Release Plan and associated Test Management Plan.

Critical components of the SDLC and key artifacts for each phase have been identified such as a Data Sharing Agreement, Business Impact Analysis, and Interface Control Document.

It is important to note that while the above mentioned artifacts are specific to the interfaces being designed and deployed, there are additional project deliverables that will need to be further enhanced/appended with interface/integration specific content throughout the Interface Life Cycle.

### **Operational Interface/Integration Management**

For the operational management of the Interface/Integration Life Cycle, key roles, responsibilities, and capabilities must be put into place.

A change management process will assist in the management of any interface/integration changes that take place both during and after implementation. The SI Contractor must ensure their process is aligned to the overarching EMP change management capability. Additionally, the Communication Management Plan developed for EMP should include the required coordination and communication activities related to interface/integration. Both these capabilities are required to ensure the successful implementation, operation and maintenance of the interface/integration requirements.

For the effective management of all interface/integration related activities, tasks, and key roles should be in place as detailed in this document and additional roles as detailed within the Request for Qualifications for System Integration (SI) Services RFQ # 32101-15557.

### **Governance**

In order to successfully manage an interface throughout its life cycle, governance will play a critical role in establishing and enforcing rules, regulations, standards, and guidance that the project must align to.

The Program Governance Management Plan (PGMP) defines the process for approving and enforcing standards, and the Interface/Integration Management Master Plan will identify standards that the project and each interface being designed and deployed must align/adhere to.

Governance bodies that are in place to support and enable the management of interface/integration activities include but, may not be limited to the Project Program Steering Committee, Technical Architecture Review Board, and the Information System Security Council.

## 2. Introduction

This document is intended to be used by MMP projects as a guide for the development of project level Interface/Integration Management Master Plans and subsequent Interface Release Plans. The Interface/Integration standards, frameworks, and methodologies included in this document are to be used by the SI Contractor in the development of the above mentioned plans which are described in detail throughout this document.

The standards used to define the content of this document are based on Centers for Medicare and Medicaid Services (CMS) guidance, Institute of Electrical and Electronics Engineers (IEEE) frameworks, and available HCFA standards and principles.

If an MMP contractor proposes an alternate approach for a project than what is presented in this Management Plan, that approach must satisfy the requirements of this plan, and the contractor must provide justification for the proposed approach as well as demonstrate how the requirements are satisfied.

### 2.1. Purpose

The purpose of this Management Plan is to define a framework for the Interface/Integration Life Cycle that will support the formation of an Interface/Integration Management Master Plan for the project.

Based on the Interface/Integration Management Master Plan, it is expected that each interface being implemented by EMP will be specified as part of an Interface Release Plan that is aligned with the overarching Release Strategy for the project.

More specifically, this document will contain specifications for a project to establish a data sharing agreement with each Interface Partner, perform a business impact analysis, and to design and manage a release of an interface throughout the Interface Life Cycle.

The guidance in this document will include frameworks and methodologies that ensure that the interface/integration approach represents industry leading practices, is appropriate for the project, and aligns to existing State standards and applicable federal regulations/requirements. This plan will also describe the type of metrics and acceptance criteria that are to be defined for all interfaces.

### 2.2. Objective

The guidance in this Management Plan will help ensure that the right activities are performed and managed effectively for each MMP Project at both the project and release level.

## 2.3. Scope

### **In Scope**

This Management Plan shall specify an interface/integration framework for EMP in the form of an Interface/Integration Management Master Plan. This Management Plan will define and establish a framework and approach for Interface/Integration planning, analysis, design, testing and deployment.

The intention is that this Management Plan will enable the development of project specific Interface/Integration Management Master Plans in alignment with the Centers for Medicare and Medicaid Services Enterprise Life Cycle (CMS-ELC). More specifically, the scope of this Management Plan will include specifications for the following:

- A Business Impact Analysis to ensure that the selected interface/integration approach and enabling technology that is selected and/or designed achieves the following:
  - Meets the needs of the projects.
  - Aligns to existing State standards.
  - Aligns to applicable federal regulations/requirements.
  - Follows industry leading practices.
- Integration process design framework detailing industry standard Interface/Integration process elements including an enterprise approach and standards for all project Interface/Integration design, testing and deployment.
- A Data Sharing Agreement detailing the terms and conditions of the exchange of data (e.g., type of data, primary and secondary use of data, level of security, privacy requirements, data owner, etc.) between HFCA and Interface Partners where system integration is required.
- Metrics and acceptance criteria that are to be identified for each project's Interface/Integration Management Master Plan.
- Roles and responsibilities for interface/integration management.

Additionally, this document will incorporate lessons learned from previous projects and identify critical success factors based on previous experiences.

## 2.4. Assumptions, Risks, and Constraints

### **Assumptions**

- The life cycle and standard presented in this document assumes that development is based on a waterfall or iterative software development methodology and would need to be updated if an Agile or other software development methodology is used.

**Risks**

- Stakeholders and Interface Partners may be engaged within MMP with different interface/integration management methodologies and approaches. As such there may be a realignment required on these methodologies and approaches when these new stakeholders and Interface Partners are engaged in order to have a consistent interface/integration approach.

**Constraints**

- Schedule, resource and budgetary constraints may impact the management of interface/integration activities and should be addressed at the onset of the project.
- Communication constraints may exist between the SI Contractor, State Agencies, Federal Agencies, IV&V, Interface Partners, and Contractors.
- Other project priorities may exist between the SI Contractor and Interface Partners in other State Agencies.

**2.5. Referenced Documents**

The Interface/Integration Management Plan is interrelated with other deliverable as illustrated in the table below. These deliverables have been considered in the design of the Interface / Integration Management Plan and will continue to be aligned to these and other relevant MMP management plans in future iterations.

Table 1: Referenced Documents

#	Document Name	Content Overview
1	Enterprise Architecture – Business Operating Model (EA -BOM) Management Plan	Requirements, templates, tools and repositories for interface/integration
2	Communication Management Plan	Defines how communication will be managed at the project level. This Management Plan has not yet been defined.
3	Project and SDLC Management Plan	Gates and gating requirements pertaining to interface/integration
4	Requirements Management Plan	Defines how integration requirements will be managed
5	Change Management Plan	Defines how changes will be managed. This Management Plan has not yet been defined

#	Document Name	Content Overview
6	Test Management Plan	Testing approach and requirements for interface/integration
7	Program Governance Management Plan	Governance framework applicable to interface/integration management
8	Request for Qualifications for Systems Integration (SI) Services (RFQ # 32101-15557)	RFQ defining the State's requirements for an SI Contractor to develop, operate and maintain the Tennessee Eligibility Determination System (TEDS).

## 3. Interface/Integration Management Plan Vision

This section describes the approach for defining the interface/integration framework for addressing the integration needs of the State while leveraging integration concepts and methodologies based on industry leading practices.

### 3.1. Vision and Concept Overview

Like any large transformation, EMP requires extensive and complex changes that are difficult to manage and control. This includes the activities required to establish and support critical system interfaces between TEDS and other HCFA systems, other State Agencies, the Federal Government, and other Interface Partners.

To successfully manage the Integration/Interface requirements, strategies and plans need to be put in place to coordinate the identification and implementation of these requirements, while effectively managing Interface Partners and aligning to overarching HCFA and MMP standards for integration.

An Interface Management Master Plan will be informed by an integration strategy and should be defined at a project level for EMP. An EMP integration strategy will identify integration approaches and associated principles, standards and patterns that should be applied and adhered to.

An Interface Release Plan will be created in alignment to the projects release strategy for each interface to be implemented by EMP. This plan must align to the overall project level Interface/Integration Management Master Plan.

Within the MMP SDLC framework as described in the Project and SDLC Management Plan, key activities and deliverables are required for interface/integration management and will be delivered through the Interface/Integration Framework and Methodology. The following figure illustrates the concept of the Interface/Integration Framework and Methodology in the context of the MMP SDLC.

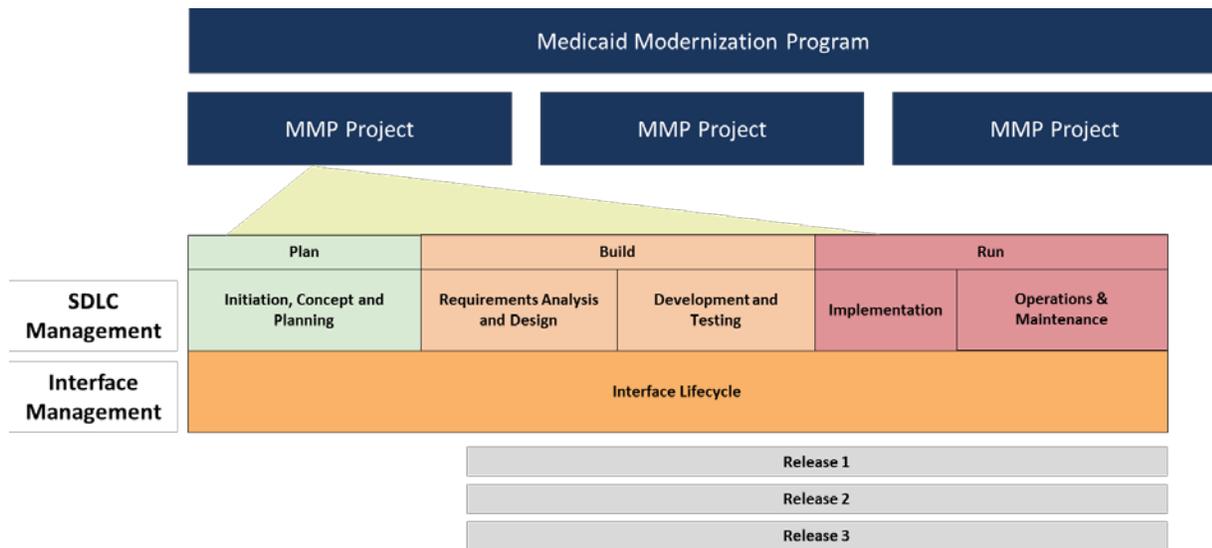


Figure 1: Interface/Integration Management Context

As described above, interface management is executed in alignment to the MMP SDLC, and the Interface Life Cycle commences prior to the SI Contractor being on boarded and continues throughout through the Life Cycle of the project. As described earlier, interfaces are deployed in releases, aligned with the projects release strategy.

### 3.2. Interface/Integration Management Master Plan

In order to successfully manage integration and interface requirements for EMP, strategies and plans must to be put into place to coordinate the development and implementation of the identified interfaces while effectively managing Interface Partners and aligning to the overarching HCFA vision and standards.

As such, the intent of the Interface/Integration Management Master Plan is to outline and describe the general integration strategy, approaches and standards established for the project. These guidelines are to apply to the interfaces that will be implemented and/or managed by the SI Contractor.

This plan is to be defined by the SI Contractor in the early phases of onboarding and must leverage any upfront design work conducted by the TAS Contractor and the State.

### 3.3. Integration Strategy

In defining the Interface Management Master Plan, it is important to establish an integration strategy for EMP that aligns to the State’s vision for both HCFA and MMP in specific.

This strategy will be used to establish project level integration requirements, guide the system architecture design of a solution, and overall management of interfaces through its life cycle.

The Integration Strategy should articulate the high level plan for the system integration required for EMP and should include the following components as described in the following figure.

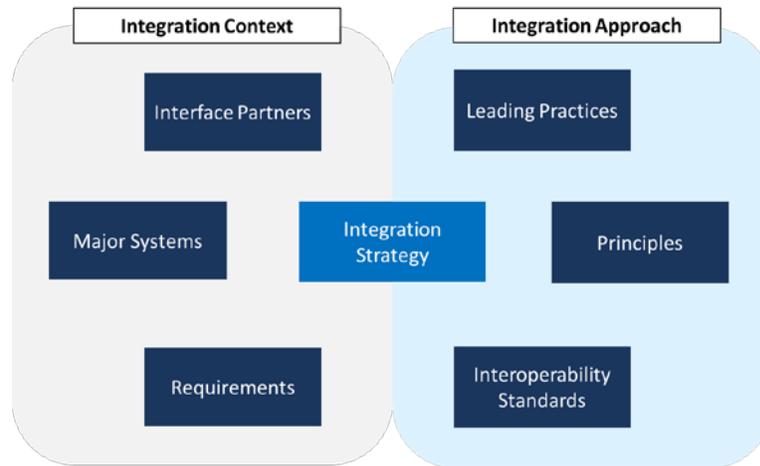


Figure 2: Integration Strategy Components

The following sections will describe the Integration Context and Integration Approach elements of the Integration Strategy in more detail.

