AHCA Florida Health Care Connections (FX)

T-4: Technical Management Strategy

Version: 400

Date: June 24, 2022

Author: The SEAS Vendor

Submitted To: AHCA FX Program Administration Team

Revision History

DATE	VERSION	DESCRIPTION	AUTHOR
4/15/2018	001	T-4 Technical Management Strategy Initial Draft Version	Rene Cabral, Steve Quante, Paul Moore
5/17/2018	002	T-4 Technical Management Strategy Revisions to Agency Review	Rene Cabral, Steve Quante, Paul Moore
5/24/2018	003	T-4 Technical Management Strategy Revisions for Final Draft	Steve Quante
5/25/2018	100	T-4 Technical Management Strategy baseline version	Sean Gibbs
5/24/2019	101	Annual Update including FX to MES, description of disaster recovery coordination role, audit log handling and strategy on use of form filling applications	Paul Moore, Som Khot, Mike Griffiths
8/14/2019	102	T-4 updates based on comments from AHCA	Paul Moore, Mike Griffiths, Steve Ruszkowski
8/21/2019	200	T-4 Technical Management Strategy approved deliverable refresh	Carol Williams
3/24/2021	201	T-4 Technical Management Strategy Annual Refresh	Prashant Zaveri, Steve Ruszkowski, Rob Bright
4/14/2021	202	T-4 Technical Management Strategy Annual Refresh – remediation/updates based on Agency review comments	Steve Ruszkowski
4/21/2021	250	T-4 Technical Management Strategy approved deliverable refresh	Carol Williams
5/20/2021	251	T-4 Technical Management Strategy deliverable draft refresh updates made: ▪ Removed recommendation that vendors have to deploy in the GovCloud ▪ Corrected that EDW and IS/IP are not currently hosted in the GovCloud	Steve Ruszkowski
6/10/2021	300	T-4 Technical Management Strategy deliverable refresh approved final	Carol Williams
5/24/2022	301	T-4: Technical Management Strategy Draft refresh updates: ▪ Added Section 3.2.7 *Internet Domain Technology* for assets access ▪ Added Section 4.3 *Defect Management* ▪ Updated Section 7.3 *Technical Principles for New Data Sources* in accordance with DET #533 to define the standard for ICD documents and that the ICD template is adopted as a formal standard ▪ Updated Section 11 *Appendices* with Appendix A	Mary Burgess Amelia McHenry Brandon Raab

DATE	VERSION	DESCRIPTION	AUTHOR
6/24/2022	400	T-4: Technical Management Strategy approved final	Carol Williams

Modifications to the approved baseline version (100) of this artifact must be made in accordance with the FX Artifact Management Standards.

Quality Review History

DATE	REVIEWER	COMMENTS
4/15/2018	Sean Gibbs	QA Submission Review
5/17/2018	Sean Gibbs	QA Submission Review
5/24/2018	Sean Gibbs	QA Submission Review
5/23/2019	Carol Williams	QA Submission Review
3/19/2021	Steve Ruszkowski	Conducted Peer Review
3/23/2021	Carol Williams	QA Submission Review
5/20/2021	Carol Williams	Conducted QA review
5/20/2022	Carol Williams	Conducted quality review

Table of Contents

Table of Exhibits

Table of Strategic Topics

SECTION 1 INTRODUCTION

1.1 BACKGROUND

The Florida Agency for Health Care Administration (AHCA or Agency) is adapting to the changing landscape of healthcare administration and increased use of the Centers for Medicare and Medicaid Services (CMS) Medicaid Information Technology Architecture (MITA) to improve the administration and operation of the Florida Medicaid Enterprise. The current Florida Medicaid Enterprise is complex; it includes services, business processes, data management and processes, technical processes within the Agency, and interconnections and touchpoints with systems necessary for administration of the Florida Medicaid program that reside outside the Agency. The future of the Florida Medicaid Enterprise integration is to allow the Agency to secure services that can interoperate and communicate without relying on a common platform or technology.

The Florida Medicaid Management Information System (FMMIS) has historically been the central system within the Florida Medicaid Enterprise; functioning as the single, integrated system for claims processing and information retrieval. As the Medicaid program has grown more complex, the systems needed to support the Florida Medicaid Enterprise have grown in number and complexity.

The Medicaid Enterprise System (MES) Procurement Project was re-named Florida Health Care Connections (FX) in the summer of 2018. FX is a multi-year transformation to modernize the current Medicaid technology using a modular approach, while simultaneously improving overall Agency functionality and building better connections to other data sources and programs.

1.2 PURPOSE

The purpose of the *T-4: Technical Management Strategy* (TMS) is to develop and establish the Agency's Technical Management Strategy. The TMS aligns with the MITA 3.0 Part III Technical Architecture - Chapter 2 Technical Management Strategy (MITA TMS) while prioritizing unique Agency requirements. The TMS is the product of current state discovery, stakeholder input, strategic analysis, program strategy, and direction about techniques and priorities to support overall improvement of Medicaid program outcomes.

The TMS document may contain paths to updated versions of documents and diagrams, referenced in the following sections of this document that resides in the FX Projects Repository (FXPR).

As per MITA guidance, the TMS will include the following content:

- Technical Management Approach
- Transformation Challenges
- FX Governance

- Current Technical Principles
- Technical Goals and Objectives
- Transition Plans
- State-specific MITA Additions

The primary audience for the TMS is state Health and Human Services (HHS) executives and lead architects.

1.3 SCOPE STATEMENT

The TMS provides technology guidance for the procurement, development, implementation, integration, and maintenance of FX technology systems and investments. The TMS works in alignment with the *T-1: Data Management Strategy* and other FX Strategic Enterprise Advisory Services (SEAS) Technology deliverables to support the business organizations implementation of the FX Strategic Priorities.

Technology strategy is a broad topic that could include almost any organizational asset other than people. The TMS provides guidance for FX projects in the following areas of technical architecture:

- Application Models and Frameworks
- Infrastructure and Hosting Supporting Applications and Systems
- Integration Technologies
- User Interface Consistency
- Transition from Existing System(s)
- Introduction of New Technologies
- Information Technology Security Standards

Exhibit 1-1: SEAS Technology Deliverables lists SEAS Technology deliverables that contain strategic direction and guidance in additional areas of technology.

SEAS TECHNOLOGY DELIVERABLE	DESCRIPTION
T-1: Data Management Strategy	Technology strategy focused on overall data strategy, conceptual data management vision and data governance approach
T-2: Information Architecture Documentation	Technology strategy documenting FX conceptual and logical data models
T-3: Data Standards	Technology strategy focused on FX Data Standards and data definitions
T-4: Technical Management Strategy	Technology strategy focused on platform and infrastructure to support modular implementation

SEAS TECHNOLOGY DELIVERABLE	DESCRIPTION
T-5: Technical Architecture Documentation	Technology strategy focused on application architecture within modular implementations
T-6: Technology Standards	Technology standards and communication and governance process for all technology standards
T-7: Design and Implementation Management Standards	Technology strategy focused on the design and system implementation life cycle
T-8: Enterprise Data Security Plan	Technology strategy focused on FX security considerations

Exhibit 1-1: SEAS Technology Deliverables

This iteration of this TMS deliverable discusses the technologies needed to achieve optimal sharing of the state's services and data with emphasis on the foundational capabilities of the Integration Services / Integration Platform (IS/IP) including Enterprise Service Bus (ESB), Enterprise Data Warehouse (EDW), Operational Data Store (ODS), Reporting Data Store (RDS), and Modular capability implementation. This document provides the Agency context, aligned with MITA, required for planning purposes.

1.4 GOALS AND OBJECTIVES

- Goal 1 - Establish the MITA compliant Florida Medicaid Technical Management Strategy.
  - Objective 1 – Define and document each of the core Technical Management Strategy areas for the Agency that aligns to the MITA standard as described in Section 1.3 Scope Statement.
  - Objective 2 – Use this deliverable as the key strategic Technical Management reference for future planning and solicitations as part of the Agency's modular implementation approach.
- Goal 2 - Provide a Technical Management Strategy that addresses the transformational challenges within the Agency while remaining aligned to the MITA Standard.
  - Objective 1 – Through discovery sessions and current state analysis identify the critical pain points within the Agency related to Technology Management.
  - Objective 2 – Recommend approaches, processes, technologies, and tools that provide a future vision for resolving the transformational challenges identified.

1.5 REFERENCED DOCUMENTS

Documents referenced to support the development of this plan include the following:

- Guidance for Exchange and Medicaid Information Technology (IT) Systems. CMS. 2.0
- MITA 3.0 Part III, Chapter 2 Technical Management Strategy

- MITA 3.0 Part III, Chapter 4 Technical Services
- The Open Group SOA Source Book, 7th Edition
- Rogers, E. (2003). Diffusion of Innovations. Free Press. 2018
- FX SEAS technical deliverables are available in the FXPR at FX Hub > Standards & Plans > Category: Technology:
  - T-1: Data Management Strategy
  - T-3: Data Standards
  - T-5: Technical Architecture Documentation
  - T-6: Technology Standards
  - T-6: Technology Standards, Attachment D: Technology Standards - Communication, Support, Compliance, and Compliance Reporting Procedures
  - T-8: Enterprise Data Security Plan
- FX SEAS deliverable *S-4: Strategic Project Portfolio Management Plan* is available in the FXPR at FX Hub > Standards & Plans > Category: Strategy

SECTION 2 ROLES AND RESPONSIBILITIES

This section identifies the roles and responsibilities for the primary stakeholders that maintain or use this document.

ROLE	RESPONSIBILITY
SEAS Vendor Technical Architect	▪ Identifies the technologies and related processes necessary to improve the FX. ▪ Proposes technology management solutions that align to MITA 3.0, State, and Agency specific Medicaid requirements. ▪ Reviews and proposes new emerging technologies to the Agency. ▪ Maintains the Agency Technical Management Strategy. ▪ Supports vendor procurements by providing information, extracts and details related to the Technical Management Strategy.
AHCA FX Technical Lead	▪ Coordinates the participation of Agency stakeholders that identify technical management strategy topics needing definition, decision or elaboration, review, and provide feedback on proposed technical management strategy topics. ▪ Communicates technical management strategy to AHCA FX Program Administration Team. ▪ Supports FX leadership communication to AHCA executive leadership. ▪ Approves communications between the SEAS Vendor and FX Stakeholder Organizations related to FX Technical Management Strategy.
FX Project Owners (SEAS, EDW, IS/IP, Agency, Module Vendors)	▪ Follows the strategic direction in the Technical Management Strategy in proposing, discussing, and implementing technology for the FX. ▪ When necessary, recommends technologies and solutions applicable to the implementation of FX projects that align to MITA 3.0 and the Technical Management Strategy.
FX Stakeholder Organizations	▪ Reviews and as appropriate may align technology solutions with FX technology standards, systems, and processes per the TMS to achieve the Agency's mission of *Better Health Care for All Floridians.*

Exhibit 2-1: Roles and Responsibilities

SECTION 3 TECHNICAL MANAGEMENT APPROACH

3.1 TECHNICAL MANAGEMENT APPROACH SUMMARY

The FX Technical Management Approach (TMA) uses a business-driven technology enabling strategy to help the Agency achieve its mission of *Better Health Care for All Floridians.*

The approach aligns to the industry direction of Everything-as-a-Service (EaaS). EaaS is an outcome-focused strategy that emphasizes delivery of results as opposed to dictating the process or mechanics of how work occurs. With the defined standards of performance, interoperability standards, and enterprise integration capabilities, each system, organization, or entire ecosystem can reuse services. The consistency and scalability provided through use of services technology provides large economic benefits in the delivery of healthcare services. Service based technology implementations are proven to promote reuse, scale more easily when compared to monolithic technology solutions, are less costly to support and enhance, and due to their modular design are less costly and disruptive to replace as technology changes.

There are many technology adoptions of EaaS:

- Data-as-a-Service (DaaS)
- Platform-as-a-Service (PaaS)
- Infrastructure-as-a-Service (IaaS)
- Software-as-a-Service (SaaS)
- Network-as-a-Service (NaaS)
- Identity-as-a-Service (IdaaS)
- Security-as-a-Service (SECaaS)

The TMS provides guidance for FX projects implementation of technology related to the above technology services. The context of the TMS is the to-be vision depicted in **Exhibit 3-1: Data Management Strategy Vision To-Be Diagram**. The diagram provides a conceptual overview of the FMMIS evolution to FX and data processing landscape of FX.

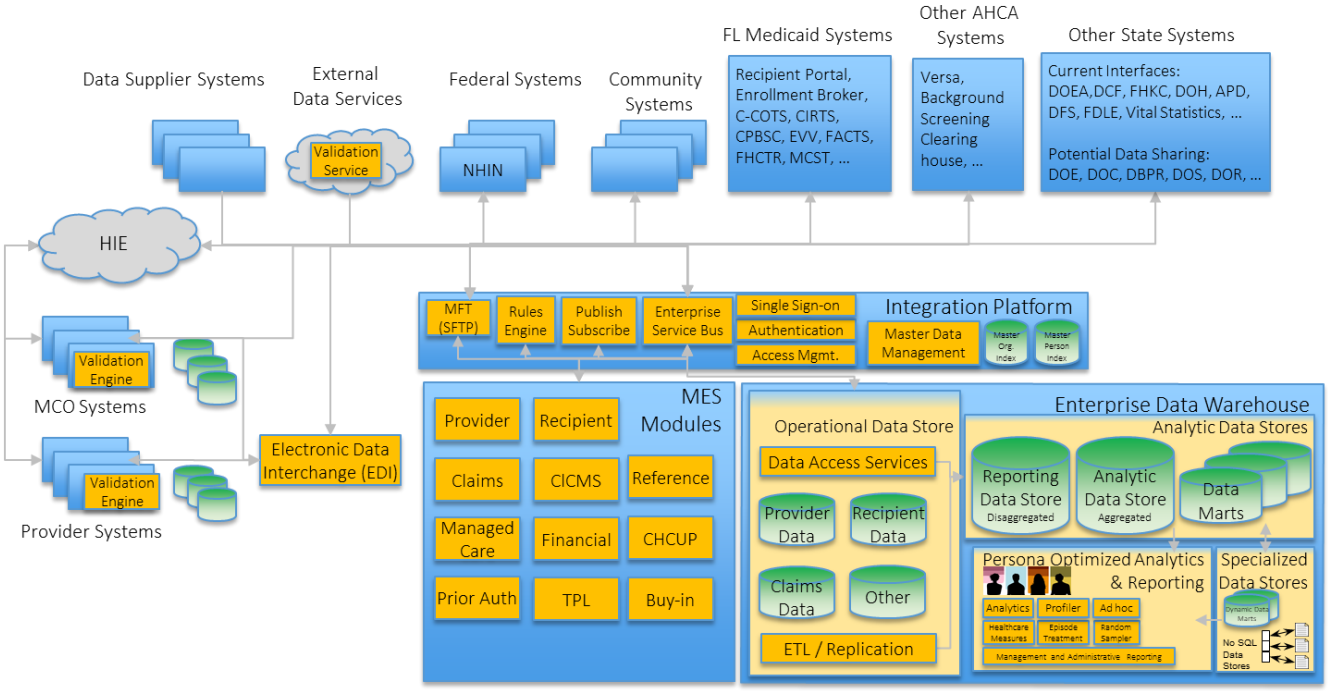

Exhibit 3-1: Data Management Strategy Vision To-Be Diagram

In the Agency's current landscape, FMMIS and other systems use technologies that are current within the last 10 years. Most applications and systems use a service-oriented architecture (SOA), communicate using extensible markup language (XML), and have web services that allow sharing and reuse. Likewise, several systems are implementing architectures that simplify replacement of commercial off-the-shelf (COTS) solution-based system software with flexible architectures. There are some small applications built with dated technologies more suitable for workgroup development (including Microsoft (MS) FoxPro, MS Excel, and others). Some of these small applications may not scale for use by the FX. The FX portfolio management process will evaluate potential FX projects to rewrite or industrialize any existing applications for FX use.

FX strategic priorities and CMS MITA guidance emphasize increasing technology maturity in data sharing, integration, and use of cloud infrastructure. A component of the FX Technical Management Strategy is to reduce proliferation of systems and copies of data. The approach is to enable people and systems to use the Integration Platform to access information in near real time from the authoritative source of truth system and data as opposed to replicating and copying data between systems using interfaces. From a technology platform and infrastructure perspective, the FX technical management strategy emphasizes use of scalable virtual infrastructure that provides redundancy, high availability, failover processing, and dynamic provisioning of capacity.

The FX Technical Management Approach emphasizes six primary technology management strategies that align with the overall FX strategic priorities:

- Enable a MITA aligned SOA through an Enterprise Service Bus
- Build modules from fine-grained modular business, technology, and data services exposed through standards-based application programming interfaces (APIs)
- Leverage a common User Interface (UI) framework and decoupled thin UI layer for all FX functionality
- Deploy cloud-ready modules, systems, and services in a Federal Risk and Authorization Management Program (FedRAMP) (recommended) authorized cloud. Less critical applications such as Agency information portals can leverage the public cloud. The IS/IP Vendor solution is implemented in the Oracle cloud and the EDW Vendor solution is implemented in the Amazon Web Services (AWS) cloud, both of which are FedRAMP compliant.
- Follow a *do no harm* business disruption strategy in the development and deployment of new modules
- Enable the application of new technologies

Enable a MITA aligned Service Oriented Architecture through an Enterprise Service Bus (ESB). Today, the Agency's system integration approach is primarily the exchange of files, custom data transformation processes, Secure File Transfer Protocol (SFTP), and some point-to-point system integration. As the technical landscape of the Agency becomes more complex, both internally and with a growing number of external system touch points, the current approach to system and data integration becomes increasingly more costly and complex. The FX strategy is to deploy an ESB which is an integration architecture that allows communication via a common communication layer between providers and consumers of data and services. Key functions of the ESB include message management, data management, service coordination, rules engine, single sign-on (SSO), and business logic which enable complex orchestration of services. The ESB, which has been implemented by the IS/IP Vendor, is a key enabler to allow the Agency greater integration possibilities with modern technologies across multiple vendors.

Build modules from fine-grained modular business, technology, and data services exposed through standards-based APIs. Today, with few exceptions, the Agency approach is to build and deploy purpose specific systems that are tightly coupled with proprietary data stores. Planning for or ability to reuse components or services is secondary. An exception to this is some of the more recent work completed by AHCA IT where focus was placed on designing and building reusable data and application services exposed through APIs. While these instances align directionally to the future state strategy, across the entire Agency code base, they are exceptions rather than the rule. The FX technology strategy is to design and build discrete services that provide independent functionality. Discrete independent services promote reuse, more flexibility in targeted application scaling, are easier to reliably test, promote test automation, and are less costly to maintain over time. As part of module implementation, discrete services allow development of more intelligent composite services to provide additional system functionality to the Agency. To ensure compliance with health care industry standards, the Fast Healthcare Interoperability Resources (FHIR) will be used as the format for data exchange within the APIs.

Leverage a common UI framework and decoupled thin UI layer for all FX functionality. Today, interChange, the FMMIS user interface built by the current fiscal agent, Gainwell Technologies, is the Agency's primary operations portal with common branding uniting the recipient portal, provider portal, and the operations user interfaces. While interChange does provide some commonality in user interface across FMMIS, the UI is not decoupled and therefore not easy to modify or replace. Some Non-FMMIS Agency systems have a different look, feel, and functionality further complicating the user experience within the Agency. The FX strategy is to describe and deploy a common unified UI framework that defines look and feel consistency, accessibility standards, naming conventions, field validations, JavaScript usage guidelines, security guidelines, interaction guidelines, etc. The implementation of single sign-on functionality by the IS/IP Vendor will also improve the consistency of the user interface when authenticating to FX applications. All new modules and systems will use the new common UI framework with a bias towards greater future use across all AHCA systems.

Deploy cloud ready MMIS modules in the FedRAMP authorized cloud. Less critical applications such as Agency information portals can leverage the public cloud. Today, the Agency's hosting strategy uses multiple hosting providers. FMMIS uses a third-party administrator (TPA) provided data center in Orlando, FL. AHCA IT systems and applications use the Department of Management Services Division of State Technology data center. Office 365 uses Azure Government for hosting. The hosting of Agency applications is increasingly technology restrictive, costly, and unaligned with industry hosting trends and capabilities toward use of cloud-based infrastructure. The FX strategy recommendation is to deploy new MMIS modules in a FedRAMP authorized cloud. FedRAMP is a government-wide program that provides a standardized approach to the security assessment, authorization, and continuous monitoring for cloud products and services providing a safe cloud-based hosting option for critical government systems which contain sensitive information. Agency applications with public information or information that is not sensitive can deploy using a public cloud provider. Regardless of hosting location, an important tenet of the Agency's modular strategy is specifying that all vendor solutions should be cloud-ready even if deployed in a traditional centrally hosted environment.

Follow a "do no harm" business disruption strategy in the development and deployment of new modules. The processing of Medicaid claims and payment of healthcare vendors represents almost 30% of the State's spending. The FX modernization strategy is to use technology selection, design, testing, implementation, and operation techniques that prevent avoidable disruption to the core mission of the Agency. This means processing in the new and legacy system both must work together to provide seamless operation during the transition. Components of FMMIS will remain operational while being incrementally replaced with modules, systems, and services resulting in a hybrid environment throughout the duration of the migration. To recipients, providers, and health plans, their interactions with the Agency should appear the result of a single cohesive system. This strategy means designing, developing, and implementing in a way that prevents having different inconsistent versions of data presented in different systems, producing duplicate correspondence or not providing correspondence, denying duplicate transactions, or showing duplicated or inaccurate information on portals or reports.

Enable use of new technologies. The FX strategy is to enable the adoption of new technologies. For example, use of artificial intelligence bots, machine learning, real-time natural language processing, and advanced predictive analytics are increasing in health care and other industries. By establishing a standards-based framework for interoperability, the FX can adopt new technologies quickly and at lower cost.

Exhibit 3-2: FX Technical Management Approach depicts the primary technology management strategies that make up the FX Technology Management.

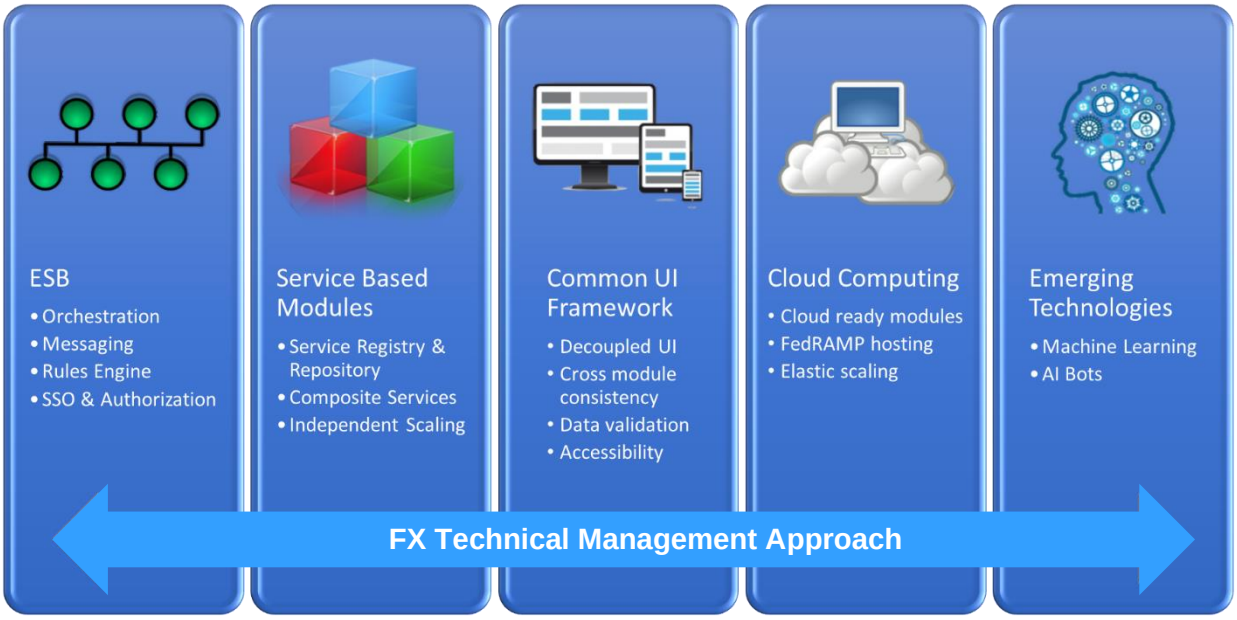

Exhibit 3-2: FX Technical Management Approach

Exhibit 3-3: Technical Management Approach Benefits Mapping shows each technical management approach benefit mapped to the five objectives of the Technical Management Approach in **Exhibit 3-2: FX Technical Management Approach**.

Technical Management Approach Benefits	Objectives				
	Enterprise Service Bus (ESB)	Service Based Modules	Common UI Framework	Cloud Computing	Emerging Technologies
Promote reuse	✓	✓	✓	✓	
Reduce support and enhancement cost		✓	✓		
Reduce copies of data		✓			
Improve integration of disparate technologies	✓				
Increased flexibility in application scaling		✓		✓	
Virtual hot site, and rapid deployment		✓		✓	
Promote test automation		✓			
Environment elastic scaling as needed		✓		✓	
Consistency in experience across modules		✓	✓		
Module redundancy, high availability, and failover		✓		✓	
Maximize fraud prevention				✓	✓
Improve recipient care by detecting important patterns in recipient data				✓	✓

Exhibit 3-3: Technical Management Approach Benefits Mapping

3.2 Technical Management Strategy

The TMS identifies mature and emerging technologies and standards and protocols that aid the sharing of data and application services. The TMS also discusses the prioritization of activities based on business need and business value. The resulting TMS Approach enables the development efforts of many organizations to contribute to the target technical management environment.

The TMS will focus on the following:

- Enterprise Service Bus (ESB)
- Performance Management Validation
- Application Logging
- Information Technology Security Standards
- Cloud Computing
- Common UI Framework
- Use of Form Filling User Interface
- Standards and Technology Maturity
- COTS Usage
- Activity Prioritization
- Technical Service Availability Strategy

3.2.1 ENTERPRISE SERVICE BUS (ESB)

The ESB provides a communication system where software applications interact in a service-oriented architecture (SOA). The SOA is an organization-wide, shared, reusable service model used by all applications integrated using the ESB. Software applications integrated in this manner provide data and processing through web services. The ESB performs message management, service authorization and access control, availability management, usage and cost accounting, and service coordination for complex orchestration of services.

The ESB is a key architectural piece of the FX TMS and future key enabler of the MITA SOA. The ESB decouples the network design from the underlying platform and allows the Agency greater integration possibilities with modern technologies across multiple vendors, multiple platforms (e.g., cloud, COTS), and supports the Agency's EaaS approach. The ESB also supports the approach by enabling near real time information sharing between applications. This reduces the need for nightly batch interfaces that replicate large amounts of information between systems. The ESB simplifies integration complexity and enhances standardization by performing the most complex and challenging aspects of interoperability with common architecture. Specifically, the ESB can enforce and support transformation of message vocabulary and data formats between systems to a standard consistent vocabulary. When messages are in or transformed to a standard vocabulary, the ESB can perform fine grained access controls based on many characteristics including content values. The ESB can enforce security policy to mask data values (e.g., SSN) or filter entire message content based on policy. These and many other capabilities enable the vision of secure data sharing and service reuse that will reduce the duplication of data and increase the timeliness and accuracy of information. The IS/IP Vendor has implemented their ESB solution using the Oracle Service Bus software.

3.2.2 PERFORMANCE MANAGEMENT VALIDATION

Performance Management (PM) includes activities to confirm systems and FX Project Owners consistently meet performance goals in an effective and efficient manner. These activities should adhere to the CMS document Guidance for Exchange and Medicaid Information Technology (IT) Systems (IT Guidance):

- Ensure quality, integrity, accuracy, and usefulness of functionality and information
- Provide timely information transaction processing, including maximizing real-time determinations and decisions
- Ensure systems are highly available and respond in a timely manner to Agency requests

The MITA Framework provides guidance for a basic three-tier performance monitoring structure, which the Agency will use in its expression of Performance Management:

- Performance Standard - A management-approved expression of the performance threshold(s), requirement(s), or expectation(s) that CMS expects States to meet to appraise at a particular level of performance.
- Performance Measure - Based on established Performance Standards and tracks past, present, and future business activity.
- Performance Metric - A measure of an organization's activities and performance also known as a Key Performance Indicator (KPI). Often closely tied in with outputs, performance metrics usually encourage improvement, effectiveness, and appropriate levels of control.

The technical requirements for technology procurements should specify performance metrics. Performance validation occurs at different stages of the delivery of the technology. Prior to system integration, modules must pass standard development testing such as unit tests, functional tests, end-to-end tests, stress tests, etc. After successful module or system specific testing, modules should pass integration and specification testing in a staging environment.

Systems, applications, and modules brought into the Agency should have standards-based mechanisms that allow data collection on performance such as log files, service-based status indicators, log or service-based usage statistics, etc.

In modern distributed systems, it is common practice to use System Performance Monitoring Tools to monitor, aggregate, analyze, and perform actions based on system events or transactions. The IS/IP Vendor selected, implemented, and operates the performance monitoring software – Oracle Enterprise Monitoring (OEM). The monitoring software will centralize performance and monitoring for all software systems in the enterprise.

When new systems, applications, or modules are deployed into the production environment they should be connected in a way that allows monitoring and alerting on any metric defined in the performance standards pertinent to that system, application, or module.

The modern Software Monitoring System, OEM includes the following features to enable continuous performance validation:

- Monitoring
- Alerting
- Dashboards
- Visualizations
- Reporting

3.2.3 APPLICATION LOGGING

Application logging is the practice of recording information about an application's behavior and storing the information to a target data store for later review. This section shares guidance on application logging practices, application logging frameworks, and use of application logging levels to improve IT operations and application performance. Application logging is also a necessary system requirement for a number of public sector auditing levels. Application logs are to be made available for certain audit requests and investigations. The system administrators are responsible to monitor the logs on a regular basis. Given the large amount of log data generated by the systems, log monitoring and auditing software is employed that uses rules to automate the review of these logs. The software points out events that might represent actions, problems, or threats. Reports generated from the log monitoring and auditing software can be used to support audit requests or investigations. This software is further discussed below in Section 3.2.3.4.