Additional components of the strategy that help establish the integration approach to be used include **integration principles, standards and patterns**. These are to be used when designing and implementing integration components and interfaces. This includes application, data, and security principles and standards that must be adhered to.

Enterprise Architecture also plays a key role in the definition of an integration strategy. Particularly in the development of the **conceptual target state integration architecture** that needs to be in place to meet integration requirements. This target state architecture should align to an integration strategy, integration principles and standards set for HCFA and MMP.

These components will be described in the Methodology and Governance sections of this document.

### Integration Context

A major component of this strategy includes identifying the context of the integration. More specifically, an integration strategy should specify the Interface Partners involved, major systems (internal and external) and high level requirements for data exchange and/or access to services.

Interface Partners refer to all parties involved in the integration of two systems. This includes the system owners and those accountable for managing, implementing and maintaining the interfaces.

An understanding of data sharing requirements (e.g., data standards, communication protocols, security and privacy controls) specific to each Interface Partner involved in the integration is included as part of the context of the integration.

**Integration Approach**

An integration strategy will provide direction on the integration approach to be implemented based on an overarching Enterprise and HCFA specific integration strategy (if available). The integration approach is also based on leading practices as applied to automated batch file transfers, automated electronic data interchange (EDI), message oriented integration, and service oriented architecture (SOA).

The integration approach should always consider leveraging existing or similar technologies in an effort to streamline operations, simplify support requirements and reduce variability. It should always consider the complete identification, acknowledgment, reconciliation and reporting of any/all transactions between systems.

Common approaches used in industry include, but are not limited to the following:

- **Automated Batch File Transfers:** Batch file transfer is an integration approach that has been present for decades and essentially extracts data from a system or application and gathers it into a “batch” file. This batch file is sent in a point-to-point fashion from one system to another, typically with a proxy (FTP/SFTP) server acting as an intermediary.
- **Message Oriented Integration:** In simple terms, message oriented integration is the idea of a consumer system, sending a message to a provider system to invoke or trigger an activity or message which is sent back to the consumer system.
- **Service Oriented Architecture:** Service Oriented Architecture (SOA) is an architectural pattern in which system components (or application components) provide services to other system components (or application components) through a communication protocol and over a network.

The following table provides an overview of the common integration approaches mentioned above along with the current use of those approaches with MMP.

*Table 2: Integration Approach for MMP*

<b>Integration Approach</b>	<b>Description</b>	<b>Current Use Within MMP</b>
Automated Batch File Transfer	<p>This batch file is sent in a point-to-point fashion from one system to another leveraging commonly used Secure File Transfer Protocols (SFTP). Often batch file transfers are triggered by scheduled jobs and therefore, are not considered real-time integration.</p> <p>EDI is a standard network protocol used in batch file transfers for data exchange to ensure data is sent in a standard format</p>	<p>TEDS to Medicaid Management Information System</p> <p>Medicaid Management Information System to Department of Human Services</p> <p>Third Party Partners, other State Agencies, and other Interface Partners</p>

<b>Integration Approach</b>	<b>Description</b>	<b>Current Use Within MMP</b>
	that is acceptable by both parties which is also used for Batch File Transfers	
Message Oriented Integration	<p>There are two types of communication approaches used in message oriented architecture:</p> <p>Synchronous Communication: Consumer system sends a call or message to the provider system and waits for a reply. No further communication can take places until the reply has been received or activity has been triggered.</p> <p>Asynchronous Communication: Consumer system sends a call or message to the provider system and instead of waiting for the reply, the consumer system can continue running system processes (if required).</p>	Eligibility request and response (e.g., provider asking if the client is eligible for Medicaid services)
Service Oriented Architecture	<p>This type of integration can involve either simple data passing or it could involve two or more services coordinating some activity.</p> <p>A consumer system will send a service request message to a provider system who will return a response to the consumer system. A consumer system can also be a provider system. Web services is the connection technology used in service oriented architecture and can include specifications such as SOAP, REST, JSON, HTTP, XLM</p> <p>An Enterprise Service Bus is commonly used to enable Service Oriented Architecture.</p>	<p>Provider Data Management System (PDMS)</p> <p>Medicaid Management Information System</p> <p>Edifecs</p> <p>Clinical Knowledge Module</p> <p>Health Information Exchange</p>

### 3.3.1. Integration Target Architecture

The Interface Management Master Plan must articulate not only the strategy for integration for the project, but must include a definition or blueprint of the anticipated future state architecture for TEDS integration with Interface Partners both internal and external to HCFA.

The integration target architecture or blueprint (also known as the Conceptual Integration Architecture diagram) defines the high-level integration architecture without including detailed integration design specifications. However, this iteration of the diagram, should provide an understanding of what systems or system components are sending and receive data, the integration approach that should be leveraged and at a high level the information and/or services that are being exchanged. Depending on the level of detail required components of the conceptual integration architecture diagram can be decomposed for logical representation.

This artifact is also useful in understanding security and privacy requirements for integration and is especially relevant when assessing risks and security concerns.

The EA-BOM Management Plan provides a specification of the Conceptual Integration Architecture diagram. This should be completed by the State and TAS Contractor prior to the onboarding of an SI Contractor.

### 3.3.2. Integration Roadmap

Once an Integration Strategy and target architecture has been established, high level requirements for TEDS integration are defined. These high level requirements should be prioritized based on agreed upon prioritization criteria (e.g., timing, risk, funding, business criticality, regularity/legal requirements, etc.)

Based on this, the State and/or TAS Contractor will define a roadmap for implementing TEDS integration requirements which identifies the projects required to deliver interface releases.

### 3.3.3. Integration Scenarios

There are three types of integration scenarios that EMP will require and that must be delivered by an SI Contractor:

- Scenario 1: TEDS and HCFA System (e.g., TEDS sends data to MMIS to enroll a client in Medicaid)
- Scenario 2: TEDS and External System (e.g., TEDS receives data from the Federal Data Services Hub (FDSH))
- Scenario 3: TEDS and State System (e.g., TEDS integration with other State systems and other third party partners)

While each scenario is described independently, it is likely that the overarching architecture target state or future state vision for EMP includes all three scenarios.

For each scenario, key considerations must be made and managed by the SI Contractor. These include the following:

- Determining whether an existing interface to that system can be reused.
- Updating or establishing a Data Sharing Agreement between Interface Partners.
- Determining the business impact of integrating with the system.
- Identifying and complying with internal and external integration, data, security and privacy requirements and standards that must be adhered to when integrating with this system.
- Establishing Data classifications.
- Identifying appropriate security protections, policies, control and reporting requirements.

These high level considerations will guide the overall design and implementation of interfaces and may be identified in the early phases of the project and must be completed by SI Contractor once mobilized, where applicable the SI Contractor is responsible for coordinating with the Interface Partners. Additionally, this must be described as part of the Interface/Integration Management Master Plan.

### **3.4. Interface Release Plan**

An Interface Release Plan is required for the interfaces that are to be deployed as part of a project release. The Interface Release Plan will adhere to the Interface/Integration Management Master Plan as relevant to the integration and interface requirements that are to be delivered through a project.

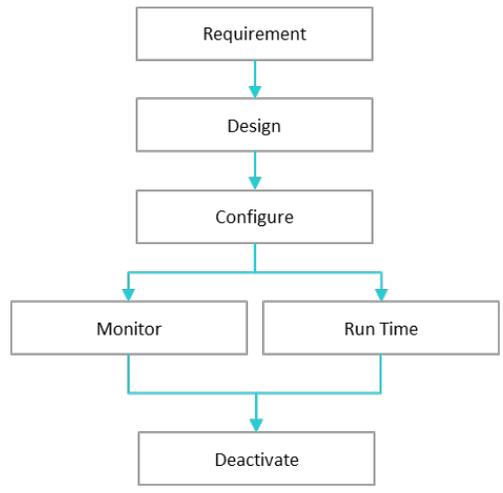
This plan must identify individual interface requirements and manage the implementation of this interface throughout the Interface Management Life Cycle while aligning to the overarching master plan.

The SI Contractor must ensure that their plan for the interface/integration release is aligned to the overarching Interface Management Master Plan for EMP, and must coordinate with the Interface Partners as required. As such, the SI Contractor will update the Interface/Integration Master Plan accordingly in relation to the Interface Release Plan they are managing.

### **3.5. Interface Management Life Cycle**

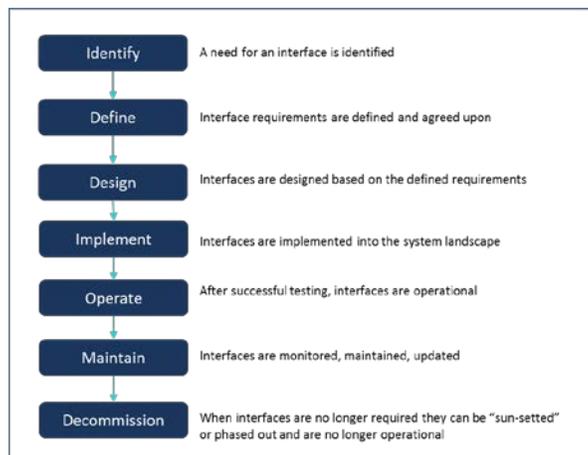
Interface management is key to the design and implementation of an interface and all associated activities must be coordinated, managed, and communicated effectively by the SI Contractor to allow for the successful implementation of an interface.

Interfaces should be managed throughout their life cycle within a system landscape as seen in the following diagram:



*Figure 3: Management of Interfaces during their life cycle in a System Landscape © 2011 IEEE*

For the management of interfaces for TEDS, the above mentioned Life Cycle has been elaborated to include more detailed interface management activities as described below:



*Figure 4: TEDS Interface Management Life Cycle*

The above mentioned phases are executed by the MMP SDLC. This allows for the effective management of interface/integration implementation activities through the initiation, design, development, and testing, implementation, and Operations/Maintenance Phases of the MMP SDLC.

Detailed activities and deliverables related to integration/interface management that should be addressed for each interface release are described in the Framework and Methodology section of this document.

## 4. Governance

This section describes the governance mechanisms that will be in place to provide guidance and monitoring for the management of interfaces/integration for MMP and associated projects.

### 4.1. Governance Bodies

The MMP governance structure and gates provide the rules, regulations, and decision making bodies that are accountable for providing guidance, review, and approval at the most important stages of the MMP SDLC. These mechanisms play a key role in the management of interface/integration throughout the Interface/Integration Life Cycle.

Below are descriptions of major governance bodies and their impact on interface/integration management:

**Project (Program) Steering Committee(PSC):** The PSC is the key body within the governance structure and is responsible for the business issues associated with the project that are essential to ensuring the delivery of the project outputs and the attainment of project outcomes. This body is interested in understanding the business impact of the overall interface/integration that is being implemented, but also the impact of the activities involved in managing these interface/integration throughout their Life Cycle.

**Technical Architecture Review Board (TARB):** The TARB will fulfill the role of reviewing and approving architecture at the MMP SDLC Gate Reviews. Specific to interface/integration, the TARB will review the interface design specific to a particular solution. This includes:

- Compliance to internal and external integration principles and standards including legal and regulatory standards.
- Integration architecture and interface design alignment to the target integration architecture for the project ensuring that solutions under development, or that have been implemented, align with requirements.
- Business and technology impact and risk associated to integration architecture and interface design.

**Information Systems Security Council (ISSC):** The ISSC will provide guidance and approval related to information security and privacy concerns, standards, and principles that must be adhered to when integrating systems. The ISSC ensures that risk is managed appropriately and the required risk mitigating controls are put into place. This is critical for ensuring that the data being transferred both within and outside of the bounds of the organization is secure.

Please refer to the Program Governance Management Plan for PSC, ISSC, TARB charters.

## 4.2. Integration Principles

In order to encapsulate the overall vision of the integration strategy for the organization and to ensure a successful implementation of interfaces, it is important to establish integration principles to guide such implementations.

The PGMP defines the process for approving and governing principles while the Interface/Integration Management Master Plan identifies principles that the project must align to.

It is suggested that for EMP, a series (between 10 – 20) of integration principles be defined and these principles should align to the overarching integration strategy for HCFA.