3.2.3.1 APPLICATION LOGGING PRACTICES

Most of the application logging framework vendors provide best practices for application logging. Below is a brief set of highlights of application logging guidance:

- Use formatted data / clear key-value pairs – A powerful feature of most monitoring tools is the ability to extract fields from events when searching, creating structure out of unstructured data. To make sure field extraction works as intended, use the following string syntax (using spaces and commas is fine):

  key1=value1, key2=value2, key3=value3 . . .

  Wrap values that contain spaces in quotes (for example, username="bob smith").

- Create human readable events – Avoid using complex encoding that would require lookups to make event information intelligible. For example, if logs are in a binary format, provide tools to easily convert them to a human-readable (American Standard Code For Information Interchange [ASCII]) format. Don't use a format that requires an arbitrary code to decipher it. Don't use different formats in the same file—split them out into individual files instead.

- Use timestamps for every event – The correct time is critical to understanding the proper sequence of events. Timestamps are critical for debugging, analytics, and deriving transactions.
- Use the most verbose time granularity possible – Put the timestamp at the beginning of the line. The farther you place a timestamp from the beginning, the more difficult it is to tell it's a timestamp versus other data. Include a four-digit year. Include a time zone, preferably a GMT/UTC offset. Time should be rendered in microseconds in each event. The event could become detached from its original source file at some point, so having the most accurate data about an event is ideal.
- Use globally unique identifiers (GUIDs) – Unique identifiers such as transaction IDs and user IDs are tremendously helpful when debugging, and even more helpful when you are gathering analytics. Unique IDs can point you to the exact transaction. Without them, you might only have a time range to use. When possible, carry these IDs through multiple touch points and avoid changing the format of these IDs between modules. That way, you can track transactions through the system and follow them across machines, networks, and services.
- Log in text format – Avoid logging binary information because monitoring software cannot meaningfully search or analyze binary data. Binary logs might seem preferable because they are compressed, but this data requires decoding and won't segment. If there is a need to log binary data, place textual meta-data in the event to enable search. For example, don't log the binary data of a JPG file, but do log its image size, creation tool, username, camera, GPS location, and so on. If binary data absolutely must be logged, store it in an accessible location and provide a link in the log to the file.
- Use developer-friendly formats – Developers like the ability to receive a stream of data over HTTP/S when possible, and with data structured so that it can be easily processed.
- Log more than just debugging events – Put semantic meaning in events to get more out of the data. Log audit trails, what users are doing, transactions, timing information, and other relevant information. Log any information that can add value when aggregated, charted, or further analyzed. In other words, log anything that is interesting to the business.
- Use application logging severity categories – Categorize the event. For example, use the application logging severity values described below (e.g., INFO, WARN, ERROR, and DEBUG).
- Identify the source – Include the source of the log event, such as the class, function, or filename.
- Minimize creation of multi-line events – Multi-line events generate a lot of segments, which can affect indexing and search speed, as well as disk compression. Consider breaking multi-line events into separate events.

3.2.3.2 APPLICATION LOGGING FRAMEWORK

An application logging framework is a utility specifically designed to standardize the process of logging in applications. Examples of widely used third-party logging frameworks are log4j for java applications, or log4net for .NET applications. The application logging framework helps standardize the solution by taking care of the logging for developers, exposing a standard API. FX applications are to use an industry standard application logging framework appropriate to the programming language of the application.

The application logging framework APIs are frequently invoked making it important that calls to the application logging framework don't reduce the application's performance. Consider using a logging facade pattern such as SLF4J to enable changing the logging framework in future without the need to change source code.

Applications are to use the logging framework to provide formatted information that can be filtered and parsed to enable machine-based monitoring and review.

Many cloud providers are providing application logging frameworks integrated to their cloud application and infrastructure services.

Examples of acceptable application logging frameworks include:

- Java Applications – Log4j 2.x, Logback
- .NET Applications – Log4net, Serilog
- Software as a Service Applications – Loggly
- Browser-bunyan for front end browser logging

FX Project Owners shall disclose and confirm approval of use of an acceptable application logging framework with the Agency.

3.2.3.3 APPLICATION LOGGING LEVEL

Applications are to generate logging event requests that can be use the application logging levels to support development, debugging, analysis, and operation of application processing. Application logging levels are labels assigned based on severity that can be used to categorize log entry events and filter to accelerate action. During runtime, the application code will make logging requests, which have a logging level. The logging framework will evaluate the log level configured and if the logging request level is at the configured level or higher, the entry gets logged. Logging requests at levels lower than the requested logging level are not logged to the target. The logging levels from highest to lowest are:

- ALL
- TRACE
- DEBUG

- INFO
- WARN
- ERROR
- FATAL
- OFF

For example, if the logging framework level is set to INFO, requests with any of the levels INFO, WARN, FATAL, and ERROR will be logged and logging requests with other logging levels are not logged.

Below are standard logging levels that can be specified for application logging:

- **ALL –** This level is the highest level and includes all other levels. With this level everything is going to be logged including custom logging levels that you may have defined.
- **TRACE –** This level provides log entries in a way that is used for detail analysis and problem solving. This level is rarely used in production environments because of the high consumption of resources.
- **DEBUG –** The DEBUG level is primarily used to provide very detailed information for developers to perform diagnostics on the application.
- **INFO –** The INFO level records entries about routine application operation. This logging level represents the mundane, everyday usage of the application and are used to understand user behavior and gather usage statistics.
- **WARN –** The WARN level designates potentially harmful occurrences. This logging level is for entries that could indicate a potential problem.
- **ERROR –** The ERROR level denotes a serious problem that has to be dealt with.
- **FATAL –**The FATAL level, designates a really serious error event. In most situations, when a fatal event happens, the application should be aborted immediately to prevent more serious damage from happening.
- **OFF –** With this level, nothing gets logged at all.

3.2.3.4 APPLICATION LOGGING STORAGE

Active application logs are written to application server storage. Most application log files will be in the format of flat files or formatted logging framework files. The IS/IP Vendor selected, implemented, and operates Splunk as the enterprise application logging solution. The enterprise security information and event management (SIEM) solution, Splunk, will access application log files from the application server source location and load application log content into the SIEM solution. The SIEM solution will provide the user interface to access event information, correlate events, and automation of analysis of application log content. After application logs on application server storage reach specific sizes the application server will switch to writing to a different file with different version number or timestamp. Application log

files that have been pulled into the SIEM tool are archived and removed from application server storage based on the applicable archive criteria for the application.

3.2.4 Information Technology Security Standards

IS/IP, EDW, and module vendors need to adhere to the security requirements, processes, policies, and standards of the FX and state statutory and Rule requirements. FX security standards reside in the Technology Standards Reference Guide located in the FXPR at FX Hub > Reference Materials > Category: Technology > Technology Standards (T-6) > Technology Standards Reference Guide (TSRG). Once in the Technology folder select *T-6 Technology Standards* to view the TSRG document. A comprehensive description of the FX Security Standards is contained in the *T-8: Enterprise Data Security Plan* located in the same document library in the FX Hub. The TSRG is a repository of standards relevant to technology components that identifies and prioritizes the relevance of specific technology standards in the enterprise. FX technology standards entries, categorized in the security area of the TSRG, provide transparency to required security standards applicable to FX projects and describes the standards compliance approach used to confirm the implementation of security standards. The TSRG is an important tool to document and govern relevant standards and provide clear communication between the Agency and vendors.

3.2.5 Cloud Computing

This section provides significant background, definition, and context about cloud computing. Section 3.2.5.7 *Cloud Adoption Strategy* summarizes the FX direction related to adoption of cloud technologies.

The Executive Order *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* issued May 11, 2017, reinforces the directive to use shared IT services for federal systems, including a cloud-first approach where possible. This aligns with the overall industry's move to hosting platforms, infrastructure, and software as services within both privately and publicly accessible cloud environments.

Cloud computing is a model which enables dynamically scalable resources to be provisioned as services over a network. These resources can be networks, servers, storage, applications, services, platforms, datacenter infrastructure, etc. Cloud computing infrastructure is a combination of hardware and software. Cloud Computing is enabled by two key technologies: service-oriented architecture (SOA) and virtualization technologies.

3.2.5.1 Characteristics of Cloud Computing

According to the National Institute of Standards and Technology (NIST) Definition of Cloud Computing (DCC), cloud computing infrastructure enables five key characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. **Exhibit 3-4: NIST DCC Five Cloud Key Characteristics**.

CHARACTERISTIC	DESCRIPTION
On-demand Self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
Broad Network Access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick recipient platforms (e.g., mobile phones, tablets, laptops, and workstations).
Resource Pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
Rapid Elasticity	Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the used service.

Exhibit 3-4: NIST DCC Five Cloud Key Characteristics

3.2.5.2 CLOUD COMPUTING DELIVERY MODELS

The NIST DCC was authored in 2011 and describes three delivery models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Server-less computing is a new delivery model which became publicly available in 2014 and has been added to the models list. Detailed descriptions are provided in **Exhibit 3-5: NIST DCC Four Cloud Delivery Models**.

DELIVERY MODEL	DESCRIPTION
SaaS	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various recipient devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

DELIVERY MODEL	DESCRIPTION
PaaS	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
IaaS	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Server-less	Server-less computing relies on the infrastructure vendor to manage capacity planning and management of the underlying servers. Server-less computing offerings range from application engines that run custom code functions to data warehousing, analytics, and machine learning. The benefits of a server-less architecture include reduced management from not having to administer servers, and a true pay-as-you-go model that only bills users for the resources used to run their functions and does not charge them for idle time.

Exhibit 3-5: NIST DCC Four Cloud Delivery Models

3.2.5.3 CLOUD COMPUTING DEPLOYMENT MODELS

The NIST DCC identifies four deployment models for cloud infrastructure: private, community, public, and hybrid.

- **Private Cloud** – In this model the consumer organization has exclusive access to and usage of the cloud infrastructure. The deployment can be on-site or outsourced to a third-party provider.
- **Community Cloud** – This deployment is a multi-tenant version of private cloud that supports a community of consumers with a shared mission, objectives, security, privacy, and compliance policy. The deployment can be on-site or outsourced to a third-party provider.
- **Public Cloud** – This deployment is cloud infrastructure made available to the public over a public network and managed by the provider.
- **Hybrid Cloud** – This deployment model uses two or more distinct cloud infrastructure deployments. Although these deployments remain unique entities, they are connected. The FX Project Owner orchestrates use of services and resources for the deployment models used in the solution.

3.2.5.4 CLOUD COMPUTING CONSIDERATIONS

The considerations in deciding where to use cloud technology in the enterprise are security, privacy, and performance. Adopting cloud technology means giving control over several issues that may affect any of these aspects. The State of Florida has mandated by section 282.206, *Florida Statutes*, a *cloud-first* initiative in 2019, which considers cloud solutions first in new system, or solution architecture.

The planned FX includes the Enterprise Service Bus (ESB), Enterprise Data Warehouse (EDW), Operational Data Store (ODS), Reporting Data Store (RDS) and Application Modules (AM).

Implementing the FX infrastructure in a private or community cloud on startup would enable the Agency to retain some of the benefits of on-premises infrastructure like data privacy, predictable latency, and isolation. Private cloud deployment of the FX infrastructure will also benefit from cloud infrastructure features like elastic resource allocation and node clustering. The ESB infrastructure is most effective when there is low network latency communication between the ESB and the highest volume data sources (e.g., operational data) and services.

3.2.5.5 THE FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FEDRAMP)

FedRAMP is a government-wide program that provides a standardized approach to the security assessment, authorization, and continuous monitoring for cloud products and services. The General Services Administration, as the federal government's generic authority for management of information technology policy and practices across civilian agencies, is responsible for implementation of FedRAMP.

FedRAMP uses a *do once, use many times* framework that reduces cost, saves time, and staff resources required to conduct redundant agency security assessments. Where the Agency requirements and mission needs support the use of specific cloud services (IaaS, PaaS, or SaaS), services with a current FedRAMP authorization should be included in the total set of products and services evaluated. The potential for cost reduction, which includes meeting baseline security requirements, should be addressed in the Agency IT procurement guidance.

The Government Accountability Office (GAO) has described the purposes of FedRAMP to be:

- Ensure that cloud-based services have adequate information security
- Ensure FedRAMP supports all needed security control baselines to match security requirements to risk
- Eliminate duplication of effort and reduce risk management costs
- Enable rapid and cost-effective procurement of information systems/services for federal agencies

Additionally, continuous monitoring provides risk visibility into and across FedRAMP approved services while assisting Cloud Service Providers (CSP) to maintain secure baselines over time. This also provides a risk framework that could identify and report security breaches.

There are two types of FedRAMP authorizations: Provisional Authority to Operate (P-ATO), which is issued by the Joint Authorization Board (JAB), and an Agency Authority to Operate (ATO), which is issued by the Agency planning to use the Cloud Service. A JAB P-ATO is not a risk acceptance, but an assurance to Agencies that the risk posture of the system has been reviewed and approved by federal agencies such as Department of Defense (DoD), Department of Homeland Security (DHS), and General Services Administration (GSA). Each Agency planning to use the Cloud Service Offering (CSO) reviews and issues their own ATO, which covers their Agency's use of the cloud service. More information is available at the FedRAMP official website.

Although the full participation in the FedRAMP program is designed for federal agencies, state agencies can use the FedRAMP JAB P-ATO as an assurance that the risk posture of the system has been reviewed and approved by DoD, DHS, and GSA. The JAB will only authorize multi-tenant clouds (public, hybrid, and community), and not private cloud.

The Agency's cloud strategy recommendation is to favor CSPs that have obtained a FedRAMP JAB P-ATO.

3.2.5.6 CLOUD FOR GOVERNMENT

A Government-only cloud or Cloud for Government demonstrates that the CSP has a dedicated, physically isolated cloud environment instance designed specifically to meet government requirements and serve only public-sector tenants. This service is usually a configuration of the hybrid cloud model.

Exhibit 3-6: FX Future State Cloud Adoption depicts the FX future state cloud adoption layout.

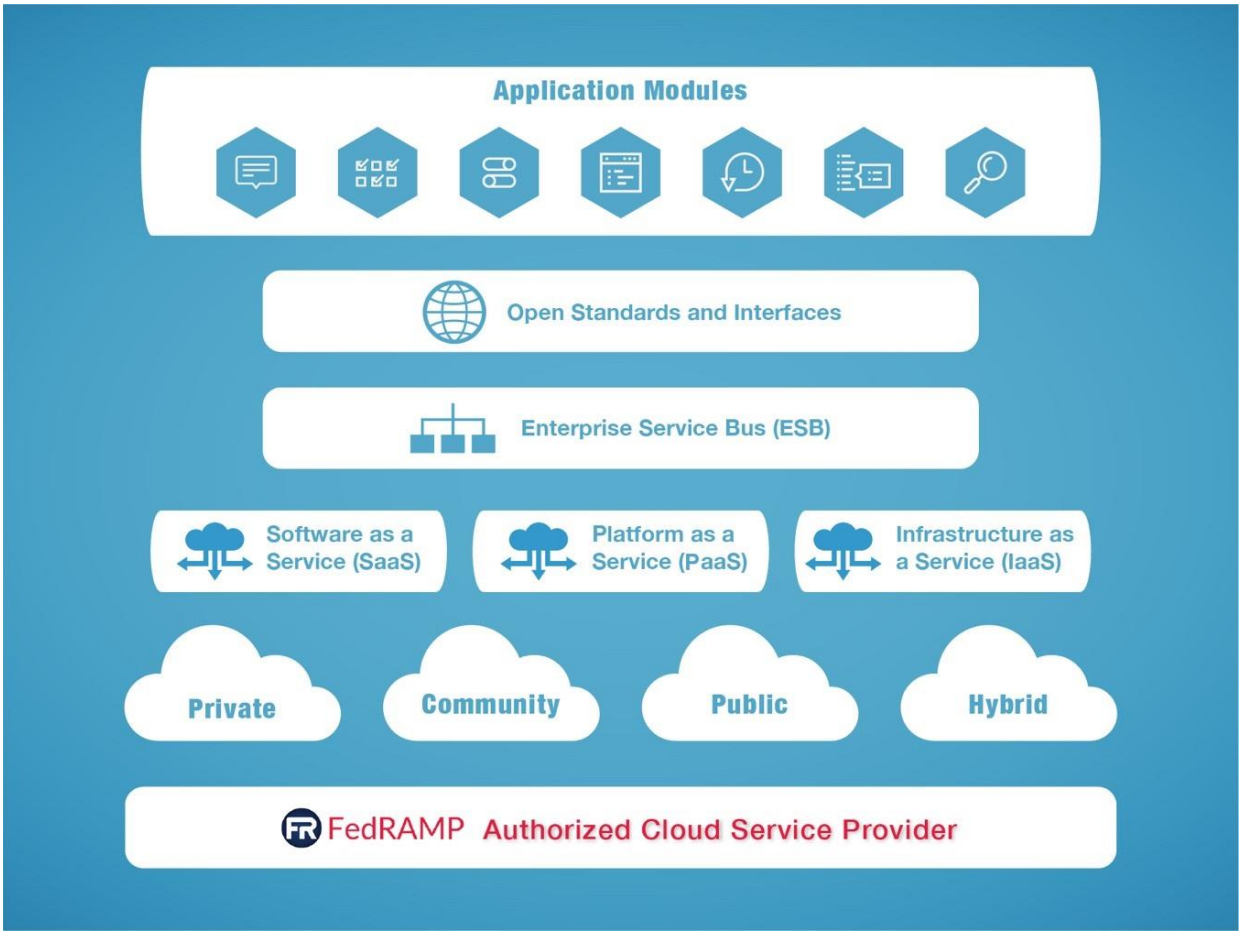

Exhibit 3-6: FX Future State Cloud Adoption

3.2.5.7 CLOUD ADOPTION STRATEGY

The cloud adoption strategy defines the acceptable use of cloud for modules and systems. The cloud adoption strategy defines the recommended future state and maps the progression from the current state. Through the progression toward the future state, the enabling foundations incrementally develop capability and maturity for realization of the future state.

Strategic Topic 3-1: FX Infrastructure Cloud Computing Adoption describes the recommended hosting strategy direction for the FX Infrastructure (ESB, EDW, RDS, ODS, and Application Modules) and its context with the existing FMMIS.

CLOUD ADOPTION LEVEL	TIMELINE				
	Current	2018	2020	2022	2025
On Premise					

DMS Division of State Technology Hosted	Non-FMMIS	->			
Fiscal Agent Data Center	FMMIS	->	->	->	Not Used
Vendor Hosted					
State Private Cloud					
FedRAMP			IS/IP, ODS, RDS, EDW, App Modules, Non-FMMIS	->	
Public Cloud			App Modules, Non-FMMIS, Dev Environments using non-sensitive data	->	

ANALYSIS

The FX cloud strategy is a Cloud first strategy where new and replacement components of the FX that replace FMMIS are implemented using cloud infrastructure. A reliable low latency network connection between IS/IP and FMMIS infrastructure is needed to provide acceptable performance for data requests from or to the existing FMMIS via the integration platform. As the use of data services begins to shift from FMMIS to the EDW and ODS solutions, the reliable low latency network connections between the IS/IP, EDW, and ODS will be important. The ESB infrastructure is most effective when there is low network latency between the ESB and highest volume data sources (EDW, ODS). The cloud exchange software, Equinix, was procured and facilitates low latency network connections between systems hosted in various cloud implementations.

During the transition away from FMMIS, the speed of data replication between FMMIS and the ODS plays a key enabling role. The tight data dependency between the systems requires that they both have access to current data. The replication speed should be fast enough to not be disruptive to the operations of FMMIS. Geographical proximity and fast reliable low latency networks are key enablers of near-real-time replication.

The recommended future state is deployment in a FedRAMP authorized cloud for mission-critical applications and sensitive data. Less critical applications such as Agency information portals that do not have sensitive information can leverage the public cloud. Services and resources can be orchestrated in a Public Cloud when security, privacy, and performance requirements are satisfied for that deployment. Although FedRAMP compliance is not a state level mandate, the Agency will favor solutions that use CSPs with a JAB P-ATO.

Cloud enabling virtualization technologies like containers, e.g., Docker, and container clustering technologies, e.g., Kubernetes, are recommended to enable solution portability, platform independence, and rapid deployment.

FX Vendor solutions that use cloud infrastructure should have the ability to use multiple cloud providers or to migrate between cloud providers quickly and at low cost on Agency request. Having this ability reduces cloud provider specific risks and costs of business disruption.

All vendor solutions should be cloud-ready according to the State's Cloud First initiative. All modules will be interconnected using the high-bandwidth low-latency connectivity of the Equinix solution.

Evaluation of moving the FMMIS infrastructure to cloud based infrastructure would likely only be cost justifiable if the fiscal agent provided infrastructure became unreliable, required significant increased capacity, required major technology refresh, was not able to support business continuity requirements, or the Fiscal Agent had a demonstratable low-cost migration approach.

Strategic Topic 3-1: FX Infrastructure Cloud Computing Adoption

3.2.6 COMMON UI FRAMEWORK

A Common UI Framework defines look and feel consistency, accessibility standards, naming conventions (e.g., buttons, field tags), field validation, JavaScript usage guidelines, security guidelines, interaction guidelines, system role-based access control guidelines, embedded SQL, etc. Refer to Attachment A *FX System UI Standards* referenced in Appendix A.

Strategic Topic 3-2: Agency UI Strategy for FX and Non-FMMIS

AGENCY UI DIRECTION	TIMELINE				
	Current	**2018**	**2020**	**2022**	**2025**
Each Application Defines its own UI	Agency applications, and contracted Medicaid applications (Enrollment Broker, TPL) have unique UI	->	Agency Approved Exceptions (e.g., some COTS)	->	
Common UI Framework with Module Specific Portals			Residual Interchange UI		
Common UI Framework for all FX functionality			Preference for consistency between FX Modules based on number of users and cost of consistency	->	
Common UI Framework for all AHCA Agency Systems					AHCA Applications
Common UI Framework used for Systems accessed by Medicaid Agencies				Available for use, Organization preference level of use	->

AGENCY UI DIRECTION	TIMELINE				
	Current	2018	2020	2022	2025
Common UI Framework Used by All Agencies, Plans and Providers				Available for use, Organization preference level of use	->

ANALYSIS

The desired future state will leverage the FX Common UI Framework for all FX Module user interfaces. The FX Common UI Framework provides for a cohesive and intuitive user experience even if different vendors implement Module or Service solutions. The Common UI Framework will also enable Agency-developed Medicaid related applications to deliver and contribute to a consistent user interface. An overview of FX System UI Standards can be found in Section 11 Appendix A – FX System UI Standards.

As part of using an FX Common UI Framework, vendors can refer to the FX UI Component library to achieve a common look and feel. The component library is a collection of UI components arranged in a meaningful manner. The component library allows development teams to work in a consistent way and can increase overall development efficiency. The library contains the specifications and base code necessary to implement consistent UI elements.

Vendors that deliver COTS based solutions are expected to provide a user experience that is consistent with the FX Common UI Framework.

Strategic Topic 3-2: Agency UI Strategy for FX and Non-FMMIS

3.2.7 INTERNET DOMAIN

Any outward facing or internet facing technology assets, need to use the Florida Health Care Connections Governance FX Governance (myflorida.com) domain as the standard.

AHCA IT will utilize certificates from domains FloridaHealthCareConnections.gov and FloridaFX.gov to secure the FX Application Lifecycle Management (ALM) solution and future FX components and sites (external facing sites). For all users, any navigation to FloridaFX.gov will be automatically redirected to FloridaHealthCareConnections.gov.

3.2.8 USE OF FORM FILLING USER INTERFACE

An electronic form filling user interface is popular where the user population may interact with both paper forms and online entry systems or where there is a need to print copies of information that is entered into a system. A common service for this functionality will provide a uniform solution.

Strategic Topic 3-3: FX Electronic Form Filling describes the recommended electronic form filling strategy direction for the FX Infrastructure (ESB, EDW, RDS, ODS, and Application Modules) and its context with the existing FMMIS system.

Electronic Form Filling	Timeline				
	Current	2018	2020	2022	2025
Module / System specific implementation of vendor's preference	X	->	Exception only for new systems		
Module / System implementation of Agency specified COTS product or solution					
Reusable FX Provided Service			Required for new FX projects		Migrate non-FX systems from previous solutions
Reusable Cross-Agency Service				Pilot as Optional for new projects	

Analysis

The benefits of modules standardizing form filling user interface service or solution is primarily consistency of user interface (field naming, format validation, etc.), standardization of productivity features (barcoding), and operational processing consistency of paper forms. A common service can reduce complexity for vendors and the costs of duplicated infrastructure and software.

A drawback is the widespread use of mobile and browser devices, which has reduced and eliminated paper form data collection support and options for many organizations and business processes. Also, one consideration of using a form filling data entry metaphor is that if information is auto populated on to a form, the information may not be legally considered to have been provided by the person. To alleviate this issue, a disclaimer is typically added to guarantee the validity of the data.

All FX solutions replacing FMMIS will occur as FX business area processing is replaced with new modules.

Strategic Topic 3-3: FX Electronic Form Filling

3.2.9 Standards and Technology Maturity

To achieve best value for the FX, it is important to consider the maturity of the standards and technologies used in modules and FX projects. Continuous improvement and market driven incentives will always present new opportunities to improve cost or service delivery effectiveness. The FX recognizes that while newer standards and technologies can provide benefits there may also be uncertainty, risks and costs associated with the implementation of new standards and technology. The FX also recognizes that use of mature technologies also increases the risk of obsolescence or higher operational costs. The FX seeks to implement solutions that consider these factors and aligns with the Agency's desired level of solution maturity.

The Rogers Bell curve, **Exhibit 3-7: Rogers Bell Curve: Category Percentages Are Across All Industries** categorizes an organizations tolerance for change and novelty. Note that the

chart graphically depicts the percentages of organizations in each category as the area under the curve. The FX Technology adoption toward innovation recognizes the principle of preventing avoidable Agency disruption. Looking at the chosen categories in **Strategic Topic 3-4: FX Technology Adoption Category** can be useful in understanding the Agency's position on the desired maturity of adopted technology.

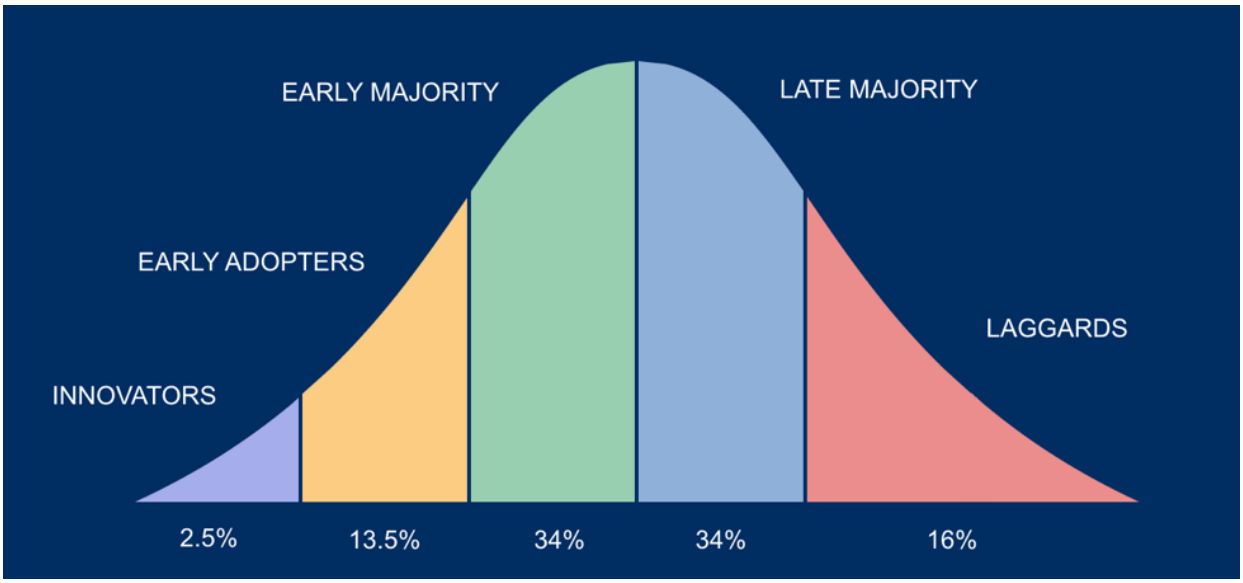

Exhibit 3-7: Rogers Bell Curve: Category Percentages Are Across All Industries

Strategic Topic 3-4: FX Technology Adoption Category describes the FX adoption category positions over time.

ADOPTION CATEGORY	TIMELINE				
	Current	**2018**	**2020**	**2022**	**2025**
Innovators					
Early Adopter		FX	->		
Early Majority	AHCA IT, Non-FMMIS	->			FX
Late Majority	FMMIS				
Laggards					

ANALYSIS

ADOPTION CATEGORY	TIMELINE				
	Current	2018	2020	2022	2025
Currently AHCA IT and Non-FMMIS applications are in the early majority category and are expected to remain that way to balance technological innovation with stability and security requirements. FMMIS is currently in the late majority. The Agency position on FX is to be an early adopter in the Medicaid space of technologies established in other industry sectors. The technologies that will differentiate FMMIS as late majority versus the FX as an early adopter are, for example, cloud computing, EaaS, fine-grained modular services, ESB, and decoupled UI framework. It is expected that by the start of 2025 the Agency's strategic position will move to early majority because FX will have an operational maturity and will likely be looking at new proven solutions implemented from other states and other markets.					