The following lists a sample set of integration principles and definitions:

- **Plan Early:** Integration should be planned as early as possible. Usually, integration is an afterthought resulting in quick builds on tight budgets, maintenance of these integrations become very costly and inefficient in the future.
- **Establish Standards:** Integration standards should be identified, made available and complied with by the developer for both consumer and provider systems. Compliance to standards will result in consistency and low implementation costs.
- **Reuse Components:** To reduce the number of integrations attempting to execute the same logic, reusability of components is preferred and should be identified. This would reduce the cost of subsequent development of components.
- **Interoperability Component:** Describes the identification, acknowledgement, reconciliation, and reporting of any/all transactions between systems occurs and how it should be managed to ensure interfaces are available and operating accordingly.
- **Flexible Designs: Flexibility** reduces costs related to adding new systems and/or migration from one system to another.
- **Loosely Coupled Interfaces:** Interfaces should be loosely coupled and backward compatible to reduce the impact of change to the business.
- **Message Based Interfaces:** Message based interfaces will enforce architectural principles and will simplify integration.
- **Integration Security:** Users should be authenticated with an internal access control and should ensure that all authentication and authorization requirements have been met. Incoming messages should also be authenticated to ensure they are being sent from a secured source.
- **Manage Change:** A change management process should be defined and enforced to ensure that changes are implemented in a timely manner.
- **Monitor and Update:** Integration should continuously be monitored through the use of tools to administer and check the diagnostics of the system.

Integration Principles are defined, established and enforced by the TARB as a subset of overarching enterprise architecture principles. Interface and integration design and implementation solutions are subject to design reviews and should adhere to the established principles.

### 4.3. Interoperability Standards

Interoperability standards allow data to be shared across stakeholders and Interface Partners. In the case of HCFA, this could include HCFA itself, members, business partners, other agencies (e.g., Department of Human Services), Managed Care Organizations and the Federal Government.

The PGMP defines the process for approving and governing standards while the Interface/Integration Management Master Plan identifies standards that that project must align to.

It is suggested that for EMP, interoperability standards be defined, agreed upon and enforced. The Interface/Integration Management Master Plan should identify the integration standards the project and each interface release will need to adhere to.

HCFA has established some standards that must be adhered to depending on the integration approach being taken. The following represents some (not all) categories of standards accepted by HCFA that the EMP project should comply with:

- ASC X12 (ANSI ASC X12): EDI standards for the exchange of data related to eligibility, coverage and benefit related transaction. These standards can be found in the Health Care Legibility Benefit Inquiry and Response implementation guide for developers.
- Health Level Seven (HL7) Standards: These standards define how electronic information is packaged and communicated from one party to another, setting the language, structure and data types required for seamless integration between systems.
- National Council for Prescription Drug Programs (NCPD) Standards: These standards define how health care related information is to be exchanged for pharmacy service and are named in federal legislation, including HIPAA.
- Secure Socket Layer (SSL) Standards: These standards define how connections between two systems that are communicating can be made secure through encryption.
- Centers for Medicare and Medicaid Services (CMS): Alignment to CMS standards for integration and interface development (e.g., Interface Control Standards etc.).

Integration Standards are defined, established and enforced by the TARB as a subset of overarching enterprise architecture standards. Interface and integration design and implementation solutions are subject to design reviews and should adhere to established standards.

### 4.4. Integration Patterns

The Interface/Integration Management Master Plan should identify and include any existing patterns that are applicable and can be reused for the EMP project.

In the case of TEDS, some interfaces may already exist that would need to be updated. In other cases, there could be TEDS interfaces that do not already exist and need to be created.

The following example illustrates the pattern HCFA has defined, in the form of a work flow, for establishing new interfaces with Interface Partners. Additional patterns should be included as required.

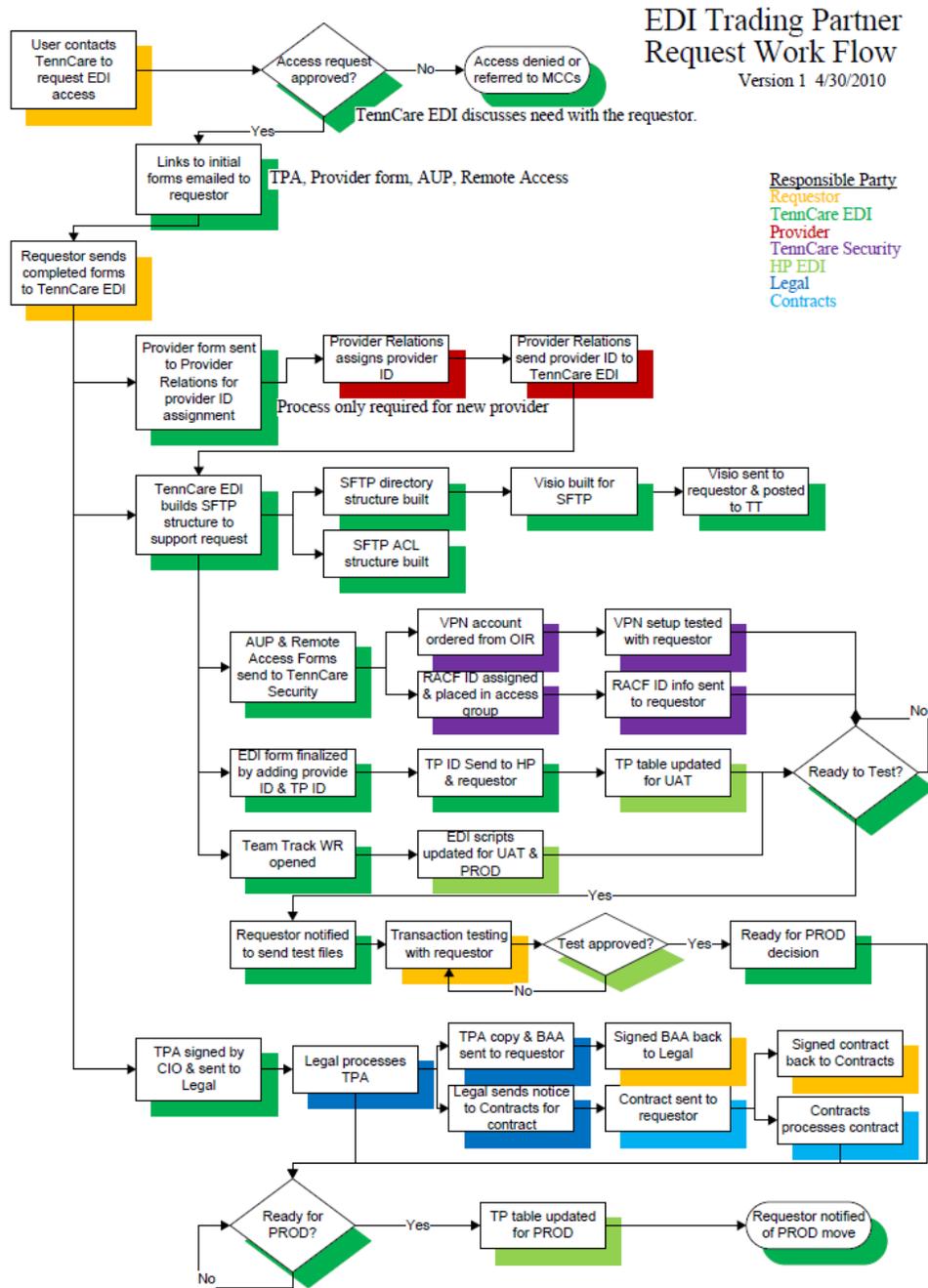


Figure 5: EDI Trading Partner Request Flow

## 5. Interface/Integration Framework and Methodology

As described in the preceding section, the Interface Release Life Cycle as part of the MMP SDLC is the basis of the Interface/Integration management framework and methodology that will be applied to EMP.

The framework and methodology to be followed, as articulated in the Interface/Integration Management Master Plan, is relevant at the project level, but should be applied in the context of managing each interface release.

As seen in the figure below, the Interface/Integration Management Master Plan is defined by the SI Contractor once mobilized and is used to inform the development of the Interface Release Plan.

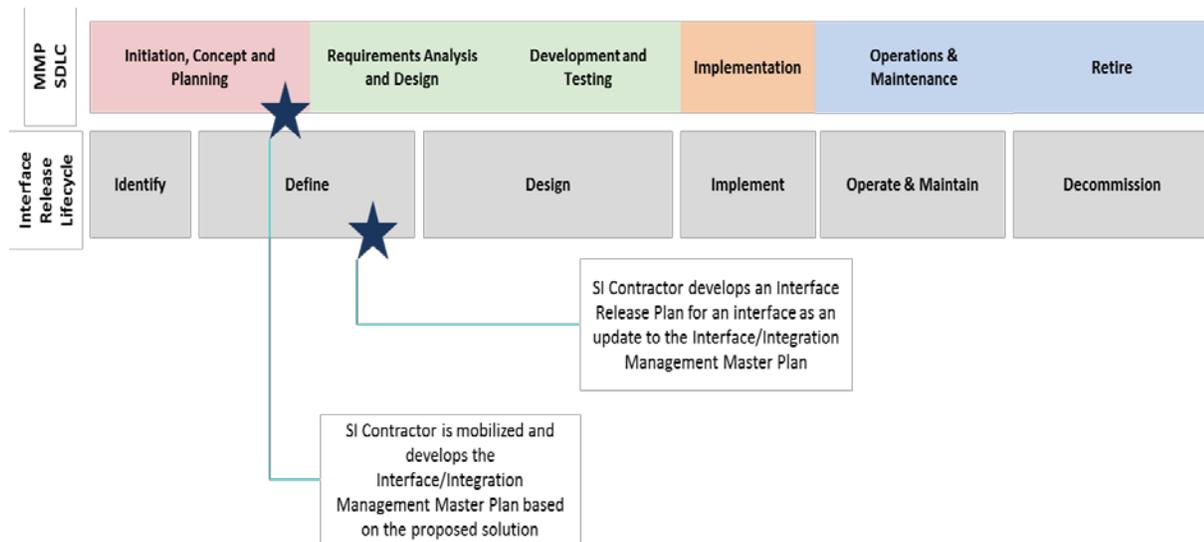


Figure 6: Interface Management Life Cycle Alignment to the MMP SDLC

In the following sections of the Interface/Integration Framework and Management Methodology, each phase has been further detailed and where applicable critical artifacts to be developed have also been identified.

Please refer to the MMP SDLC Management Plan for additional detail.

### 5.1. Identify Phase

At the onset of the Interface Release Life Cycle, project planning as related to interface/integration takes place in which the program roadmap, priorities, interface needs and gaps are identified.

Additionally, data sharing needs and requirements are identified with the potential Interface Partners. It is the responsibility of the SI Contractor once onboard to coordinate, complete and finalize these agreements where applicable. It is important to emphasize that although the SI

Contractor is responsible for the coordination, the State will have ownership over any and all Trading Partner and Data Sharing Agreements.

Based on the output of this planning, the State and/or TAS Contractor will identify high level project specific interface requirements.

In this phase, the current inventory of interfaces will be identified to:

- Identify a need for an interface.
- Determined if any existing interfaces can be reused.
- Determined if any existing interfaces can be decommissioned.

### **SDLC Alignment:**

The Identify Phase is linked to the Initiation Phase of the SDLC Life Cycle and is linked to the Project Start-Up Consult SDLC Stage Gate.

### **Output:**

A key output of this phase will include, but may not be limited to the following:

- High level program roadmap
- Interface needs and gaps

## **5.2. Define Phase**

During the Define Phase, the State and the TAS Contractor will address underlying gaps and further detail out interface/integration requirements through the iterative development of conceptual integration architecture and data flow diagrams specific to the project.

These diagrams will map the flow of information between source and target system(s).

- Specifications for the **Conceptual Integration Architecture diagram** and the **Data Flow diagram** can be found in the EA-BOM Management Plan.

Requirements derived from these diagrams will inform the definition of Interface/Integration requirements and will be documented as part of the Requirements Traceability Matrix, Business Requirements Definitions and Solution Requirement Specification.

Additional requirements such as data, security and privacy requirements are also defined during this phase and should be included in the corresponding artifacts as stated above.

- Specifications for the **Requirements Traceability Matrix, Business Requirements Definition** and **Solution Requirement Specification** can be found in the EA-BOM Management Plan.

During this phase the SI Contractor is mobilized, once onboard the SI Contractor must develop the Interface/Integration Management Master Plan. As described in earlier sections of this document, the Master Plan includes the following:

- EMP Integration Strategy.

- EMP Integration Target Architecture (integration blueprint).
- EMP Integration Roadmap.

A detailed definition of what the Interface Management Master Plan consists of is described in section 3.2 of this document.

Additionally, specific to each interface release and as defined by the State, the **Data Sharing Agreements** if not already established with the Interface Partner must be completed during this phase by the SI Contractor. In the case that a Data Sharing Agreement already exists, it must be validated or updated according to the needs of the required interface.

In order to ensure the successful implementation and operations of an interface, it is critical to have alignment between the SI Contractor and Interface Partner, particularly with regards to the scope and target architecture of the project and the identified interface/integration requirements. Where applicable the SI Contractor will identify additional requirements including, but not limited to scope, design, development, installation, integration, testing and implementation.

Requirements identified by the State and TAS Contractor are to be confirmed and agreed upon by all project stakeholders.