Strategic Topic 3-4: FX Technology Adoption Category

3.2.10 COTS USAGE

COTS products exist on a wide spectrum, from turnkey systems like the Microsoft Office Suite, to system components like the InRule rules engine to full claims processing products like Pega Claims Processing Software and CNSI eCams. Moving toward the components end of the spectrum, the value of well-defined interfaces which use open standards for file formats and communication protocols grows substantially.

When open standards are not required and promoted, integration of COTS products toward the components end of the spectrum can require tightly coupled custom code, referred to as *glue code*, to be integrated into the system. The more customized the integration the more complex the decision process to adopt and the subsequent implementation of the product integration. This type of tightly coupled integration adds inflexibility to the system and increases the overall system costs of maintenance and support.

A strong adherence to open standards and discouraging highly coupled integrations requiring *glue code* will encourage and facilitate the integration of COTS products and allow the Agency to maximize the savings benefit of using off the shelf solutions. Loosely coupled integrations through an ESB, API's and fine-grained services that use open standards are highly reusable, testable, and less complex to maintain and upgrade.

An important consideration when adopting a COTS technology is the adoption risk. FX will consider technology adoption risk to realize better returns from COTS product investments.

3.2.11 ACTIVITY PRIORITIZATION

The Agency, through FX Governance, acts on recommendations from the FX Portfolio. The portfolio management processes help align the strategic plan to prioritized activities based on business needs and on expected business value. The Agency's portfolio management process: *SEAS S-4: Strategic Project Portfolio Management Plan* (SPPMP) will evaluate business value continually as the platform matures and requirements become more defined and targeted. As with most enterprises, the Agency has resource constraints with respect to funding, staff, and

time. The SPPMP helps identify, categorize, evaluate across multiple dimensions, and select appropriate FX projects. Section 2 of the SPPMP, **Exhibit 2–2: System Strategy and Portfolio Management**, presents a visualization of the Agency's portfolio management process.

3.2.12 Technical Service Availability Strategy (TSAS)

Ensuring high technical service availability is paramount in maintaining continuous operations in the FX. All components of the FX from the enabling infrastructure (e.g., servers, storage, communications, platforms, etc.) to the technical services exposed by the application modules will participate in the TSAS. The TSAS also covers datacenter considerations.

3.2.12.1 Datacenter Availability

The FX technology strategy recommendation is to use a carrier-neutral datacenter to address capacity and resilience requirements and maintain high service availability.

Use of an alternate site can improve datacenter availability. The alternate site must support the same system operations as the main site. The three alternate site types are cold sites, warm sites, and hot sites.

- **Cold Site** - is datacenter space without any server-related equipment installed. The cold site provides power and cooling, which can be used if there is a significant outage to the main datacenter. The cold site will need extensive engineering and IT personnel, in addition to all necessary servers and equipment set up, migrated, and made functional. Cold sites incur the longest delay to achieve full operation and are the least expensive choice to use. This choice is suited for non-critical applications that can have long downtimes.
- **Warm Site** - offers datacenter space and has the hardware necessary to achieve full production operation. A warm site will have only servers ready for the installation of production environments. Systems must be updated; latest backups must be delivered, and restoration completed before service can be restored. This choice is suited for non-critical applications that can have moderate downtimes and need some degree of redundancy.
- **Hot Site** - is a mirror of the current datacenter infrastructure. The most important feature offered from a hot site is that the production environment(s) are running concurrently with the main datacenter. System deployments, application deployments, and data replication keep both the main site and the hot site in sync. In case of a significant outage event to the main datacenter, the hot site can take the place of the affected site immediately. This choice is the most expensive one to use. This choice is suited for mission-critical applications that can have minimal downtimes and need a high degree of redundancy.

Considering the critical services that the FX provides, the FX disaster recovery strategy recommendation for FX technical services is to use a hot site. The main site houses production, development, and testing tiers. The alternate hot site houses a mirror of the

production site used for failover. Both the main and alternate hot site continuously synchronize information and systems artifacts to keep the hot site current in case it is needed for failover. Either site should provide system operations as necessary in case of a disaster or outage. Additionally, the FX must follow Agency standards and practices for backing up data and systems including the use of offsite storage where appropriate.

It is worth noting that the TMS cloud strategy future state is designed to eliminate the need for a physical hot site expense and substitutes the availability strategy with a combination of hot site cloud failover deployment, node clustering, and rapid cloud deployments.

3.2.12.2 Availability Principles for Application Modules and their Services

Application modules should adhere to the following principles to participate in the TSAS.

- **Deploy in virtualized environments** – application modules will deploy in virtualized environments, register, and communicate with the ESB using standard protocols and interfaces.
- **Handle large request volumes and provide high availability** – Application modules must have a high availability strategy such as load balanced multiple instances, node clustering, etc.
- **Possess rapid deployment capabilities** – Application modules must have clear image build configurations and versioned image builds available for download from secure repositories.
- **Self-configure on startup** – Application modules must be able to configure themselves on startup using parameters supplied by a configuration management service.
- **Participate in the FX deployment** – FX services in both locations have the same availability requirements and participate in the same deployment orchestration. Application modules deployed to the main site production tier usually deploy simultaneously to the alternate hot site. To reduce risk associated with deployment of new or updated modules or changes in data, the deployment approach may introduce changes at a single site and take the other site offline until validation of the new deployment completes. This allows use of the alternate site to restore service if deployment back-out processes are complex or time consuming.
- **Configuration Item or Data Corruption** – In a hot site model with simultaneous deployment and near real time data synchronization, there is a risk the corruption of an application software core, configuration item or data would reduce the ability to operate from either location. Deployment processes must consider this risk and provide the ability to recover from corruption events within service standards.

3.2.12.3 COTS Considerations

When considering a hot alternate site, software license agreements may be affected. COTS products should have clear licensing options to support the hot site deployment, as the

applications will be in operation. Some license agreements allow for the installation of software at a hot site at no additional cost, if only one site is in operation at a time.

3.2.12.4 SaaS Considerations

While SaaS products may not adhere to the specific implementation details of FX Technical Service Availability, they should adhere to the principle which prescribes application modules to load balance requests, avoid single points of failure, and provide high availability. SaaS application modules also participate in the ESB service registration.

Because SaaS products may lack transparency of technology architecture, infrastructure, operations monitoring, and implementation details, the Agency should:

- Define specific Service Level Agreements (SLAs) and performance criteria for SaaS solutions
- Specify testing to assess risk including stress, volume, and continuous operation testing
- Include requirements for notification of internal operations deployments, changes, and maintenance that affect system availability
- Require visibility to internal solution architecture and operations monitoring insights of the solution

3.2.13 Disaster Recovery Coordination

In a modular environment where multiple vendors operate inter-dependent services and systems, there is an increased need for coordination of disaster recovery planning and service recovery and restoration. This section defines disaster recovery coordination in the broader context of overall business continuity and disaster recovery and describes the role of organizations specifically related to disaster recovery coordination. The overall description of disaster recovery planning and recovery requirements and roles is specified in Florida Statutes and as standard contract language in Agency procurements.

3.2.13.1 Business Continuity and Disaster Recovery Context

The definition of Business Continuity (BC) and Disaster Recovery (DR) have been changing over a period of time. **Exhibit 3-8: Business Continuity Components** shows the major functions of business continuity processing.

Exhibit 3-8: Business Continuity Components

Business Continuity refers to how a business should prepare and plan to ensure that its key products and services continue to be delivered in case of a disaster. This includes:

- Crisis Management strategy – defining the personnel and steps to take in the event of a crisis and how these will impact employees, stakeholders, and the Agency's reputation and value.
- Crisis Communication – defining the key roles and responsibilities, alternative mechanisms, and protocols for establishing and maintaining open lines of communication in the event of a crisis.
- Impact Analysis – a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident, or emergency.
- Prioritizing Business Operations – establishing the criticality and sequence of restoration of business processes to minimize disruption and loss.
- Service Level Agreements – the commitments between FX Project Owners and the Agency defining the quality, availability, and responsibilities of all parties and specified in predefined metrics.
- Regulatory Compliance – Regulatory compliance describes the goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws, policies, and regulations.

- Disaster Recovery – the policies, tools, and procedures needed to recover or continue operation of vital technology infrastructure and systems following a human-induced or natural disaster.

Normally, the Agency would own the overall Business Continuity plan. FX Project Owners and vendors might have a little content to contribute to the Agency's Business Continuity. As the Agency progresses on the transformation to the FX and implementation of modular systems, the Agency would have responsibility to develop and execute the Enterprise DR/BC plan that includes interactions with Executive Office of Governor, agency level declaration of disasters, prioritization of system recovery, business processing decisions, directing the Disaster Recovery coordinator to recover systems, directing Agency workforce, and specifying work locations. The Business Continuity roles and responsibilities can be found in the FX Responsible, Accountable, Consulted, and Informed (RACI) Matrix.

Disaster Recovery refers to how the Information Technology should recover in case of a disaster. This includes documenting the inventory of hardware and software, information of system/data backups, configuration of the DR site, roles and responsibilities, and cross-system dependencies. For Disaster Recovery, the Agency would provide a primary and secondary coordinator responsible for coordinating disaster scenarios among the FX Project Owners since it includes system recovery and cross-system coordination of recovery points. All FX Project Owners are responsible for developing their own internal DR/BC plans. The FX Project Owner's DR/BC plans would be an input to the Agency's Enterprise DR/BC plan.

One of the most critical parts of a disaster recovery is the restoration of data. The Agency will be the central coordination point across systems for disaster recovery activities with the FX vendors. The IS/IP Vendor, who is responsible for the Integration Platform (that is used by all vendors), and the EDW Vendor, who is responsible for data integrity, will be key coordination parties. All FX Project Owners will coordinate communications and DR activities through the designated coordinators. FX project owners would participate in disaster recovery planning, testing, and execution as participants. The disaster recovery roles and responsibilities can be found in the FX RACI Matrix.

3.2.13.2 Disaster Recovery Coordination Definition

Disaster Recovery Coordination is a function to ensure that disaster recovery plans of multiple systems, services, and applications are initiated and executed in accordance with the Agency Business Continuity Plan.

3.2.13.3 Disaster Recovery Coordination Roles and Responsibilities

In the event of an incident, the primary duties of the disaster recovery coordination role are:

- Ensure activation of response teams and communications plans with appropriate vendors and Response Team as defined in their DR Plans
- Coordinate dependencies and sequencing of DR activities between impacted business processes
- Receive status updates and communicate to affected parties

- Escalate issues as needed

The primary duties of the disaster recovery coordination role related to disaster recovery planning are:

- Conduct Business Impact Analysis (BIA)
- Conduct Risk Analysis
- Define Metrics
- Develop Risk Management Plan
- Develop Cross-Vendor Incident Coordination and Communications Plan
- Develop Disaster Recovery Coordination Plan

The primary metrics to track to measure disaster recovery coordination effectiveness are:

- Number (#) of Business Processes Threatened by a Potential Disaster (Do you know all your processes? Have any new ones been created since the plan was last updated?)
- Percentage (%) of Business Process Coverage
- Amount of Time Since Each Plan Was Updated
- Recovery Time Objectives (RTO) – Agency standard is 24 hours
- Recovery Point Objectives (RPO) – Agency standard is 15 minutes or less
- Actual Time to Recover a Business Process
- Gap Between Target and Actual Recovery Time

SECTION 4 TRANSFORMATION CHALLENGES

4.1 OVERVIEW

There will be many technology challenges to overcome on the transformation to FX. The primary categories of technology challenges span a wide spectrum including:

- Technology implementation
- Operations considerations
- Technology interoperability
- Scalability and capacity
- Security
- Technology industry and market disruptors
- Technology change management

The FX Technology Strategy identifies, communicates, engages, and monitors FX projects for the purposes of avoiding, mitigating, and overcoming technology challenges.

4.2 INVENTORY OF TECHNOLOGY CHALLENGES

Exhibit 4-1: Transformational Challenges Detailsdisplays the challenge, impact, and mitigation for transformational challenges.

CHALLENGE	IMPACT	MITIGATION
Technology Implementation		
FX technologies implementations need to consider the entire technology ecosystem including technology modernization impacts to health plans, providers, and recipients	▪ Modernization efforts external to the Agency may not align with FX technology direction ▪ May want to expand use and reuse of technology and data services for use outside traditional system scope areas	▪ Ongoing communication of strategy ▪ Use of collaborative governance processes ▪ Perform periodic strategy refreshes considering overall ecosystem ▪ Use technical requirements verification and validation
Increased role of technology in business processing (e.g., enterprise business rules, real-time analytics, artificial intelligence bots)	▪ Difficult to change ingrained and mature business processes ▪ More attention on system availability, capacity, and scalability ▪ Organizational change and position descriptions affected	▪ Include organizational change management in transition services ▪ Validate capacity, availability, and scalability assumptions early

CHALLENGE	IMPACT	MITIGATION
Modular technology solution implementation takes longer to implement	▪ Increased elapsed time and total cost to modernize entire system	▪ Communicate and manage expectations ▪ Communicate benefits including reduced risk, faster and larger outcomes, increased competition, increased business agility ▪ Use technical requirements verification and validation. ▪ Use FX Modularity Strategy
Inconsistent user interfaces (UI) and user experiences across multiple vendor solutions	▪ Higher training and change management ▪ Reduced user productivity	▪ Develop an Agency standard Common UI Framework and promote use of the framework ▪ At a minimum enforce UI style standards ▪ Use technical requirements verification and validation
Modularity increases use of multiple technology vendors	▪ Increased integration complexity ▪ Increased vendor management costs ▪ Reduced licensing negotiating power ▪ Increased variety in maintenance and support skills ▪ Increased dependency on vendors	▪ Ongoing analysis of cost and benefits ▪ Select appropriate mix that balances competition and synergy impacts ▪ Knowledge transfer to Agency Full Time Employees (FTEs)
Monitoring and auditing multi-vendor solutions	▪ Each technology solution could require unique monitoring and audit tools and techniques	▪ Use a centralized logging and monitoring solution that correlates system events with service requests ▪ Require services to have default monitoring methods ▪ Use technical requirements verification and validation
Technology procurement and implementation process have significant bureaucracy	▪ Benefits of modular technology implementation diminished by overhead in procurement and project implementation	▪ Evolve to agile procurement and technology implementation processes ▪ Embrace *fail fast* for technologies or projects that don't produce outcomes or where better alternatives exist

CHALLENGE	IMPACT	MITIGATION
Service versioning and service introduction	▪ Upgrades and changes to business, technology, or data services used across modules is difficult to coordinate and implement	▪ Design integration platform, service providers, and service consumers to support concurrent use of service versions to simplify deployment coordination ▪ Dependency management solutions will allow a system to be composed of independently developed modules and services which are at different levels of maturity. These solutions rely on versioning standards and the service registry ▪ Use technical requirements verification and validation
Vendor adoption of FX Data and Technology Strategy	▪ Modularity and decoupling of proprietary application data stores may commoditize the market and reduces vendor profit potential ▪ Smaller project sizes may reduce interest causing fewer technology opportunities and increased vulnerability to single vendor dependence.	▪ Use buying power to shape market toward modern, standards-based architectures, communication protocols, and technologies that align with market and industry trends ▪ Proactively communicate expectations with vendor community ▪ Coordinate with other states to accelerate vendor adoption
Technical challenges with use of data replication as transition strategy between ODS and FMMIS	▪ Cross system data inconsistencies ▪ Decreased data integrity	▪ Evaluate which data to replicate or synch and at what frequency ▪ Test and validate replication speed requirements of the FX and the requirements for transactional consistency ▪ Geographical proximity and fast networks may reduce latency issues ▪ Use technical requirements verification and validation

CHALLENGE	IMPACT	MITIGATION
Operations Considerations		
Maintenance of technologies and systems that will be replaced	▪ Difficult to justify maintenance and upgrade expenditures for technology and systems that will be replaced ▪ Business improvement frozen during period of transition to new technology and systems	▪ Prioritize replacement of technologies that are deemed crucial to FX business continuity to avoid pressures to upgrade old systems ▪ As the transition occurs, identify dependencies and make their continuous operation a requirement of integration testing
Difficult to incrementally replace or upgrade parts of a large highly integrated system (e.g., FMMIS, FLORIDA)	▪ The large legacy system will need to expend transition service costs to perform maintenance to allow parallel operation or partial decommissioning during transition	▪ Use strategies (e.g., interim data replication) that reduce changes to the large system as functionality is decommissioned ▪ Evaluate benefit of integrating new components to legacy system for interim benefits to legacy system ▪ Use technical requirements verification and validation
Monitoring use of cloud-based infrastructure and systems management of cloud-based services	▪ Inability of modules to scale on demand (auto-scale) ▪ Cloud services costs incurred in excess of use	▪ Use a cloud management module that can integrate modules and systems to the cloud infrastructure provisioning APIs and dynamically allocate and de-allocate nodes as needed
Technology Interoperability		
Use of multiple technology architectures and platforms (e.g., Java, .NET, PaaS, SaaS)	▪ Increased vendor management ▪ Increased monitoring complexity ▪ Reduced reuse and processing consistency ▪ Resistance to use of enterprise technology services ▪ Vendor and platform dependence ▪ Increased skill variety for maintenance and support	▪ Define and communicate core acceptable platforms and preference for use of core platforms ▪ Ongoing analysis of cost and benefits ▪ Transition solutions on non-core or outdated platforms to core platforms over time

CHALLENGE	IMPACT	MITIGATION
Platform dependence due to a lack of a standards-based service layer on the platform	▪ Creates a dependence on the underlying platform's custom communication protocols and data formats	▪ Technical standards, a universal data dictionary, a business and technical service dictionary, and standard definitions of common elements will enable the FX 's platform independence ▪ Use technical requirements verification and validation
Coordination between technology and module vendors	▪ Increases in collaborative governance requirements, potential for strategy misalignment, issue tracking.	▪ Vendor that provides Integration Services and Integration Platform provide leadership and coordination between technology solutions ▪ Use FX strategy for collaborative governance
Continuous technology deployment across a distributed ecosystem	▪ Configuration management and release management complexity increases based on the number and types of technology deployed	▪ Use a continuous integration infrastructure and process that can validate integration testing of new or updated technology before deployment to production environments ▪ Use a change management approach for continuous deployment ▪ Use technical requirements verification and validation
Scalability and Capacity		
Ability to support scale and capacity due to new projects such as the 360 view where information exchanges could increase exponentially	▪ The inability to support large data volumes and data access requests could result in system crashes, outages, service disruption, and slow system response time ▪ Some vendor solutions may not be viable at the scale envisioned to support the FX	▪ Validate solutions early and often beginning at procurement phase ▪ Seek solutions that incorporate high-capacity techniques like: Cloud auto-scaling, application node monitoring, database clustering, database partitioning, sharing, and caching strategies ▪ Use technical requirements verification and validation

CHALLENGE	IMPACT	MITIGATION
Continuous high availability needed by SOA	▪ Service instances can become unresponsive due to a high request volume	▪ An increase of load balanced service instances, and request work queues. ▪ Use technical requirements verification and validation.
Storage strategy for rapid increases in data volume	▪ Storage requirements increase over time. Transitioning to a SOA is anticipated to further increase storage requirements	▪ Proactively perform storage capacity planning and monitoring ▪ Stay closely aligned with business on changes in storage usage factors ▪ Use elastic resource allocation capabilities inherent in cloud solutions (e.g., Storage as a Service) ▪ Use technical requirements verification and validation
Network capacity and resiliency	▪ The deployment of modules on remote cloud technologies increases the dependency on network capacity and resiliency for system access and processing availability. Increasing recipient populations, encounter data, real-time integrations, and reuse of business and technical services place additional demands on the network	▪ Capacity modeling, testing, and proactive monitoring help avoid impacts ▪ Consider Ethernet backbones in carrier neutral facilities to address capacity and resilience. Virtualization technologies can play a critical role in addressing resiliency issues
Communications latency due to increased services over the network	▪ Quality of user experience could be degraded ▪ Processing delays in FX services (e.g., eligibility responses)	▪ Optimize physical proximity of highly interactive services, increased bandwidth allocation, system design, and caching strategies
Change in network usage patterns	▪ Changes in size and number of network messages may alter network design requirements	▪ Model, test, and monitor network throughout technology and system implementation life cycle

CHALLENGE	IMPACT	MITIGATION
Security		
Data privacy and security technologies and responsibilities are distributed across many vendors and service providers	▪ Increased coordination effort between vendors ▪ Increased effort to monitor and address issues that could cause compromised recipient data, system user data, and security breaches	▪ A comprehensive security strategy focused on prevention ▪ Integration services vendor plays active role ▪ Clear communication to vendors on security requirements in the T-8: *Enterprise Data Security Plan*, T-6: *Technology Security Standards*, and the TSRG ▪ Use technical requirements verification and validation
Departmental and personal data stores and applications may not use enterprise security policy	▪ Bypass access controls ▪ No logging of usage ▪ Unknown data loss ▪ Higher risk of data breach ▪ Processes to identify and respond to data breach are less mature	▪ Enforce enterprise security policy and standards with equal to all systems with sensitive data ▪ Eliminate need for departmental and personal data stores and applications
Technology and Industry Market Disruptors		
Technology industry and market disruptors (e.g., Blockchain, crypto currency, telemedicine, cognitive processing, behavioral economic processing) gain rapid adoption	▪ Current FX technology and module planned FX infrastructure investments could be disrupted or not used ▪ New investments of capital and resources needed to accelerate adoption of disruptive technologies	▪ Consider technology strategy contingency strategy if technology market disruptors accelerate or fail ▪ Perform ongoing strategy refresh to assess market disruptors and adjust strategy ▪ SPPMP
COTS solution vendor reluctance to use Enterprise Services	▪ COTS solutions that use their own custom or proprietary services could introduce processing inconsistency ▪ Duplication of processing could raise long term maintenance cost ▪ Vendors charge *extra* to use FX Enterprise services	▪ Validate COTS solutions' use of open standards and protocols and ability to use FX services ▪ Use technical requirements verification and validation

CHALLENGE	IMPACT	MITIGATION
Open-source technology solutions and conversion of vendor modules to open source	▪ Lack of support and maintenance ▪ Lack of ongoing investment in module improvement ▪ Reduced opportunity for vendor investment recovery across multiple states	▪ Select open-source products if vendor support is available ▪ Monitor use of open-source solutions by other states ▪ Use technical requirements verification and validation ▪ Use TMS for guidance
Technology Change Management		
Establishing a culture of real-time information and integration	▪ Resistance to adoption of real-time information exchange and data access may drive legacy processing styles into design that undermines benefit to the Program	▪ Agency and FX leadership should reinforce importance of real-time high-quality data to support decision-making and program operations where appropriate
Culture of analyzing data in the new FX	▪ Resistance to data analysis tool changes, utilization of data marts, and perceived loss of control of data may drive legacy data handling and ownership styles into design that undermines benefit to the FX	▪ Agency and FX leadership support for future vision ▪ Selection of appropriate persona specific tools ▪ Appropriate data mart design ▪ Appropriate user tool training
Data sharing agreements to enable use of social determinants of health data	▪ Organizations routinely describe large value propositions of using data from other systems but are reluctant to share data in their own systems	▪ Strong executive sponsorship is the most effective technique to break down data sharing barriers ▪ Simplify / Streamline data sharing agreement process
Data duplication and data ownership issues	▪ Business units create data silos independent from the authoritative data sources. Use of these data silos results in inconsistent implementation of policy, inaccurate reporting, and decision-making based on different data sources	▪ The FX Data Management Strategy including use of the ODS, RDS, and EDW will provide the single source of truth for FX data ▪ A granular implementation of data services, caching strategies, and persona-based data marts will facilitate quick access to data avoiding the need for business unit specific implementations

Exhibit 4-1: Transformational Challenges Details

4.3 DEFECT MANAGEMENT

Defect Management is the process of detecting and fixing bugs that occur in the software. All defect management standards and definitions are found in the *T-7: Design and Implementation Management Standards* Attachment F: *Testing Management Plan* Section 9.

SECTION 5 FX TECHNOLOGY OVERSIGHT

Specific implementation and use of the FX governance processes and framework has been defined in SEAS deliverable *S-1: FX Governance Plan*. This section describes how the FX Governance Plan processes and procedures are used to make and implement FX technology decisions. In addition, responsibilities for key roles in technology governance are defined and technical management topics governed through the structures and processes are described.

5.1 USE OF FX GOVERNANCE PROCESSES

The FX Governance Plan provides a tiered structure and processes that provide leadership, guidance, decision-making, and overall direction for FX projects. The FX Governance Plan describes the use of workgroups (e.g., FX Tech, FX Data) to provide specialized input or analysis on specific topics or recommendations requiring subject matter expertise. The workgroup to address FX Tech related specialized input is referred to as FX Technology Standards Committee (TSC). The TSC advises other FX governance vehicles as needed. The TSC supports both establishment and advisory services about technology standards.

5.2 ROLES AND RESPONSIBILITIES

Exhibit 5-1: Technical Services Roles and Responsibilities lists the technical services roles and responsibilities.

ROLE	RESPONSIBILITIES
SEAS Technical Architect	▪ Identifies the Technical Services to perform within the system ▪ Evaluates Technical Service Requests ▪ Proposes new, updates, and retirement of technology service components to the TSC ▪ Maintains Service Registry
FX Technology Standards Committee (TSC)	▪ Reviews proposed Technical Services ▪ Advises FX Governance committees on Technical Services recommendations
FX External Organizations	▪ Reviews and may align technology solutions to FX technology architecture service standards ▪ Contributes recommendations for enhancements to existing Service Registry entries ▪ Contributes recommendations for new Service Registry entries
Integration Services / Integration Platform (IS/IP) Vendor	▪ Consults with technology stakeholders in the use of integration platform ▪ Consults and guides FX Project Owners in designing, implementing, and maintaining interoperability between FX modular components

ROLE	RESPONSIBILITIES
Enterprise Data Warehouse (EDW)	▪ Consults with technology stakeholders in the development of the physical data model ▪ Consults with technology stakeholders in the development of the Operational Data Store and Operational Data Services ▪ Consults with technology stakeholders in the development of the Data Conversion Plan
FX Project Owner	▪ Identifies and understands FX Service Registry entries ▪ Provides vendor specific Service Registry entries

Exhibit 5-1: Technical Services Roles and Responsibilities

5.3 GOVERNANCE PROCESS

FX Governance processes align with the FX Technology standards setting processes via the TSC. For this reason, the Agency and SEAS Vendor will leverage the processes and tools used for FX Technology standards.

The governance of FX Technology standards follows a defined process to communicate, support vendors, assess compliance, and report compliance to FX Technology standards. A summary of the defined process is that:

- The TSC is an FX Governance authorized workgroup that provides advisory technology recommendations related to the technology assets of the Agency. Technology services are a type of technology asset and thus the TSC is the workgroup that is the entry point for technology.
- The Data Governance workgroup establishes the policies for data quality and data ownership. The workgroup conducts Data Quality reviews and establishes business rules to ensure quality. Data Governance also determines and establishes data retention policies.
- The SEAS Vendor researches, advises, and prepares materials for TSC approval of recommendations. The SEAS Vendor develops communication materials, implements the communication processes, provides FX Project Owner support, conducts compliance assessments, and reports compliance to the Agency.
- The AHCA FX Technical Lead directs the SEAS Vendor and authorizes the release of communications, providing vendor support, conducting compliance assessments, and reporting compliance to the Agency.

5.4 TECHNOLOGY GOVERNANCE FUNCTION

The FX TSC provides the structure to define and communicate FX Technology direction and provide recommendations on technology-related decisions. Other important functions of the TSC are to:

- Ensure the Agency has a vehicle to make technology-related recommendations to FX Governance and ultimately the Secretary to make decisions
- Provide the Agency a vehicle to evaluate technology-related issues and opportunities from a context broader than a specific project perspective
- Allow qualified Agency personnel to provide direction and make recommendations on technology-related issues
- Provide checks and balances to review and accept vendor technology standard recommendations
- Provide a forum for vendor requests for exemptions to following FX technology standards
- Provide an authority to act on and make recommendations on standards compliance findings that occur on FX projects
- Ensure representative inclusion of multiple Agency perspectives on technology standards and technology direction setting

SECTION 6 COLLABORATIVE GOVERNANCE

6.1 COLLABORATIVE GOVERNANCE OVERVIEW

The Collaborative governance strategy defines direction, processes, and tools to implement modules and systems in an open and flexible way that promotes interoperability. Collaborative governance focuses on communication, input gathering, technology information and asset sharing, and technology decision-making including with indirect stakeholders to the FX. Indirect stakeholders to FX technology include external organizations, other states, providers, health plans, healthcare software vendors, the general public, and other stakeholders.

6.2 COLLABORATIVE GOVERNANCE PRINCIPLES

The FX seeks to leverage the insights, expertise, and collective synergies of stakeholders to the FX to create the most effective use of technology. The FX seeks engagement and trust enhancing contributions and communications among the FX Technology community. Below are collaborative governance principles:

The TREATS acronym highlights collaborative governance principles of the FX strategy and vision:

- **Trust** – Trusted relationships with organizations and individuals achieve more with less. The FX collaboration approach emphasizes communications that establish, maintain, and enhance system and human interactions using the power of increased trust.
- **Reliability** – Reliability is an important foundation of trust-based collaboration. FX emphasizes that FX Project Owners and indirect stakeholders provide reliable information, insights, and discussion on architecture, technology, implementation, and strategy. The result of collaboration is reliable delivery by people that provide or use FX services.
- **Experience enabling** – Experience enabling refers to FX's simultaneous focus on participant experience and experience-based analytics.
- **Agility** – Agility in collaboration governance refers to collaborative communication, and decision-making at speed. Likewise, the pace of change affecting health care is accelerating. Collaborative governance positions the FX to quickly adapt to opportunities and issues that arise from changes in technology, policy, process, or funding.
- **Technology** – Collaborative governance related to technology includes alignment with MITA and balancing emerging and future technologies with understanding of risk and practicality.
- **Services** – Collaborative communications related to technology emphasize service orientation. The FX Technical Management Approach emphasizes services. These include services vendors provide, the service-oriented architecture technology in MITA, and modular processing capabilities provided as technology or business services.