HCFA has specific interface/integration requirements for the following:

- TennCare VPN communication requirements.
- File encryption procedure requirements.
- HIPAA Transaction Set requirements.
- Requirements to support TennCare rules regarding multiple transactions types within a file.
- Size requirements for Transmissions and Batches.
- Acknowledgement Process and Transmission completion checks.
- Requirements around balancing data elements.

The SI Contractor must then define their plan for the management of the release of an individual interface. This Interface Release Plan, will be a sub-set of the overarching Interface Management Master Plan for EMP and as such, updates to the Master Plan will be made at this point.

#### **SDLC Alignment:**

The Define Phase is linked to the Concept, Planning, and Requirement Analysis Phase of the SDLC Life Cycle and is linked to the Architecture Review, Project Baseline Review, and Preliminary Design Consult SDLC Stage Gate.

#### **Output:**

Key outputs of this phase will include, but are not limited to:

- Conceptual integration architecture diagrams and data flow diagrams.
- Requirements traceability matrix, business requirement definition and solution requirement specification containing interface/integration requirements as required.
- Data Sharing Agreement.

- Interface Release Plan.
- Test Management Plan.

## Data Sharing Agreement

The Data Sharing Agreement is a formal contract between two or more parties clearly outlining what data is required, how the data will be provided through system integration and the purpose and use of the data. The primary purpose of these agreements is to ensure that the data is being provided through secure data exchanges. Additionally, the Data Sharing Agreements will also prevent any miscommunication on part of the provider of the data and/or the consumer of the data by ensuring that the terms and conditions and use of data have been discussed and agreed upon prior to the start of design.

SI Contractor will be responsible for identifying and securing the Data Sharing Agreements with other Interface Partners within the State and other external partners such as CMS, and/or IRS.

In some cases there may already be Data Sharing Agreements in place, for example the agreements around the Authority to Connect (ATC). In such cases the agreements will be revisited during the renewal process and updated as required.

Please refer to the detailed Data Sharing Agreement specification in Appendix C1.

### 5.3. Design Phase

In the Design Phase, the SI Contractor must design an interface based on interface requirements for the project. Additionally, a **Business Impact Analysis** is conducted by the SI Contractor to ensure that the interface/integration design achieves the following:

- Meets interface/integration project requirements including data, privacy and security requirements.
- Adheres to the internal and external integration and relevant data, security, privacy, legal and regulatory principles and standards.
- Utilizes the appropriate integration approach as outlined in the Interface/Integration Management Master Plan.
- Aligns to the Interface/Integration conceptual target architecture (blueprint).
- Operational Support Plan, should detail and describe how the identification, acknowledgment, reconciliation and reporting of any / all transactions between systems will be developed and managed.

Additional detail regarding the Business Impact Analysis at the end of this section.

To document the design of an interfaces for release, the SI Contractor must provide an **Interface Control Document**. This document provides a detailed definition of the interfaces to be deployed for each Interface Partner that TEDS will be integrating (e.g., Additional details regarding the Interface Control Document can be found at the end of this section.

- SI Contractor is required to incorporate all relevant interface/integration design components into the Functional/Technical design of the solution.

The SI Contractor and the State must identify **Acceptance Criteria and Metrics** for each interface:

- Acceptance criteria should address the following considerations:
  - All business rules have been successfully triggered and the associated interface test cases have passed successfully.
  - All requirements and associated test cases have been successfully tested at the system integration level.
  - All security / privacy requirements related to the data being transmitted, data at rest, access and authorization have been successfully tested.
  - All appropriate data conversion activities have been successfully completed, field and record validations are completed, and unneeded data elements have been isolated.
  - Stress/performance testing activities have been successfully performed verifying that interface(s) function appropriately at average and agreed upon peak levels.
  - All critical interface defects have been closed and the remaining open defects have a severity classification assigned to them and a target fix date.
  - The interface has demonstrate the ability to support peak loads and is able to return to normal performance after withdrawal.
  - All notices have been successfully triggered and the associated interface test cases have passed successfully.
  - All notices have been printed successfully with the correct formatting and meet the requirements for mass printing of various notice types.
- It expected that the SI Contractor will collect and report on the following interface/integration metrics within the Interface Control Document. Definitions and examples of these metrics includes in Appendix D.
  - Error Discovery Rate.
  - Test Execution Coverage.
  - Application Defect Density.
  - Average Defect Age.
  - Test Schedule Variation.
  - Requirements Stability Index.
  - Test Design Coverage.
- Based on the availability/acceptance criteria, Service Level Agreement components specific to interface/integration should also be established.

Once design has been accepted by all stakeholders and Interface Partners, a Test Management Plan is to be created by the SI Contractor in order to develop, manage, and monitor the testing schedule for the interface being deployed. All testing such as development, connectivity, validation and end-to-end testing is to be completed as defined in the Test Management Plan.

The SI Contractor must create documentation to show the successful testing for completeness, accuracy, timeliness and performance of the interface and will provide this to the State and the appropriate IV&V personnel to support attestation. Test cases and scenarios are to also be provided to the State, as required during User Acceptance Testing (UAT)

Testing must be completed in a collaborative manner in which the State UAT and SI Contactor work together in close proximity to test and perform UAT simultaneously.

- Refer to the Test Management Plan for additional detail. Please note that integration testing is captured as a component of the larger Test Management Plan for the solution.

### **SDLC Alignment:**

The Design Phase is linked to the Design, Develop, and Test Phase of the SDLC Life Cycle and is linked to the Final Detailed Design Consult, Validation Readiness Review, and Implementation Readiness Review SDLC Stage Gate.

### **Output:**

There are several critical outputs of the Design Phase which need to be completed and agreed upon by all stakeholders prior to moving on to the Implementation Phase. These include the following:

- Business Impact Analysis.
- Interface Control Document.
- Definition of Availability/Acceptance Criteria.
- Interface/Integration design components required in the Functional/Technical Design of the Solution.
- Interface/Integration Test Management Plan and associated testing artifacts (e.g., test scripts, system readiness certifications etc.) as required.
- Interface/Integration design components within the Service Level Agreement for the solution.

### **Business Impact Analysis**

The Business Impact Analysis is to be completed by the SI Contractor in coordination with the State, and TAS Contractor in order to determine the impact of the interfaces on existing operations and on the organization as a whole. The analysis will identify the criticality of the business functions, dependencies and prioritize interfaces using relevant criteria. The SI Contractor will also identify fail-over approaches to addressing availability and system interruptions.

Additionally, the SI Contractor will analyze the existing risks to understand their significance and will identify risk mitigation strategies for the identified risks. The assessment will identify and describe any open issues such as interface defects that the project team will need to resolve in later project phases and/or prior to moving into implementation. Based on the assessment, critical success factors will be identified and agreed upon for the remainder of the project.

Please refer to the Business Impact Analysis specification in Appendix C2.

### **Interface Control Document**

The SI Contractor is responsible for the creation of the Interface Control Document describing the relationship between the two interconnected systems. The document will specify the interface requirements to be met by the participating systems. The document will also describe the concept of operations, the governance of the data exchange, and identifies the communication paths along which the data is expected to flow. Additionally, the document will provide a control mechanism for each integration to ensure successful and complete exchanges of information takes place from the specified data elements.

It is the responsibility of the SI Contractor to work jointly with the State and other Interface Partners to ensure the document is accurate, complete, reviewed, and approved, and that access to information is granted at the appropriate times.

Please refer to the Interface Control Document specification in Appendix C3.

## 5.4. Implementation Phase

Once the design, build, and testing has been successfully completed and accepted by the State, interfaces are to be deployed by the SI Contractor to the production environment closely adhering to the overarching change, configuration, deployment, and risk mitigation plans.

Prior to the deployment of the interface the SI Contractor, Interface Partner, and the State are to participate in Pre-Deployment Gate Reviews ensuring readiness of the interface for integration for deployment.

As part of the Implementation Phase, maintenance and support documents are to be updated and end-users are to be trained by the SI Contractor.

### **SDLC Alignment:**

The Implementation Phase is linked to the Implementation Phase of the SDLC Life Cycle and is linked to the Operational Readiness Review SDLC Stage Gate.

### **Output:**

A key output of this phase will include, but may not be limited to the following:

- Plan for mitigating interface/integration related risk.
- Interface/Integration components of System Operation documents.

## 5.5. Operate and Maintain Phase

Interfaces are operational once successfully implemented. The SI Contractor will operate and maintain the interfaces defect free for the duration of the contract. At the completion of the contract the SI Contractor must transition interface operations and maintenance to the State and the designated replacement SI Contractor if applicable.

During operation and maintenance of the interface, exceptions and errors should be analyzed through a root cause analysis. Resolutions, escalation and communication plans and procedures are to be developed. Planned and/or suggested changes are to adhere to the change control process as identified within the Change Management Plan. As part of the update of an interface, the Business Impact Analysis Document should be referenced and updated as needed.

### **SDLC Alignment:**

The Operate and Maintain Phase is linked to the Operations and Maintenance Phase of the SDLC Life Cycle and is linked to the Post Implementation Review SDLC Stage Gate.

**Output:**

A key output of this phase will include, but may not be limited to the following:

- Interface/Integration Root Cause Analysis.
- Updates to the Operation & Maintenance Run Books.
- Updates to the Business Impact Analysis.
- Interface Release Plans.

## 5.6. Decommission Phase

An interface may be decommissioned with State approval as a result of end of life and/or as a result of taking a different approach. A decommissioning plan is to be developed to identify the approach on how the interface will be decommissioned, who will be involved, and identify the data that is to be converted over to a new interface and/or archived.

Additionally, during decommissioning the Business Impact Analysis for the interfaces to be decommissioned is to be conducted as to minimize the impact of the operations of the business.

**SDLC Alignment:**

The Decommissioning Phase is linked to the Operations and Maintenance Phase of the SDLC Life Cycle and is linked to the Post Implementation Review SDLC Stage Gate.

**Output:**

A key output of this phase will include, but may not be limited to the following:

- Updated Business Impact Analysis.
- Plan for decommissioning existing interfaces/integration.

## 6. Operational Interface/Integration Plan Management

The MMP SDLC is the methodology used to align the activities required for the development of the solution. This includes activities related to interfaces and integration. The effective management of the interface/integration activities is critical to ensuring a successful implementation of project and program.

For this to be possible the following capabilities need to be put in place:

- Change Management Support.
- Communication Planning and Coordination.
- Key Roles accountable for the management of interface/integration.

The following sub-sections of this document will provide additional detail describe the above mentioned capabilities.

### 6.1. Change Management

A change management process must be in place to manage changes to the interfaces while in production and non-production environments. The SI Contractor must define a process that is aligned to the overall project level change management expectations as outlined in the Change Management Plan. During a project SDLC, if the project's Interface/Integration Management Master Plan requires changes to its scope, methods, tools, stakeholders and activities, etc. it will go through the proper change management process within the project.

From this plan, the SI Contractor will receive guidance for developing plans to manage interface/integration related changes and defining a change management process for interface/integration.

For interface/integration change management, key roles will be involved in the review and approval of the interface/integration changes depending on impact of the required change. For interface/integration this should include relevant Interface Partners, project sponsors (technology and business) and Enterprise Architects.

Please refer to the Project Change Management Plan.

### 6.2. Communication Management

A Communication Management Plan for interface/integration management should be included as part of the project level Communication Management Plan.

Specific to interface/integration management, a Communication Management Plan should include, at minimum, the following:

- A mechanism to alert the stakeholder when a review or approval is required.
- A plan or process for raising and escalating concerns, issues, decision points and for issue resolution.

- Alert procedure for contacting key personnel in the event of interface/integration interruptions, failures and related disruption to business operations etc.

This communication management capability must be established to effectively manage all activities associated to the management of interface/integration activities through the entire life cycle of an interface.

### 6.3. Roles and Responsibilities

To successfully implement interfaces, key capabilities need to be delivered by the State and all identified MMP Contractors. This section defines the general responsibilities of each of key role in the context of the Interface/Integration Management Plan.

The following table summarizes the key roles and responsibilities for the State and MMP Contractors using the Interface Life Cycle as a reference. It is important to keep in mind that responsibilities identified within the signed contractual agreement will take precedence over the responsibilities identified within this section.

Refer to Appendix B for detailed role descriptions and RACI convention used.