6.3 FX GOVERNANCE STRATEGY

The FX Governance Strategy defines the governance structure for decision-making and communication directly related to FX projects. The initial implementation of the FX Governance Strategy supports FX projects focused on Agency systems. The FX Governance Strategy includes mechanisms for communication with other agencies that are Medicaid stakeholders. The FX Governance Strategy will evolve to optimize communication with the statewide Medicaid Enterprise when planning and implementation of FX Enterprise Integrations and modules begin.

Below is an overview of collaborative governance of technology topics. The approaches described support direct and indirect FX stakeholders.

- **Communication** – The SEAS Vendor is the central point of focus for bi-directional communications about FX technology topics. The SEAS Vendor manages the FXPR that holds technology information and assets on a wide range of topics related to FX. Other organizations including the Agency, IV&V Vendor, FX Project Owners, EDW Vendor, and IS/IP Vendor coordinate the development and release of technology related communications via the SEAS Vendor.
- **Input gathering** – The SEAS Vendor solicits and accepts FX technology related input and recommendations from direct and indirect stakeholders to FX projects. The SEAS Vendor uses the equivalent technology standards (refer to T-6: Technology Standards Attachment D *Technology Standards Communication, Support, Compliance, and Compliance Reporting Procedures* located in the FX Hub) governance processes to process input received about technology standards.
- **Technology information and asset sharing** – The SEAS Vendor manages the FXPR including access, content publication, and distribution. The IS/IP Vendor is responsible for the Integration Platform managing technology web service information and assets using the service registry, service repository, and service contract management tools described below.
- **Technology decision** – Technology decisions identified via collaborative governance process follow the normal process used for FX Technology standards (see FX-SEAS - T-6-*Attachment-D -Technology-Standards-Procedures*) governance process. The SEAS Vendor works with the Agency FX Technical Lead to make decisions about communication and escalation of technology related issues identified or introduced by indirect stakeholders to FX projects.

At a tactical level collaborative governance of technology services, the SEAS Vendor will use capabilities provided in the procured Integration Platform to establish and maintain a collaborative environment for all users of technical services, both providers and consumers. The FX Technical Management Approach to modular implementation requires all module vendors and system integrator(s) to closely use the collaborative governance enablers.

The key governance enablers for collaborative governance are:

- Service Registry

- Service Repository
- Service Contract Management

Exhibit 1-1: SEAS Technology Deliverables lists SEAS Technology deliverables that contain strategic direction and guidance in additional areas of technology. Together, these areas contribute to the overall effort to foster a common awareness of the standards, strategic approach, and processes governing the strategic management of technology in the FX. The common reference and language used in the SEAS Technology deliverables are a key enabler of the FX collaborative governance strategy.

6.4 Collaborative Governance Tools and Techniques

Collaborative governance tools provide the repository of technology service information. The tools facilitate a communication strategy that provides quick access to information of interest by providers and consumers of technology services. Collaborative governance is enabled through the following three tools described below. The service registry, service repository, and service contracts are the tools, specifications, and service vocabulary that provide the enabling technology to aid in achieving the Agency strategy of building modules from fine-grained modular services, data services, and micro services exposed through standards-based APIs.

- **Service Registry** – The Service Registry is a catalog of services, their instances and their locations which helps in service definition, service selection, and in enforcing service policies. Service providers register service instances to the service registry at startup and deregister instances on shutdown. Consumers of the service and routers query the service registry to find the available instances of a service.
- **Service Repository** – The Service Repository stores artifacts and assets about the services including functional specs, user and other documentation, and SLAs that define transaction capacity, maximum throughput, downtime, etc. The service registry manages run-time assets. The service repository manages both for design time and run-time assets.
- **Service Contract Management** – The Service Contract Management Tool(s) manage the technical web service contract metadata that defines what a service offers and how and where to access the service.
- **FX Hub** – The FX Hub, located in the FXPR, is the hub of technology vision, strategy, standards, and other reference information. It also documents direction on a wide range of technology topics and enables interactive discussion among FX stakeholders.

The Integration Platform implementation included an API management tool, Oracle API Management, that provides service registry, service repository, and service contract management capabilities.

SECTION 7 TECHNICAL PRINCIPLES

FX Technical Principles provide direction for making technology decisions to implement FX technology services. The FX Technical Principles guide FX projects, modules, and system implementations to create a FX future state that is:

- Aligned with MITA
- SOA-based
- Cloud-deployed
- Built in open and flexible way that promotes interoperability

The Technical Principles are accessible to stakeholders of the FX. The principles also reside in the Guiding Principles List in the FXPR.

7.1 FX TECHNICAL PRINCIPLES

Business Driven – Business needs and opportunities that create business value are the basis for technology selection and use. The FX adopts and uses technologies that support business goals or objectives. Technology implementations are to enable achievement of business needs.

Platform Independence – Stakeholders will develop solutions that are reusable and platform-independent. Technologies used are to be cloud-ready and SOA-based.

Adaptability, Extensibility, and Scalability – Module, system, and service design and implementations are to enable reuse. Solutions are to provide and use flexible responsive technologies that support future use, growth, and adaptation.

Open Technology and Standards Based – Stakeholders will leverage the advantages of standardization (e.g., data sharing, interoperability). Solutions and services should be accessible through open, standard interfaces that are easy to integrate, extend, and reuse. Stakeholders will adhere to the technology standards in the FX Technology Standards Reference Guide (TSRG).

Integrated Security & Privacy – Modules, systems, and services will secure and protect the privacy of FX data.

Interoperability – Modules, systems, and services will use the FX interoperability enablers including the integration platform, enterprise service bus, FX Standards, and the guidance and direction of the SEAS and IS/IP Vendors to enable data exchange and reuse between services and other entities.

Quality Data – Technologies are to provide high quality data via the services they provide. Services are to provide data that is accurate, relevant, accessible, and understandable data aligned with the Data Quality Framework described in the FX Data Management Strategy.

Current and Proven Technology – FX projects are to use technologies that are market relevant, available, supported, and where possible, proven to support the processing complexities and scale of the FX.

7.2 SOA Technical Principles for Module and System Implementation

In addition to aligning with FX Technical Principles, FX technology services are to follow the technical principles in the *Best Practices* section in The Open Group's *SOA Source Book*. The SOA Source Book can be found through an internet search of *The Open Group's Legacy Evolution to SOA Best Practices* and it describes widely agreed upon key principles for services.

Well-Defined Service Contract

A well-defined service contract is one which describes all available functionality the service provides. Service providers and consumers are to use well-defined service contract standards (e.g., WSDL) that describes details of use to assist the service requestor to invoke the service(s) required. Automatic generation of service contracts from APIs or services that are undocumented or under documented is unacceptable. Likewise, direct database-to-schema conversion contract generation is also unacceptable because it introduces tight-coupling between message and database.

Define Services with Appropriate Granularity

Service providers are to design services for appropriate granularities that offer greater flexibility to service requestors without affecting the performance and security. Services granularity should make it easy for service requestors to assemble services to execute business scenarios. This is not always possible, especially for (multi-step) transaction-oriented systems. Each service should define the granularity of the service (e.g., which steps of functionality and invocations of other services or modules take place).

Loosely Coupled Services

Service requesters can consume services without any knowledge about the technical details associated with a service implementation. As long as the implementation meets the specified Service-Level Agreement (SLA), knowledge of the technical solution implementation is unnecessary. This also relates to the principle of well-defined service contract, described earlier.

Design Services for Stateless Operation

Services invocation is to be independent of the state of other services and each service invocation has all the required information from one request to another.

Ensure Services have Appropriate Security Enforcement Standards

Service providers are to design and implement services with appropriate security policy enforcement mechanisms to ensure that only authorized requesters can successfully invoke them. An objective of the FX integration platform is to centralize identity management and access policies at the integration layer to enforce consistency of security policy.

Follow SOA Ontology/Vocabulary Standard

Team members and stakeholders of FX projects are to communicate using common vocabulary standards throughout the FX Program Life Cycle to effectively facilitate SOA adoption and align the business and IT communities. An FX ontology defines the SOA concepts and semantics commonly understood by all stakeholders and enables effective communications. Refer to the SEAS deliverable *T-5: Technical Architecture Documentation* (i.e., FX Hub > Standards & Plans > Category: Technology > Technical Architecture Documentation).

7.3 TECHNICAL PRINCIPLES FOR NEW DATA SOURCES

New data sources will be accessed via the Integration Platform ESB and exposed to systems requiring the data through defined interfaces. Interface Control Documents (ICD) will describe the necessary information required to effectively define interfaces and rules for communicating. Both the sending and receiving interface points will define the communication exchange using the ICD. An ICD template has been created by the IS/IP Vendor containing all of the information needed to properly define the integration The ICD Template is the approved formal standard to document interface control development deliverables for FX projects and located in the FXPR at FX Hub > Templates > Category: Technology.

The ICD specifies the interface requirements that the participating systems must meet. 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 system expects data to flow.

All modules and external entities utilizing the integration platform to access data sources must document the interface using the ICD template and work closely with the IS/IP Vendor to detail input and output parameters for successfully establishing access to the data source(s). Establishing access to data sources will require close collaboration between the IS/IP Vendor and data sourcing entity and detailed documentation (ICD) for both end points to access the data in a secure, reliable, and accurate manner. Any data feeds from external sources are required to utilize the IS/IP Vendor's integration platform.

SECTION 8 TECHNICAL GOALS AND OBJECTIVES

In addition to being aligned with MITA technical goals in Part III Chapter 2 Technical Management Strategy, the FX Technical Goals and Objectives are achievement targets aligned with the FX Strategic objectives that support the Agency mission to improve health care for all Floridians.

- Goal 1: Apply Cloud Computing concepts where possible and feasible.
  - Objective 1: Enable scalability, elastic resource allocation, and high availability across FX.
- Goal 2: Use rules engines technologies, where possible, to extend the system configuration abilities to the business community.
  - Objective 1: Enable and support interoperability, integration, and open architectures.
- Goal 3: Follow FX performance standards for accountability and planning.
  - Objective 1: Review national standards for health and data exchange and open standards for technical solutions, using existing national standards whenever possible. When Medicaid-specific standards are necessary, the Centers for Medicare and Medicaid Services (CMS) will support collaboration efforts of industry groups in the submittal of proposed standards to national standards organizations for review and approval.
  - Objective 2: Use the set of MITA Framework common business processes and Data Standards to make it possible to develop performance standards, measurement techniques, and corresponding utility services.
- Goal 4: Develop systems that can effectively communicate to achieve common program goals through interoperability and common standards.
  - Objective 1: Adhere to technology standards, specifically open standards, to facilitate integration of Commercial off-the-Shelf (COTS) solutions and the reuse of solutions within the Agency and the State, resulting in lower development costs and reduced development risk.
  - Objective 2: Adopt data and industry standards and promote the development of appropriate standards when needed.
  - Objective 3: Promote the use of data and technology standards to improve the cost effectiveness of development. The use of Data Standards provides better access to data by promoting data consistency and enhanced sharing through common data-access mechanisms.
  - Objective 4: Use standard definition formats to map data to standard data elements, where appropriate, and provide the data descriptions when the data elements are nonstandard.
  - Objective 5: Represent security and privacy access rules for each data element in a standard manner.

- Objective 6: Employ a collection of services to read the data descriptions and security/access rules to release information to authorized users for processing.
- Objective 7: Promote secure data exchange. MITA defines and integrates security and privacy capabilities throughout the architecture by identifying access requirements in the business processes, defining them within the data models, and applying them through the MITA technical models.

- Goal 5: Promote an environment that supports flexibility, adaptability, and rapid response to changes in programs and technology.
  - Objective 1: Promote reusable software and hardware components and modularity.
  - Objective 2: Maximize the benefit across the State Medicaid Enterprise, while promoting innovation and creativity in the FX environment.
  - Objective 3: Enable and support interoperability, integration, and open architectures.
  - Objective 4: Employ services that make it possible to deploy common interoperability (i.e., system-to-system communication) and access (i.e., system-to-person communication).
  - Objective 5: Package common functionality and capabilities with standard, well-defined interfaces (i.e., services), used by new applications, legacy applications, COTS software, or all three, to invoke the functionality.
  - Objective 6: Provide adaptability and extensibility. An adaptation (i.e., the capability that allows users to change the specifics of processes, data, or technical solutions using configuration files) enables the Agency to customize FX elements to meet their unique needs. An extension (i.e., the capability that allows users to add functionality and capabilities) enables the Agency to add new functionality to FX elements to meet their needs, while still meeting MITA goals and objectives.
- Goal 6: Provide data that is timely, accurate, usable, and easily accessible to support program analysis and decision-making.
  - Objective 1: Develop reusable services to allow a single service to pass eligibility information from a variety of program systems to a mechanized claims processing, information retrieval, or eligibility determination systems.
  - Objective 2: Improve data quality by using Data Standards, applying standard performance standards, and relying on the availability of the enhanced data exchange and sharing provided by the hub architecture.
- Goal 7: Reduce duplication of costs by collecting data already available elsewhere and using that data to administer the program more effectively.
  - Objective 1: Enable data sharing without requiring extraction and loading of the data to a central location allowing each organization control and ownership of its own data.
- Goal 8: Put the best interest of the recipients first.

- Objective 1: Provide a recipient-centric focus of operations.

SECTION 9 TRANSITION PLANS

9.1 OVERVIEW

The FX applies outcome-driven decision-making to achieve the FX Strategic Priorities. The future state is a statewide Medicaid Enterprise optimized to use its people, technology, and processes to deliver better health care for all Floridians. Some of the technology characteristics of the FX future state are:

- Cross-Agency use of high quality, real-time, *single source of the truth* information. Additional details on the single source of truth and master data management (MDM) are in the Common Data Architecture section in the *T-1: Data Management Strategy*
- Reuse of business, technology, and data services
- Seamless integration and interoperability between business, technology, and data services
- A *single source of the truth* electronic policy including data edits, validations, transformations, and business rules
- Data analytic capabilities to identify and act on data driven insights
- Agile maintenance and change to business processing
- Data capture, validation, and data-driven decision-making at the point of recipient and provider interactions
- A consistent user interface and user experience especially for recipients, providers, and Agency users that use multiple business or technical services
- A highly available dynamic, scalable infrastructure and network that supports business and technology services
- Secure protection of business and technology assets
- Defense in-depth protection of data and privacy for recipient and provider information

The FX is using a systematic, risk averse approach to execute the transition that will make the statewide Medicaid Enterprise vision a reality. The transition plan follows and builds upon Agency FX Procurement Approach that initially focuses on replacement of the FMMIS:

- Phase 1 - Contract with a SEAS and IV&V Vendor to establish the vision, strategy, standards, and implementation enablers for a FX modular implementation
- Phase 2 - Establish the FX Infrastructure to support
  - Enterprise Integration (e.g., ESB)
  - Enterprise Data Management (e.g., ODS/EDW)
- Phase 3 - Use the FX Infrastructure to implement FX Enterprise system integrations, data sharing, and interoperability between Agency systems, and with other agency systems

- Phase 4 - Implement modular systems and services to improve processing currently performed within the FX Enterprise

FX projects are actively implementing Phase 1 and Phase 2 of the FX procurement strategy. The FX Enterprise integration platform is in place and the Agency is actively pursuing integration services to extend the use of the platform. The specific sequencing of Phase 3 FX Enterprise system Integrations and Phase 4 Module implementations is under evaluation to define specific FX integrations and FX projects. The transition strategy is to leverage the technology enablers implemented in Phase 2 Establish the FX Infrastructure, as the specific capabilities are available. The specific sequencing of integrations and module implementations will consider the impact on the FX strategic priorities and the overall impact and improvement in health care for all Floridians. The sequencing will also consider whether the integrations should initially focus on only FMMIS, Agency Medicaid Systems, all Agency systems, or include considerations of other systems in other agencies. Scope and sequencing of activities will be determined through portfolio management processes described in SEAS deliverable *S-4: Strategic Project Portfolio Management Plan* (SPPMP).