*Table 3:Interface Life Cycle Roles and Responsibilities*

Interface / Integration Activities	STATE					CONTRACTOR			
	HCFA Business	HCFA IS	HCFA Enterprise	Program and Project	STS (Infrastructure)	SI	TAS	SPMO	IV&V
<b>IDENTIFY NEED</b>									
Identify Program Roadmap and Priorities	A	SR	C	C	I	-	R	I	C
Identify interface requirements for APD and RFQ	A	SR	C	C	I	-	R	I	C
List of interface needs/ gaps for APD and RFQ.	A	SR	C	C	I	-	R	I	C
<b>DEFINE INTERFACES</b>									

Interface / Integration Activities	STATE					CONTRACTOR			
	HCFA Business	HCFA IS	HCFA Enterprise	Program and Project	STS (Infrastructure)	SI	TAS	SPMO	IV&V
Define conceptual interface(s) and conceptual interface diagrams for APD and RFQ	C	A	C	I	I	-	R	I	C
Approve conceptual interface requirements and design for APD and RFQ	C	A	C	SR	I	-	R	I	C
Review and refine interface requirements	C	A	C	I	I	R	SR	I	C
Conduct business impact assessment and business continuity planning	I	A	C	SR	I	R	SR	C	C
Complete and formalize data sharing agreements	A	SR	SR	I	I	R	C	C	C
Develop Interface/Integration Management Master Plan	C	A	C	C	I	R	C	C	C
Gather and escalate interface/integration risks and develop risk mitigation strategies	SR	SR	SR	A	I	R	SR	SR	SR
Assess integrations and interface compliance with standards	I	A	C	SR	I	SR	R	I	C
Finalize Interface/Integration Management Master Plan	C	A	C	I	I	R	C	I	C
Review and approve Interface/Integration Management Master Plan	C	A	C	SR	I	C	R	C	C

Interface / Integration Activities	STATE					CONTRACTOR			
	HCFA Business	HCFA IS	HCFA Enterprise	Program and Project	STS (Infrastructure)	SI	TAS	SPMO	IV&V
Further define and refine Interface(s) and Integration Requirements	C	A	C	I	I	R	C	I	C
Define data conversion requirements and the schedule of data conversion activities	C	A	C	C	I	R	SR	SR	C
Approve interface and integration requirements	A	SR	C	SR	I	C	C	C	C
Develop Interface Release Plan(s) and update the interface/integration management Master Plan	C	A	C	C	I	R	C	C	C
<b>DESIGN INTERFACES</b>									
Further refine Interface(s) and Integration Requirements based on Design considerations	C	A	C	I	I	R	C	C	C
Identify performance and availability criteria for each interface integration	SR	A	C	I	I	R	C	C	C
Develop interface control document(s) (ICD)	C	A	C	I	I	R	C	I	C
receive approval for interface control document(s) (ICD)	C	A	C	SR	I	R	C	C	C
Develop and complete service level agreements / memorandum of understanding (MOUs)	A	SR	I	C	I	R	C	C	C

Interface / Integration Activities	STATE					CONTRACTOR			
	HCFA Business	HCFA IS	HCFA Enterprise	Program and Project	STS (Infrastructure)	SI	TAS	SPMO	IV&V
Review and approve design compliance with applicable requirements and standards	C	A	SR	SR	I	I	R	C	C
Update Interface Release Plan(s) based on design considerations and update the Interface/Integration Management Plan	C	A	C	C	I	R	C	C	C
Provide Support in procurement of necessary agreements with third parties	SR	A	C	SR	I	R	C	C	C
Develop / code interface integrations	I	A	C	I	I	R	C	I	C
Coordinate integration efforts with interface partners and all State agencies	SR	A	SR	I	I	R	I	SR	C
Development of control mechanisms for each integration	I	A	SR	C	I	R	I	I	C
Develop fail-over approaches	I	A	I	I	I	R	I	I	C
Receive approval to move from development to testing	SR	A	C	SR	I	R	C	C	SR
Conduct Interface Testing ( Refer to Test Management Plan)	C	A	C	I	I	R	SR	C	C
Conduct business impact assessment and business continuity planning	SR	A	C	SR	I	R	SR	C	C

Interface / Integration Activities	STATE					CONTRACTOR			
	HCFA Business	HCFA IS	HCFA Enterprise	Program and Project	STS (Infrastructure)	SI	TAS	SPMO	IV&V
Support IV&V reviews and attestation requirements	C	A	C	I	I	R	I	I	SR
IV & V Post attestation documents	I	A	I	I	I	I	I	I	R
<b>IMPLEMENT INTERFACES</b>									
Perform final data conversion activities	I	A	I	I	I	R	C	C	C
Finalize interface and integration deployment risk mitigation and contingency/roll back plans	C	A	I	SR	I	R	C	SR	C
Implement interface(s)	I	A	I	I	I	R	C	I	C
Monitor operational interface	I	A	I	I	I	R	C	I	C
<b>OPERATE and MAINTAIN INTERFACES</b>									
Operate Interface(s)	I	A	I	I	I	R	I	I	C
Maintain / update interface(s) performing root cause analysis on all identified issues	I	A	I	I	I	R	I	I	C
Perform routine maintenance of interface integrations	I	A	I	I	I	R	I	I	C
Conduct business impact assessment and business continuity planning	C	A	C	C	I	R	SR	C	C
Manage and monitor daily interface/integration activities	I	A	I	I	I	R	I	I	C

Interface / Integration Activities	STATE					CONTRACTOR			
	HCFA Business	HCFA IS	HCFA Enterprise	Program and Project	STS (Infrastructure)	SI	TAS	SPMO	IV&V
<b>DECOMMISSION INTERFACE(S)</b>									
Conduct business impact assessment and business continuity planning	C	A	C	SR	I	R	SR	C	C
Decommissioning of Interface(s)	I	A	C	I	I	R	I	I	C
Archive Data	I	A	C	I	I	R	I	I	C

### 6.4. Additional Roles for Consideration

Each key role mentioned above can be further decomposed into several other sub roles. Although this section will not go into such granularity, it will identify additional roles required by both the State and the MMP Contractors which are critical to the management and successful implementation of interfaces. Further details on additional roles can be found within the RFQ.

- SOA Architect:** The SOA architect will be responsible for designing and implementing the integration between the TEDS and other state standard Commercial of the Shelf (COTS) software using the latest SOA technologies and Web Services.
- Interface / Integration Lead:** The Interface / Integration Lead will serve as the interface and integration lead for the solution. The lead will also play the role of a liaison, and will be responsible for coordinating with parties taking part in the development and implementation of interfaces to ensure agreement and alignment as it relates to interface design and development in order to mitigate the risks of poorly designed and implemented interfaces. Additionally, the lead will also monitor and report on the progress made by Interface Partners.
- Change Manager:** The Change Manager will be responsible for working with the state HCFA Technical Change Control Board to ensure that all interface / integration changes are recorded, evaluated, authorized, prioritized, planned, tested and implemented in a controlled manner. Additional roles and responsibilities of the Change Manager and related change roles are highlighted in the Change Management Plan

- **Operations Manager:** The Operations Manager will be responsible for the daily operational activities needed to manage the IT interfaces according to the performance standards defined during Service Design. Additional roles and responsibilities of the Operations Manager and other related operations and maintenance roles are highlighted within the Operations and Maintenance Management Plan
- **Test Manager/Lead:** The Test Manager and Lead will be responsible for overseeing the development and scheduling of testing activities, approaches, and results. Additional roles and responsibilities of the Test Manager/Lead and related testing roles are highlighted within the Test Management Plan.

## Appendix A: Definitions, Acronyms and Abbreviations

Table 4: Definitions, Acronyms and Abbreviations

Acronym	Definition
ACL	Access Control List
AR	Architecture Review
ATC	Authority to Connect
AUP	Acceptable Use Policy
BAA	Business Associates Agreement
BOM	Business Operating Model
CIO	Chief Information Officer
CKM	Clinical Knowledge Module
CMS	Centers for Medicare and Medicaid Services
CMS-ELC	Centers for Medicare and Medicaid Services Enterprise Life Cycle
DDC	Detailed Design Consult
DED	Deliverable Expectations Document
DHS	Department of Human Services
DR	Disposition Review
EA	Enterprise Architecture
EA - BOM	Enterprise Architecture – Business Operating Model
EDI	Electronic Data Interchange
ELC	Enterprise Life Cycle
EM	Eligibility Modernization

Acronym	Definition
EMP	Eligibility Modernization Project
ESB	Enterprise Service Bus
FDDR	Final Detailed Design Review
FDSH	Federal Data Services Hub
FTP	File Transfer Protocols
HCFA	Health Care Finance and Administration
HIE	Health Information Exchange
HTTP	Hypertext Transfer Protocol
ID	Identification
IRR	Implementation Readiness Review
IRS	Internal Revenue Services
ISSC	Information System Security Committee
IV &V	Independent Validation & Verification
JSON	JavaScript Object Notation
MCC	Managed Care Contractor
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MMP	Medicaid Modernization Program
MOU	Memorandum Of Understanding
OIR	Office of Information Resources (Now Strategic Technology Services (STS))
O&M	Operations & Maintenance

<b>Acronym</b>	<b>Definition</b>
ORR	Operational Readiness Review
PGMP	Program Governance Management Plan
PBR	Project Baseline Review
PDC	Preliminary Design Consult
PDMS	Provider Data Management System
PIR	Post Implementation Review
PROD	Production environment
PSC	Project Steering Committee
RACF ID	Term referencing the Healthcare Finance and Administration (HCFA) employee and contractor user/log in identification number
REST	Representational State Transfer
RFQ	Request for Qualifications
RTM	Requirements Traceability Matrix
SDLC	System Development Life Cycle
SI	System Integrator
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPMO	Strategic Project Management Office
SFTP	Secure File Transfer Protocol
STS	Strategic Technology Solutions
TARB	Technical Architecture Review Board (TARB)
TAS	Technical Advisory Services

<b>Acronym</b>	<b>Definition</b>
TEDS	Tennessee Eligibility Determination System
TP	Trading Partner
TP ID	Trading Partner Identification Number
TPA	Trading Partner Agreement
TT	Serena TeamTrack
UAT	User Acceptance Testing
VPN	Virtual Private Network
VRR	Validation Readiness Review
WR	Work Request
XML	Extensible Markup Language

## Appendix B: SDLC RACI Chart Role Definition

This appendix defines roles and responsibilities that key stakeholders have in the SDLC Phase activities and deliverables.

The following defines what each letter in the RACI acronym means:

(R) Responsible: Those who are primary responsible for the work to complete the task or deliverable. Only one party shall be responsible for any activity, task, or deliverable.

(SR) Shared Responsibility: Those who are charged with completing some supporting work relative to the activity or task. There may be no, one, or multiple SR parties for any activity, task, or deliverable.

(A) Accountable: Those who are accountable for ensuring the correct and thorough completion of the task or deliverable. There should be only one Accountable party for any activity, task, or deliverable.

(C) Consulted: Those whose opinions and input are sought (two-way conversation).

(I) Informed: Those who are kept up to date on progress, often only on completion of the task or deliverable (one-way conversation).

Table 5: RACI Participants Definition

RACI Participants Definitions		
<b>State</b>	Program and Project Management	The management team that includes the Medicaid Modernization Program (MMP) Director and assigned Project Managers.
	HCFA Business	Organizational units that oversee the policies and operations of HCFA business functions, such as member services.
	HCFA IS	HCFA IS provides support for planning, design, implementation and operation of information technologies and methodologies.
	HCFA Enterprise Security	HCFA's enterprise security, includes HCFA & contractor resources responsible for reducing the risk of unauthorized access to systems and data.
	STS (Infrastructure)	Strategic Technology Solutions provides direction, planning, resources, execution, and coordination in managing the information systems needs of the State of Tennessee. STS is a division within the Department of Finance & Administration.

<b>RACI Participants Definitions</b>		
<b>MMP Contractors</b>	<b>TAS</b>	Technical Advisory Services supports and advises the State in completing the Medicaid Modernization Program (MMP) by offering Organizational Change Management and Training, Operations & Maintenance Planning, System Development Life Cycle Advisory Services, Quality Management, and Enterprise Architecture services.
	SPMO	The Strategic Program Management Office provides program and project management support to the State in completing the MMP
	IV&V	Independent Verification and Validation is an independent contractor responsible for verifying that any developed systems perform as designed and will continue to operate correctly in the future. IV&V provides objective evidence that all software requirements have been implemented correctly and completely. This includes evidence that the solution produces the intended results and that all functionality is traceable to solution requirements.
	SI	The System Integrator is responsible for the design, development, testing, implementation, and the operations and maintenance (O&M) of a new system to modernize and enhance eligibility determination, redetermination, and eligibility appeals for the State of Tennessee’s Medicaid program (TennCare) and Children’s Health Insurance Program (CHIP, known as CoverKids in Tennessee).

# Appendix C: Framework Specification

This section provides details pertaining to artifacts contained in the Interface/Integration Management Plan

## Appendix C.1: Data Sharing Agreement Document

Data Sharing Agreement Document	
<b>Name</b>	Data Sharing Agreement Document
<b>Alias(es)</b>	Data Use/Data Exchange/Interconnection Security Agreements
<b>Objective</b>	The objective of a data sharing agreement is to formalize an agreement between two or more parties outlining the terms and conditions, implications and protocols on sharing data.
<b>Definition</b>	<p>The data sharing agreement is a formal contract between two or more parties clearly outlining what data is required, how the data will be provided through system integration and the purpose and use of the data. This includes information that the IRS Office of Safeguards expects from an agency regarding their procedures for safeguarding Federal Tax Information (FTI), in any instance where that agency intends to receive, store, process, or transmit FTI.</p> <p>The primary purpose of these agreements is to ensure that the data is being provided through secure data exchanges. Additionally, the data sharing agreements will also prevent any miscommunication on part of the provider of the data and/or the consumer of the data by ensuring that the terms and conditions and use of data have been discussed and agreed upon.</p> <p>It is important to note that the process of setting up a data sharing agreement may vary from organization to organization and is also dependent on the data that is being shared. At a minimum the following sections should be included within the document:</p> <ol style="list-style-type: none"> <li>1 Introduction</li> <li>2 Purpose</li> <li>3 Overview and Scope</li> </ol>

<b>Data Sharing Agreement Document</b>	
	<ul style="list-style-type: none"><li>4 Assumptions / Constraints / Risks /Dependencies</li><li>5 Agreement Period</li><li>6 Parties to the Agreement</li><li>7 Description of Data</li><li>8 Data Transfer Approach</li><li>9 Location and Access to Data</li><li>10 Use of Data</li><li>11 Confidentiality</li><li>12 Data Destruction</li><li>13 Conflict Resolutions</li><li>14 Termination of Agreement</li><li>15 Terms and Conditions</li></ul>
<b>Sample</b>	A sample Data Sharing Agreement template is included in the following section.

## **Data Sharing Agreement Document**

### **Table of Contents**

1	Introduction
1.1	Purpose
1.2	Overview and Scope
2	Assumptions / Constraints / Risks /Dependencies
2.1	Assumptions
2.2	Constraints
2.3	Risks
2.4	Dependencies
3	Agreement Period
4	Parties to the Agreement
4.1	Responsibilities
5	Description of Data
6	Data Transfer Approach
7	Location and Access to Data
8	Use of Data
9	Confidentiality
9.1	Regulatory Compliance
10	Data Destruction
11	Conflict Resolutions
12	Termination of Agreement
13	Terms and Conditions
14	Costs
15	Definitions

## **1 Introduction**

### **1.1 Purpose**

Instructions: The purpose of the Data Sharing Agreement is to identify the Partners involved in the sharing of data and formalize the reason why these parties have entered agreed into the agreement.

### **1.2 Overview and Scope**

Instructions: This section will provide an overview of the agreement and will define the scope and boundaries of the agreement. It will identify at a high level introduce the project and/or program which requires the data, the type of data, the reason why the data is required and the frequency of the data requirements.

Additionally, this section will also outlines at the high level the terms and conditions which governs the agreement.

## **2 Assumptions / Constraints / Risks / Dependencies**

### **2.1 Assumptions**

Instructions: This section should describe any assumptions regarding the Data Sharing Agreement between the parties.

Assumptions are statements that can be proven to be incorrect, such as assuming that data will always be made available and is accessible as needed in a defined format. In the event assumptions are proven incorrect, identify how impacts will be mitigated and make reference to any change management and approval process.

### **2.2. Constraints**

Instructions: This section will describe any constraints which may impede on the delivery of information. Constraints will include, but may not be limited to:

legal and regulatory

established standards

### **2.3 Risks**

Instructions: This section will describe any risks associated with the sharing of data and propose mitigation strategies.

## **2.4 Dependencies**

Instructions: Describe any dependencies which apply to the BRD, especially any external factors outside of the control of the business. This may just be a reference to a project plan where dependencies are already documented.

## **3 Agreement Period**

Instructions: This section will identify the period of time which will be governed by this agreement.

## **4 Parties to the Agreement**

Instructions: This section of the document will identify the individuals and/or organizations which are bound by the agreement.

### **4.1 Responsibilities**

Instructions: This section will define in detail the roles and responsibilities of the provider and the consumer of the data. This may include, but may not be limited to:

establishing policies and procedures to prevent unauthorized access and use of data

providing data in a timely manner

conduct periodic audits to ensure data has not been breached

establish protocols on identifying how data breaches will be addressed

## **5 Description of Data**

Instructions: This section will provide specific details and information concerning the data that will be shared and its use.

## **6 Data Transfer Approach**

Instructions: This section will describe the method in which data will be transferred. The parties to the agreement will establish specific safeguards and protocols to ensure the security of the data.

For example if information is to be transferred over the internet, the use of encryption is required. Additionally information being transferred via the internet will need to be in compliant with federal and statutory regulations relating to the electronic transmission of identifiable information.

## **7 Location and Access to Data**

Instructions: This section will describe will identify the location of where the data will be stored once transferred.

Additionally this section will also identify the individuals who have access to the identified location to access data and the current security protocols in place to grant access and/or deny access to the location.

## **8 Use of Data**

Instructions: This section will describe that the data provided will be used for. For example, will the data be used internally to complete certain business transactions, or will the data be repacked and provided to another consumer such as a patient and/or a customer/

## **9 Confidentiality**

Instructions: This section will identify and describe the administrative, technical, and physical safeguards which will be put in place and adhered to by all parties of the agreement to ensure confidentiality of the data and to prevent unauthorized use or access to it.

### **9.1 Regulatory Compliance**

Instructions: This section will identify any federal and state regulations which the parties to the agreement are required to adhere to.

## **10 Data Destruction**

Instructions: This section will describe the method used to destroy the data once consumed, for example, if the data was provided as hard copies, data will be destroyed using confidential shredding services.

This section will also identify any additional time frames which may be associated with the destruction of the data and or archival of the data.

## **11 Conflict Resolutions**

Instructions: In the event of challenges, disagreements and conflicts pertaining to the agreement. This section will describe how conflicts will be mitigated between the parties involved in the agreement. For example, if a party no longer agrees to the terms and conditions, what are the steps taken to address this issue.

## **12 Termination of Agreement**

Instructions: This section will describe the process of terminating an agreement prior to its scheduled term and the various reasons as to why an agreement may be terminated. For example, an agreement may be terminated with cause as a result of one of the parties breaching the agreement.

## **13 Terms and Conditions**

Instructions: This section will describe in detail the legal terms and conditions pertaining to the data sharing agreement.

#### **14 Costs**

Instructions: This section will detail how the costs associated with the sharing of data will be met. For example, will the consumer of the data cover all costs or will the costs be shared by all parties involved.

Additionally, this section will also address how unforeseen costs will be handled.

#### **15 Definitions**

Instructions: This section will define acronyms and key term

## Appendix C.2: Business Impact Analysis Document

Business Impact Analysis Document	
<b>Name</b>	Business Impact Analysis Document
<b>Alias(es)</b>	
<b>Objective</b>	The objective of a Business Impact Analysis Document is to prioritize and assess system interfaces and/or components on their benefits, risks, constraints and potential impact to other related business operations and technologies.
<b>Definition</b>	<p>The Business Impact Analysis Document determines the impact of the proposed interfaces on existing operations and the organization as a whole. The analysis will identify the criticality of the business functions, dependencies and prioritize interfaces using defined criteria.</p> <p>The document will also analyze the existing risks to understand their significance and identify the risks which will remain after implementing the design. The assessment will identify and describe any open issues that the project team will need to resolve in later project phases. Based on the assessment, critical success factors will be identified for the remainder of the project.</p> <p>At a minimum the following sections should be included within the document:</p> <ul style="list-style-type: none"> <li>Purpose</li> <li>Introduction</li> <li>Overview and Scope</li> <li>Assumptions / Controls / Risks /Dependencies</li> <li>Points of Contact</li> <li>Interface/Integration Description</li> <li>Interface/Integration Dependencies</li> <li>Interface/Integration Resources</li> </ul>

<b>Business Impact Analysis Document</b>	
	Impact Assessment Definitions
<b>Sample</b>	A sample Business Impact Analysis template is included in the following section.

## **Business Impact Analysis Document**

### **Table of Contents**

- 1 Purpose
- 2 Introduction
- 3 Overview and Scope
- 4 Assumptions / Controls / Risks /Dependencies
- 5 Points of Contact
- 6 Interface/Integration Description
  - 6.1 Interface/Integration Dependencies
  - 6.2 Interface/Integration Resources
- 7 Impact Assessment
  - 7.1 Business Architecture Impacts
  - 7.2 Application Impacts
  - 7.3 Technical Architecture Impacts
  - 7.4 Data Architecture Impacts
- 8 Definitions

## **Business Impact Analysis Document**

### **1 Purpose**

Instructions: The purpose of the document is to provide an understanding of the business impact related to the interface/integration being deployed.

### **2 Introduction**

Instructions: This section of the document should give an overview of organization(s) and roles involved in the business impact analysis activities for the specific proposed change.

### **3 Overview and Scope**

Instructions: This section of the document should give an overview of the interface/integration requirement being deployed. It should describe the logic behind the request for the proposed change and intended goals/success factors, (2) providing a definition of the scope of work required, and (3) providing a description of areas that are out of scope.

### **4 Assumptions / Controls /Standards/Applicable Federal/State Regulations**

Instructions: This section of the document will note the relevant assumptions for relevant to the interface/integration being deployed. This section will also describe the process controls in place that potentially will be affected by the proposed change. Applicable integration standards and Federal/State regulations for the proposed change will also be described in this section.

### **5 Points of Contact**

Instructions: This section will list the points of contact involved in the business impact assessment, and the roles and responsibilities of the individuals. This section should also capture points of contact outside of HFCA if applicable to support efficient communication during interface/integration activities with outside interface partners.

### **6 System Description**

Instructions: This section will provide a description of the system(s) impacted by the proposed change. The section should include multiple views of the system(s) in diagram or model representations to provide a clear description of the impact systems and architecture components affected by the proposed change.

#### **6.1 Interface/Integration Dependencies**

Instructions: This section will provide detailed descriptions of people, process, and technology dependencies related to system(s) affected by the proposed change this should include an examination of important dependency considerations inside and outside of HCFA.

## **6.2 Interface/Integration Resources/Users**

Instructions: This section will provide descriptions of people, processes, and technologies affected by the proposed change this should include an examination of the users inside and outside of HCFA, STS considerations, and any applicable Interface Partners that could be impacted.

## **7 Impact Assessment**

Instructions: This section will capture the results of the impact assessment across the 4 levels of the HCFA enterprise architecture.

### **7.1 Business Architecture Impacts**

Instructions: This section should consider the business architecture impacts. Potential areas under consideration include business objectives, desired business results, business process flows, employee tasks and responsibilities.

### **7.2 Application Impacts**

Instructions: This section should consider the application architecture impacts. Potential areas under consideration include adherence to information systems security policies and procedures, duplicative application functionality assessment, legacy dependencies, integration points/techniques, and scheduling/resource commitments.

### **7.3 Technical Architecture Impacts**

Instructions: This section should consider the Technical Architecture impacts. Areas under consideration include deployment locations, external and internal interface integration, enterprise architecture standards compliance, use of common services.

### **7.4 Data Architecture Impacts**

Instructions: This section should consider the Data Architecture impacts. Areas under consideration include data values, data quality, data integrity, data protection mechanisms to prevent unauthorized access, approach to creation and deletion of data and information.

## **8 Definitions**

Instructions: This section will capture any definitions that are necessary to provide clarity for review of the business impact analysis.

## Appendix C.3: Interface Control Document

Interface Control Document	
<b>Name</b>	Interface Control Document
<b>Alias(es)</b>	Interface Design Document
<b>Objective</b>	The objective of an Interface Control Document is to document and track the necessary information required to effectively define the relevant system's interface.
<b>Definition</b>	<p>The Interface Control Document (ICD) is a comprehensive report of a system's interface. The ICD describes flow of data from one system to another. It describes the concept of operations, defines the governance of the data exchange, and identifies the communication paths of the expected data flow.</p> <p>At the highest level ICD describes:</p> <ul style="list-style-type: none"> <li>• Scope: describes the assumptions, constraints, and risks</li> <li>• General Interface Requirements: gives an overview of the interface, the functional allocation, data transfer, transactions, and security and integrity</li> <li>• Detailed Interface Requirements: details the assumptions, processing steps, processing time requirements, message format, communication methods, and security requirements of the interface</li> <li>• Qualification Method: defines the method used to verify the interface requirements</li> </ul> <p>At a lower level, the ICD describes the following attributes of the system interfaces:</p> <ul style="list-style-type: none"> <li>• Name – the interface name</li> <li>• Unique Identifier – what is used to identify the interface</li> <li>• Business Purpose – the purpose the interface serves (e.g. what data is being sent from the source to target systems)</li> <li>• Target System – details on the target system, including the name, agency that houses it, host hardware platform, operating system, application software, database, and support times.</li> </ul>

### Interface Control Document

- Target System Contact – the name and contact information for the target system contact.
- Source System – details on the target system, including the name, agency that houses it, host hardware platform, operating system, application software, database, and support times.
- Source System Contact – the name and contact information for the source system contact.
- Existence of MOU – whether a Memorandum of Understanding exists and if it needs to be re-formalized.
- Description of Use – explain how the interface will be used and the direction of information travel between the source and target systems.
- Frequency – how often the interface needs to run.
- Interface Mode – whether the interface is run real-time or batch.
- Interface Interaction Mode – interaction modes of the interface.
- Data Format – data format (flat file, XML, etc.)
- Audience – the users that can interact with, schedule, or monitor the interface.
- Data Conversion – whether the data needs to be converted before being introduced to the target system. If it does, include the expected volume of data to be converted.
- Limitations/Constraints – explains limitations or constraints that may affect the implementation of the interface.
- Legacy Artifact Reference - if the interface already exists, includes references to any documented data elements and data formats of the system in the appendix.
- Security – details on data sensitivity, access rights, and restrictions of the interface
- Special Processing – the high-level rules for including and excluding data from the interface
- System Screenshots – provides additional detail into the user interface and information that can be provided by the system.
- Functional Requirements Reference – references to the functional requirements related to the specific interface.
- Business Rules – references to the business rules related to the specific interface.
- Non-functional Requirements – references to the non-functional requirements related to the specific interface
- Data Requirements – references to the data requirements related to the specific interface.

<b>Interface Control Document</b>	
	<ul style="list-style-type: none"><li>• Conflicting Controls – identifies any conflicting controls that may affect the data flow between systems</li></ul>
<b>Sample</b>	A sample CMS Interface Control Document template is included in the following section.

## **Interface Control Document**

### **Table of Contents**

1	Purpose of Interface Control
2	Introduction
3	Overview
4	Scope
4.1	Assumptions
4.2	Constraints
4.3	Risks
4.4	Dependencies
5	General Interface Requirements
5.1	Interface Overview
5.2	Functional Allocation
5.3	Data Transfer
5.4	Transactions
5.5	Security and Integrity
6	Detailed Interface Requirements
6.1	Requirements for <Given Interface Name>
6.1.1	Assumptions
6.1.2	General Processing Steps
6.1.3	Interface Processing Time Requirements
6.1.4	Messaging Format and Required Protocols
6.1.5	Communication Methods
6.1.6	Security Requirements
6.2	Requirements for <Given Interface Name>
7	Qualification Methods
8	Reporting Expectations
Appendix A: Interface Controls	

Appendix B: Record of Changes

Appendix C: Acronyms

Appendix D: Glossary

Appendix E: Referenced Documents

Appendix F: Approvals

Appendix G: System Screenshots

## 1 Purpose

*Instructions: Provide the purpose of the Interface Control document. For example: This Interface Control Document (ICD) documents and tracks the necessary information required to effectively define the <Project Name> system's interface as well as any rules for communicating with them in order to give the development team guidance on architecture of the system to be developed. The purpose of this ICD is to clearly communicate all possible inputs and outputs from the system for all potential actions whether they are internal to the system or transparent to system users. This Interface Control is created during the Planning and Design Phases of the project. Its intended audience is the project manager, project team, development team, and Interface Partners interested in interfacing with the system. This ICD helps ensure compatibility between system segments and components.*

The intended audience of the <Project Name> Interface Control is all project stakeholders including the project sponsor, senior leadership, and the project team.

## 2 Introduction

*Instructions: Provide identifying information for the source and target systems participating in the interface, including system contacts in the event of an emergency. A separate paragraph should be included for each system that comprises the interface, providing sufficient description to definitively identify the systems participating in the interface. Also describe any security or privacy considerations associated with use of the ICD.*

This Interface Control Document (ICD) describes the relationship between the <Source System Name (Acronym)> (the source system) and the <Target System Name (Acronym)> (the target system).

This ICD specifies the interface requirements to be met by the participating systems. It describes the concept of operations for the interface, defines the message structure and protocols that govern the interchange of data, and identifies the communication paths along which the data are expected to flow.

For each interface, the following information will be provided:

- A general description of the interface;
- Assumptions where appropriate;
- A description of the data exchange format and protocol for exchange; and
- Estimated size and frequency of data exchange
- Key contacts and contact detail in the event of an emergency

### 3 Overview

*Instructions: Briefly describe the purpose of each interface to another external system at a functional level and the data exchanged between the interfaces. Further information on the functionality and architecture of the participating systems is given in the subsequent sections. In particular, each system should be briefly summarized with special emphasis on the functionality related to the interface. The hardware and software components of each system are also identified.*

Where applicable, make reference to any existing data sharing agreements and/or Memorandum of Understanding (MOU) currently in place or will be put in place.

### 4 Scope

#### 4.1 Assumptions

*Instructions: Describe any assumptions or dependencies regarding the interfaces of the system. These may concern such issues as: related software or hardware, operating systems, or end-user characteristics.*

#### 4.2 Constraints

*Instructions: Describe any limitations or constraints that have a significant impact on the system interfaces. Such constraints may be imposed by any of the following (the list is not exhaustive):*

- Hardware or software environment
- End-user environment
- Availability of resources
- Interoperability requirements
- Interface/protocol requirements
- Data repository and distribution requirements

#### 4.3 Risks

*Instructions: Describe any risks associated with the system interfaces and proposed mitigation strategies.*

#### 4.3 Dependencies

*Instructions: Describe any dependencies associated with the system interfaces.*

### 5 General Interface Requirements

#### 5.1 Interface Overview

*Instructions: Describe the functionality and architecture of the interfacing systems as they relate to the proposed interface. Briefly summarize the system, placing special emphasis on functionality, including identification of key hardware and software components, as they relate to the interface. If more than one external system is to be part of the interface being defined, then include additional sections at this level for each additional external system. Additionally, if the interface*

*already exists, includes references to any documented data elements and data formats of the system.*

## **5.2 Functional Allocation**

*Instructions: Briefly describe what operations are performed on each system involved in the interface and how the end users will interact with the interface being defined. If the end user does not interact directly with the interface being defined, describe the events that trigger the movement of information using the interface being defined.*

## **5.3 Data Transfer**

*Instructions: Briefly describe how data will be moved among component systems of the interface being defined. Include descriptions and diagrams of how connectivity among the systems will be implemented and of the type of messaging or packaging of data that will be used to transfer data among the systems. If more than one interface between these two systems is defined by this ICD, each should be identified in this section. A separate subsection may be included for each interface.*

Where applicable, make reference to any data conversion strategies in place. Additionally, identify any special processing rules that will be put into place for including and/or excluding data from the interfaces.

## **5.4 Transactions**

*Instructions: Briefly describe types of transactions that will be used to move data among the component systems of the interface being defined. If multiple types of transactions will be used for different portions of the interface, a separate section may be included for each interface.*

## **5.5 Security and Integrity**

*Instructions: If the interface defined has security and integrity requirements, briefly describe how access security will be implemented and how data transmission security will be implemented for the interface being defined. Include a description of the transmission medium to be used and whether it is a public or a secure line. Include a brief description of how data will be protected during transmission and how data integrity will be guaranteed. Include a description of how the two systems can be certain they are communicating with each other and not with another system masquerading as one of them. Describe how an individual on one system can be audited and held accountable for resulting actions on the other component of the interface. Normally, this section should be an overview of how security and integrity will be implemented.*

An interface that is completely self-contained, such as movement of data between systems resident in the same computer room, may not have any security requirements. In this case it should be so stated with an explanation of why the interface has no security and integrity requirements.

## **6 Detailed Interface Requirements**

*Instructions: This section specifies the requirements for one or more interfaces between two systems. This includes explicit definition of the content and format of every message or file that*

may pass between the two systems, and the conditions under which each message or file is to be sent. If an interface between the two systems is to be implemented incrementally, identify the Implementation Phase in which each message will be available. The structure in Section “Requirements for <Given Interface> should be replicated for each defined interface between the two participating systems.

The template contained in the section named Requirements for <Given Interface> (including subsections) provides a generic approach to interface requirements definition. The specific interface definition should include only subsections relevant to the interface being defined, and liberty may be taken in the organization of subsections under the section named the section named Requirements for <Given Interface>. Where types of information not specified in the section named Requirements for <Given Interface> are required to clearly define the interface, additional subsections should be added. Other readily available documents (such as data dictionaries, standards for commercial protocols, and standards for user interfaces) may be referenced instead of stating the information here. It may be useful to include copies of such documentation as appendices to the ICD. Where possible, the use of tables and figures is encouraged to enhance the understandability of the interface definition. In defining interface requirements, clearly state which of the interfacing systems the requirement is being imposed upon.

## 6.1 Requirements for <Given Interface Name>

*Instructions: Briefly summarize the interface for the name given above. Indicate what data protocol, communication methods, and processing priority are used by the interface. Data protocols may include messages and custom ASCII files. Communication methods may include electronic networks or magnetic media.*

Where relevant make reference to the functional, non-functional, data requirements, and/or business rule being satisfied and is related to the specific interface.

### 6.1.1 Assumptions

*Instructions: Identify any assumptions that specify organizational responsibilities for specific activities or decisions, or that defines specific constraints. Assumptions might include:*

- Data acceptance constraints
- Responsibility for establishing and managing the communication protocol
- Responsibility for providing and/or accepting file feeds for test and production processing
- Allowable file sizes
- Responsibility for decisions on acceptance of test results
- Conflicting Controls

### 6.1.2 General Processing Steps

*Instructions: Describe the daily, weekly, monthly, etc., and threshold processing. Discuss the process to be used to confirm successful file transmission. Identify steps to be taken if all records in a file are received and the steps to be taken if all records are not received. Identify the reports to be used to document the results of daily, weekly, monthly, etc., processing. Describe any*

*special processing that will be performed if a certain percentage (threshold) of the records is rejected.*

### **6.1.3 Interface Processing Time Requirements**

*Instructions: If information is required to be formatted and communicated as the data is created, as a batch of data is created by operator action, or in accordance with some periodic schedule, indicate processing priority. Requirements for specific messages or files to be delivered to the communications medium within a set interval of time should be included in Subsection named "Message Format (or Record Layout) and Required Protocols". State the priority that the interfacing entities must assign to the interface. Priority may be stated as performance or response time requirements defining how quickly incoming traffic or data requests must be processed by the interfacing system to meet the requirements of the interface. Considerable latitude should be given in defining performance requirements to account for differences in hardware and transaction volumes at different installation sites of the interfacing systems. Response time requirements, which are impacted by resources and beyond the control of the interfacing systems (e.g., communication networks) are beyond the scope of an ICD.*

### **6.1.4 Message Format (or Record Layouts) and Required Protocols**

*Instructions: Specify the explicit definitions of and the conditions under which each message is to be sent. Describe the definition, characteristics, and attributes of the command. Also document query and response descriptions.*

#### **6.1.4.1 File Layout**

*Instructions: This section should contain diagrams and short descriptions of both the header and detail layouts. This information may be included in an appendix to the document that is referenced here.*

#### **6.1.4.2 Data Assembly Characteristics**

*Instructions: Define the content and format of every message, file, or other data element assembly (records, arrays, displays, reports, etc.) specified in Subsection named "Message Format (or Record Layout) and Required Protocols". In defining interfaces where data is moved among systems, define the packaging of data to be utilized. The origin, structure, and processing of such packets will be dependent on the techniques used to implement the interface. Define required characteristics of data element assemblies that the interfacing entities must provide, store, send, access, receive, etc. When relevant to the packaging technique used, the following information should be provided:*

- Names/identifiers
- Project-unique identifier
- Non-technical (natural language) name
- Technical name (e.g., record or data structure name in code or database)
- Abbreviations or synonymous names
- Structure of data element assembly (e.g., field name, type, length, valid values, etc.)

- Visual and auditory characteristics of displays and other outputs (e.g., colors, layouts, fonts, icons, and other display elements, beeps, lights) where relevant
- Relationships among different types of data element assemblies used for the interface
- Priority, timing, frequency, volume, sequencing, and other constraints (e.g., whether the assembly may be updated and whether business rules apply)
- Sources (setting/sending entities) and recipients (using/receiving entities).

#### 6.1.4.3 Field/Element Definition

*Instructions: Define the characteristics of individual data elements that comprise the data packets defined in Subsection named “Data Assembly Characteristics”. Sections “Data Assembly Characteristics” and “Field/Element Definition” may be combined into one section in which the data packets and their component data elements are defined in a single table. Data element definitions should include only features relevant to the interface being defined and may include such features as:*

- Names/identifiers
- Project-unique identifier
- Priority, timing, frequency, volume, sequencing, and other constraints (e.g., whether the data element may be updated and whether business rules apply)
- Non-technical (natural language) name
- Technical name (e.g., variable or field name in code or database)
- Abbreviation or synonymous names
- Data type (alphanumeric, integer, etc.)
- Size and format (e.g., length and punctuation of a character string)
- Units of measurement (e.g., meters, dollars, nanoseconds)
- Range or enumeration of possible values (e.g., 0-99)
- Accuracy (how correct) and precision (number of significant digits)
- Security and privacy constraints
- Sources (setting/sending entities) and recipients (using/receiving entities)
- Validation rule(s)

If there is a need to reformat data before they are transmitted or after incoming data is received, include descriptions of the tools and/or methods for the reformatting process.

#### 6.1.5 Communication Methods

*Instructions: Communication requirements include all aspects of the presentation, session, network, and data layers of the communication stack to which both systems participating in the interface must conform. Document the specifications for hand-shaking protocols between the two systems. Include the content and format of the information to be included in the hand-shake messages, the timing for exchanging these messages, and the steps to be taken when errors are identified. The following subsections should be included in this discussion as appropriate to the interface being defined and may be supplemented by additional information as appropriate.*

##### 6.1.5.1 Interface Initiation

*Instructions: Define the sequence of events by which the connections between the participating systems will be initiated. Include the minimum and maximum number of conceptions that may be supported by the interface. Also include availability requirements for the interface (e.g., 24 hours a day, 7 days a week) that are dependent on the interfacing systems. Availability requirements beyond the control of the interfacing systems (e.g., network availability) are beyond the scope of an ICD.*

#### **6.1.5.2 Flow Control**

*Instructions: Specify the sequence numbering, legality checks, error control, and recovery procedures that will be used to manage the interface. Include any acknowledgement (ACK/NAK) messages related to these procedures. Address the format(s) for error reports exchanged between the systems and their disposition (e.g., retained in a file, sent to a printer, flag/alarm sent to the operator, etc.)*

#### **6.1.6 Security Requirements**

*Instructions: Specify the security features that are required to be implemented within the message or file structure or in the communications processes. Specify the security of the communication methods used (Include safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing). For interactive interfaces, security features may include identification, authentication, encryption, and auditing. Simple message broadcast or ASCII file transfer interfaces are likely to rely on features provided by communication services. Do not specify the requirements for features that are not provided by the systems to which the ICD applies. Specifically state if the interface relies solely on physical security or on the security of the networks and firewalls through which the systems are connected.*

Refer to the Control Artifact for a description of which security and privacy controls will be used by the systems. This artifact will show if there are any conflicting controls between the systems that will need to be addressed.

### **6.2 Requirements for <Given Interface Name>**

*Instructions: All of the applicable characteristics described in section “Requirements for <Given Interface>” should be replicated for each defined interface between the two participating systems. There is no limit on the number of unique interfaces that can be defined in a single ICD. In general, all interfaces defined should involve the same two systems.*

## **7 Qualification Methods**

*Instructions: This section defines a set of qualification methods to be used to verify that the requirements for the interfaces defined in Section “Detailed Interface Requirements” have been met. Qualification methods include:*

**Demonstration** – The operation of interfacing entities that relies on observable functional operation not requiring the use of instrumentation, special test equipment, or subsequent analysis.

**Test** – The operation of interfacing entities using instrumentation or special test equipment to collect data for later analysis.

**Analysis** – The processing of accumulated data obtained from other qualification methods. Examples are reduction, interpretation, or extrapolation of test results.

**Inspection** – The visual examination of interfacing entities, documentation, etc.

**Special Qualification Methods** – Any special qualification methods for the interfacing entities (e.g., special tools, techniques, procedures, facilities, and acceptance limits).

## 8 Reporting Expectations

*Instructions: It is the expectation of HCFA that the SI contractor will collect metrics during the interface integration development activities to assess the quality of the product under development and productivity based on schedule. This SI contractor will provide this information to the project team and program management for review and assessment of progress. The metrics to be provided are listed below and seek to provide transparency for interface integration activities as development progresses. Definitions and examples of the metrics are provided in Appendix D.*

**Error Discovery Rate** – The ratio of defects per test case

**Test Execution Coverage** – Measure of number of test case executed against the plan.

**Application Defect Density** - Defined as the ratio of defects to test case or the ratio of defects to effort

**Quality of Fixes** - Determines the quality of fix done by development team. This will also show how often previously working functionality was adversely affected by software fixes.

**Requirements Stability Index** – Provides indication on effectiveness of the Requirements gathering process. It's a comparison of change to requirements (added/ deleted/ modified) and the original requirements

**Test Design Coverage** - This is to measure the percentage of test case coverage against the number of test requirements.

**Appendix A: Interface Controls**

Utilize appendices to facilitate ease of use and maintenance of the ICD document. Each appendix should be referenced in the main body of the document where that information would normally have been provided.

Include a detailed description of the required interface controls below.

*OSI Application Layer Table*

Interface Type	Interface From	Interface To	Description of Interface	Other Information

*OSI Presentation Layer Table*

Interface Type	Interface From	Interface To	Description of Interface	Other Information

*OSI Session Layer Table*

Interface Type	Interface From	Interface To	Description of Interface	Other Information

*OSI Transport Layer Table*

<b>Interface Type</b>	<b>Interface From</b>	<b>Interface To</b>	<b>Description of Interface</b>	<b>Other Information</b>

*OSI Network Layer Table*

<b>Interface Type</b>	<b>Interface From</b>	<b>Interface To</b>	<b>Description of Interface</b>	<b>Other Information</b>

*OSI Data Layer Table*

<b>Interface Type</b>	<b>Interface From</b>	<b>Interface To</b>	<b>Description of Interface</b>	<b>Other Information</b>

*OSI Physical Layer Table*

<b>Interface Type</b>	<b>Interface From</b>	<b>Interface To</b>	<b>Description of Interface</b>	<b>Other Information</b>



**Appendix C: Acronyms**

Instructions: Provide a list of acronyms and associated literal translations used within the document. List the acronyms in alphabetical order using a tabular format as depicted below.

*Acronyms Table*

Acronym	Literal Translation
<b>CMS</b>	Centers for Medicare & Medicaid Services
<b>ICD</b>	Interface Control Document
<b>LDM</b>	Logical Data Model
<b>SDD</b>	System Design Document

**Appendix D: Glossary**

Instructions: Provide clear and concise definitions for terms used in this document that may be unfamiliar to readers of the document. Terms are to be listed in alphabetical order.

*Glossary Table*

Term	Definition

**Appendix E: Referenced Documents:**

Instructions: Summarize the relationship of this document to other relevant documents. Provide identifying information for all documents used to arrive at and/or referenced within this document (e.g., related and/or companion documents, prerequisite documents, relevant technical documentation, etc.).

*Referenced Documents Table*

Document Name	Document Location and/or URL	Issuance Date

**Appendix F: Approvals**

The undersigned acknowledge that they have reviewed the ICD and agree with the information presented within this document. Changes to this ICD template will be coordinated with, and approved by, the undersigned, or their designated representatives.

**Instructions:** List the individuals whose signatures are desired. Examples of such individuals are Business Owner, Project Manager (if identified), and any appropriate stakeholders. Add additional lines for signature as necessary.

**Appendix G: System Screenshots**

**Instructions:** provides additional detail into the user interface and information that can be provided by the system.

## Appendix D: Interface/Integration Acceptance Criteria and Metrics

The following section includes definitions and examples for potential criteria and metrics that interfaces/integration should be evaluated against.

### Error Discovery Rate – It is defined as the ratio of defects per test case

- **Objective:** The aim of this metrics is to determine the effectiveness of the test cases
- **When it should be measured:** It should be measured during Test Execution Phase.
- **Benefits:** Helps to determine effectiveness of the test cases. It is used to analyze build stability and support release decision, progress metric reported on a daily basis

Input/Measure	Formula	Example
1) Total no of Defects found 2) Total no of test cases or scripts executed	Total number of defects found in application /Number of test cases or scripts executed	Total no of Defects found = 100 Total no of test cases or scripts executed = 800 Error Discovery rate = $100/800 = 0.125$ Defects/Test cases

**Test Execution Coverage** – This metrics is useful to measure the number of test case executed against the plan.

- **Objective:** The objective of this metrics is to determine the coverage of testing.
- **When it should be measured:** It should be measured at Test Execution Phase.
- **Benefits:** This metrics is used as an indicator of coverage of testing.

Input/Measure	Formula	Example
1) Total Number of test cases or scripts executed 2) Total Number of test cases or scripts planned to execute	Total Number of test cases or scripts executed / Total Number of test cases or scripts planned to execute)*100	Total Number of test cases executed = 1100 Total Number of test cases planned to execute = 1080 Test Execution Coverage = $(1080/1100)*100 = 98.18$

**Application Defect Density** – Defined as the ratio of defects to test case or the ratio of defects to effort

- **Objective:** The aim of this metrics is to determine the application stability.
- **When it should be measured:** It should be measured build wise and end of Test Execution Phase
- **Benefits:** The module in which the defect density is high can be identified. It helps to know density of defects spread across the modules.

Input/Measure	Formula	Example
1) Total number of defects found in the application	(Total number of defects found in the	Total number of defects found in the application = 80
2) Actual Size (TCP/No of test cases executed for the release)	application /Actual Size (TCP/No of test cases executed for the release)	Actual Size (TCP/No of test cases executed for the release) = 1000 (Test cases) Application Defect Density = 80/1000 =.08

**Quality of fixes** - It determines the quality of fix done by development team. This will also show how often previously working functionality was adversely affected by software fixes.

- **Objective:** The aim of this metrics is to know the quality of a build in terms of defect fixing.
- **When it should be measured:** It should be measured during each build and end of Test Execution Phase
- **Benefits:** Quantitatively calculates the quality of bug fixing. Lower the percentage indicates the poor quality of defect fixes.

Input/Measure	Formula	Example
1) Total no of Fixed Defects	(Total no of Defects reported as fixed -	Total no of Fixed Defects = 100
2) Total no of reopened bugs	Total no. of reopened bugs) / (Total no of Defects reported as fixed +	Total no of reopened bugs = 10
3) Total no of new Bugs due to fix	Total no. of new Bugs due to fix)*100	Total no of new Bugs due to fix = 5 Quality Of Fix % =((100-10)/(100+5))*100 = 85.7 %

**Requirements Stability Index** - Gives indication on effectiveness of the Requirements gathering process. It's a comparison of change to requirements (added/ deleted/ modified) and the original requirements.

- **Objective:** This is used to measure the changes that are coming in (compared to the original requirements decided at the start of the project) during the course of the project. This measures the dimension of changes in terms of number of requests.
- **When it should be measured:** It should be measured at overall project level.
- **Benefits:** This can be factored into plan and rework effort and schedule for remaining phases/activities/modules. This helps to know how stable the requirements are.

Input/Measure	Formula	Example
1) Total no of Original Requirements	(Total no of Original Requirements +	Total number of Original Requirements = 50
2) Cumulative no of requirements changed (till date)	Cumulative no of requirements changed (till date) +	Cumulative number of requirements changed (till date) = 1
3) Cumulative no of requirements added (till date)	Cumulative no of requirements added (till date) +	Cumulative number of requirements added (till date) = 2
4) Cumulative no of requirements deleted (till date)	Cumulative no of requirements deleted (till date)) / (Total no of	Cumulative number of requirements deleted (till date) = 1
	Original Requirements	RSI = (50+1+2+1)/50 = 1.08

**Test Design (Mapping) Coverage** - This is to measure the percentage of test case coverage against the number of test requirements.

- **Objective:** The objective of this metrics to measure the functional coverage of test cases designed.
- **When it should be measured:** It should be measured during Test Design Phase.
- **Benefits:** This metrics is used as an indicator of quality of test design and used to improve test coverage.

Input/Measure	Formula	Example
1) Total number of baselined testable requirements mapped to test cases 2) Total number of baselined testable requirements	$\left( \frac{\text{Total number of testable requirements mapped to test cases or Scripts}}{\text{Total number of baselined testable requirements}} \right) * 100$	Total number of baselined testable requirements mapped to test cases = 1100 Total number of baselined testable requirements = 1080 Design Coverage % = $\frac{1080}{1100} * 100 = 98.18$