While the SEAS Portfolio Management Process helps the FX make prioritization decisions, the recommendation is for the transition approach to use an incremental *wade in* vs. a *big bang* or *jump in* approach. Preceding significant investment in FX Enterprise integrations and modules, the FX will start small or pilot a small number of FX Enterprise integrations and modules to industrialize the process. The first modules developed for the FX will establish and enable a formal module integration process to mature. The FX Data Management Strategy and FX Technical Management Strategy includes technology implementation recommendations for Phase 2 Establish the FX infrastructure that have significant complexity and organizational impact.

The recommended implementation of technology services that will enable the business are implementation and use of the:

- Integration Platform Technologies
- Operational Data Store
- Enterprise Data Warehouse, Data Marts, Business Intelligence and Analytic tools
- Centralized electronic policy (e.g., rules engine) source of the truth
- Single Sign-on (SSO) and service integration security
- Unified user interface technology, policy, and templates for module use

After the above enabling technology capabilities are established, the Agency will expand availability and access to these tools for integration and migration of:

- FMMIS integrations (e.g., ODS / FMMIS data replication)
- FMMIS business area solutions (e.g., Enrollment Broker, Third Party Liability, Prior Authorization)
- AHCA IT Medicaid Systems Integrations (e.g., AHCA SunFocus, ASPEN)

- FMMIS system and services implementation (e.g., Provider, Recipient)
- AHCA IT Systems modular business capability replacement (e.g., Statewide Medicaid Managed Care (SMMC) Complaint Form)
- External Organization Integrations (e.g., Department of Health (DOH) deaths and births)
- External Organization modular business capability replacements (e.g., eligibility determination, case management, appeals processing, common letter writer module)

A strategic priority of the TMS is a *do no harm* business disruption strategy, which recognizes the importance of maintaining business continuity across the enterprise. Components of FMMIS will remain operational while being incrementally replaced with modules. The Agency expects there could be some residual FMMIS functionality retained or refactored to operate in the FX.

9.2 KEY TRANSITION PRINCIPLES

Incremental Delivery – FX projects will incrementally implement new modules, business, technology, and data services to supplement and replace the functionality of FMMIS business areas and non-Medicaid applications to create the FX.

Maximize Business Value – Module functional scope will be determined on a case-by-case basis and guided by the FX Portfolio Management processes.

Parallel Runtime – New solutions and the legacy systems or applications being replaced must be able to run side by side to satisfy testing and validation requirements.

Contingency Planning – Transitions to new systems and applications, which take over legacy systems and applications, must have a plan to revert to the legacy applications before implementation.

New Modules Use of Integration Platform ESB and Data Services – New modules communicate with other modules, systems, and APIs via web services through the Integration Platform ESB. New modules access existing FMMIS web services via the Integration Platform connection to the FMMIS web services. Communications from modules to legacy systems are also via the Integration Platform ESB. If any legacy systems communicate with new modules, the legacy systems access a registered service wrapper in the ESB and use the messaging and Data Standards of the FX.

New Modules use of Operational Data Store Data Services – New modules access data via data services to the operational data store. Applications and individual users will not access databases directly or have native SQL access to databases.

Minimal Business Disruption – The existing systems and applications on which agency business units depend must remain operational until superseded by new systems and applications which satisfy their business requirements.

9.3 FX Modular Strategy

Strategic Topic 9-1: FX Degree of Modularity describes the direction on the degree of modularity for the FX as it evolves over time.

Degree of Modularity	Timeline				
	Current	2018	2021	2022	2025
Monolithic Integrated Solution from a single vendor	FMMIS	->			Expected Replacement Completion
Multiple Vendor Applications	Enrollment Broker, TPL		FX	->	
Application Modules by Business Area Function	AHCA IT Medicaid			FX	->
Fine-grained Business and Technical Services				FX	
Fine-grained Business and Technical Modular Services and APIs	AHCA IT			FX Preferred	->
Data Services			ODS	RDS / Data Warehouse / Data Marts	->
Micro Services					Revaluate strategy and market adoption

Analysis

The FX modular strategy addresses more than the FMMIS. It also addresses Medicaid-related systems in other agencies and non-FMMIS systems within the Agency. The FMMIS is the integration of multiple systems operated by multiple vendors (e.g., TPL, EBO, PBM, PA are all separate from interChange and Fiscal Agent systems). The core system is built with an SOA architecture. Modularization occurs at a deep level within the application logic which is tightly coupled with point-to-point interfaces. The FMMIS also has external services that are consumed by other state and private systems.

The strategy for the FX modularity future state is to have fine-grained modular services, data services, and micro services exposed through standards-based APIs. This approach aligns with the evolving CMS direction to thinking of modular implementation at a much more granular level.

A key feature of this approach is the flexibility in designing solutions which minimize disruptions to the business of the Agency. The Agency expects modularity to provide more strategic opportunities as the FMMIS transitions to a modular FX.

Strategic Topic 9-1: FX Degree of Modularity

9.4 FX ENABLING TECHNOLOGIES

The FX foundational infrastructure includes five main enabling technologies: the Enterprise Service Bus (ESB) described in Section 3.2.1, Web Services, Service-Oriented Architecture (SOA), Business Rules Engine (BRE), and the Operational Data Store (ODS).

9.4.1 WEB SERVICES

A web service is a reusable software service that interacts with other software components by exchanging standards-based messages. The following are web service standards:

- Remote Procedure Call (RPC)
- Simple Object Access Protocol (SOAP)
- Universal Description Discovery and Integration (UDDI)
- Web Services Description Language (WSDL)
- Extensible Markup Language (XML)

Representational State Transfer (REST) is a web services architectural style based on HTTP verbs. In the W3C Web Services Architecture Working Group Notes Section 3.1.3 Relationship to the World Wide Web and REST Architectures of the W3C Web Services Architecture, Web Services are separated in two major classes.

- REST-compliant web services, in which the primary purpose of the service is to manipulate XML representations of web resources using a uniform set of *stateless* operations
- Arbitrary web services, such as Simple Object Access Protocol (SOAP), in which the service may expose an arbitrary set of operations

It is worth noting that in current usage, REST-compliance does not rely on the message format and resources today are represented in various formats such as JavaScript Object Notation (JSON). Additionally, SOAP can be used in a manner consistent with REST.

MITA leverages industry-standard message enablers of the Application Programming Interface (API) and XML to create its own message formats for special Medicaid transmissions (e.g., Accredited Standards Committee (ASC) X12N Insurance Electronic Data Interchange (EDI) Standards). A set of standardized messages replace the individual point-to-point interfaces. All interface modifications are local to a single set of interfaces for consistent maintenance.

The MITA Framework standardizes the use of XML-based message interchange among business services and across organizational boundaries. XML messages are self-documenting, where each field in the message has a tag that defines the field (e.g., a field with the tag *Last_Name* contains a person's last name). Consumers of a message look for and use fields required for their processing and may ignore optional or situational fields; therefore, if the

stakeholder adds a new field (e.g., *Middle_Initial*), there is no need to modify the consuming service. This approach minimizes the effort to implement changes to FX systems.

9.4.2 SERVICE-ORIENTED ARCHITECTURE (SOA)

SOA is a design principle that uses business functions and selected technical functions through documented interfaces. SOA is an architectural framework that integrates many different technologies. MITA requires the use of a modular, flexible approach to systems development. Modularity is breaking down systems requirements into component parts. Extremely complex systems can be developed as part of a SOA.

The ESB provides the key functions required for realizing a SOA:

- **Message Management** – This consists of reliable delivery of messages between services and built-in recovery.
- **Data Management** – This involves converting all messages between services to a common format and converting the common format to the application-specific format, within a service. To ensure interoperability, the message format uses XML standards. Stakeholders define information sharing and event notification standards to allow aggregated and integrated information.
- **Service Coordination** – This consists of orchestrating the execution of an end-to-end business process through all required services on the ESB. Services adapt to changes in environment and support a standards-based set of service management capabilities.

The system invokes each service in a standard way using one or more messages and each message results in the invocation of one of the documented functions supported by the service, regardless of deployment details.

In a SOA, systems invoke business functions as services with standard, message-driven interfaces. Systems can invoke services or reuse them in a platform-independent manner across the enterprise.

Existing applications are wrapped and invoked as service-provider systems. The linking between service consumers and service providers can happen at run time via a service registry. A new deployment or modification can replace an individual service without affecting the rest of the enterprise.

9.4.3 BUSINESS RULES ENGINES

Business rules engines are an effective way to make rapid changes to the logic of the system. A major benefit of rules engines is that logic is external to system application program code. MITA requires the separation of business rules from core programming, and the availability of business rules in both human and machine-readable formats.

The Agency's recommended strategy is to use a business rules engine implemented as part of IS/IP to separate business rules from core programming and provide information about the

change control process that will manage development and implementation of business rules. This strategy allows the Agency to accommodate changes to business rules on a regular schedule and on an emergency basis. Business rules that have cross state value may be submitted to a central federal repository per MITA.

A key recommendation of the T-1: *Data Management Strategy* is to establish a single source of policy truth including data edits, data transformations, and business rules. The TMS is to use business rules engines to create policy services that provide the single source of policy truth that is reusable and decoupled from specific applications. This goal is a potential FX project that may include:

- Create inventory of all locations and system implementations of policy
- Extract policy maintained in existing rules engines and custom code
- Validate system implementations of policy
- Migrate policy implementations to reusable services
- Modify systems to use the services that contain policy implementation
- Establish the organizational structure and resources that validates and tests the implementation of policy used by systems and services

The long-term strategy is that reusable policy services use the IS/IP implemented enterprise rules engine, Oracle Policy Automation (OPA), to decouple all system implementations of policy from proprietary applications. The strategy recognizes that some COTS products may use proprietary rules engines. If a COTS product is the definitive source of policy, FX would provide guidance to expose the rules and policy as a reusable service that is accessible by other modules or systems via the ESB. If a COTS system requires internal use of business rules, the strategy would be for the COTS module to consume the business rules from the enterprise service for use in the COTS module internal service.

9.4.4 FAST HEALTHCARE INTEROPERABILITY RESOURCES (FHIR) ADOPTION

FX will align with the FHIR defined messaging formats. The FHIR standards shall be used to construct the data services APIs for information exchange. The FHIR API's will be used between the Operational Data Store (ODS) and the module vendors for real time/near real time data exchanges. The FHIR APIs will use the vocabulary defined in the United States Core Data for Interoperability (USCDI) FHIR Core Implementation Guide (US FHIR Core IG) as their standardized set of health data classes and constituent data elements.

9.4.5 CUSTOMER RELATIONSHIP MANAGEMENT (CRM)

CRM is a strategy that uses technology to organize, automate, and synchronize business processes. Originally applied in the private sector to determine the needs of company clients, this concept extends to the Health Care Insurance Industry. As applied in the MITA Framework, this concept focuses on recipient and provider access to Electronic Health Record (EHR) data and individual access to health insurance alternatives. Some areas that require CRM include:

- EHR
  - An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards, and that authorized clinicians and staff across more than one healthcare organization can create, manage, and consult.
- Health Information Exchange (HIE)
  - The electronic movement of health-related information among organizations according to nationally recognized standards.

9.4.6 OPERATIONAL DATA STORE (ODS)

The Operational Data Store establishes a single source of the truth for transactional data. Data in the ODS is independent of a specific application or system. For this reason, after migration to the ODS, the Agency can replace a module from one vendor with modules from another vendor. Applications access data in the ODS using data services or API calls as opposed to passing SQL language directly to a proprietary database. The ODS is implemented on the Amazon Web Service (AWS) Aurora platform. Primary information on the ODS is in the FX Data Management Strategy Deliverable and **Strategic Topic 9-1: FX Degree of Modularity** .

.

SECTION 10 STATE SPECIFIC MITA ADDITIONS

The FX has considered the following additions of new functionality and will be watching for advancements of technological capabilities to leverage in the future. While these additions are not integrated into the current timeline, the Technology Management Strategy recommendation is that they be explored as possible additions to the FX future state as mature, industry-specific offerings appear in the vendor landscape.

10.1 COGNITIVE SERVICES

Cognitive Services is an emerging area which delivers cognitive computing technologies based on artificial intelligence and signal processing. Cognitive Services includes two rapidly evolving technologies: Machine Learning (ML) and Natural Language Processing (NLP), which are subfields of Artificial Intelligence (AI) computing. Machine Learning attempts to allow systems to adapt their behavior through learning from previous results and are useful for classification and predictive problems. Natural Language Processing attempts to comprehend human languages and respond in appropriate ways; translators, voice response systems, and chatbots depend heavily on NLP.

Exhibit 10-1: Cognitive Services Use Cases depicts example cognitive services use cases.

Exhibit 10-1: Cognitive Services Use Cases

10.1.1 Machine Learning

As the Agency upgrades to a modular infrastructure and some systems move toward cloud, the application of machine learning technologies becomes increasingly relevant and accessible. Major cloud service providers (CSP) have accessible machine learning offerings as a service. The Agency could use these solutions to reduce improper payments, improve recipient care by detecting important patterns in recipient data, or offer an Artificial Intelligence (AI) chatbot that improves customer service.

Real-time Improper Payment Detection and Prevention – Bad actors constantly increase the sophistication and speed at which they perpetrate fraud. Increasingly their techniques are tactical and focused on quick gains and result in lower risk of detection and reduced opportunities for the recovery of losses. Applying machine learning to the examination of FX information (e.g., new claims and provider enrollment applications) could allow proactive identification and prevention. The enabling technologies learn to identify new techniques or new patterns in real time as they emerge to help to avoid the improper payments or improve the coordination of care.

Predictive Recipient Outcomes – Datasets including recipient demographics, diagnosis, admissions, procedures, vitals taken at doctor visits, history of medications, and lab results could be created using anonymized recipient data. Machine learning could be applied to predict which recipients are more at risk for being hospitalized, develop substance dependencies, or are at risk of having a heart attack. Once identified, these recipients could be candidates for health interventions via education, treatment, or services which could prevent the adverse outcome.

10.1.2 AI Chatbots

Customer Service AI Chatbots – AI chatbots make use of Cognitive Computing technologies, like Natural Language Processing and Machine Learning, to interpret user requests and mimic human conversation to respond to those requests. Chatbots could be deployed to tackle routine questions about providers, benefits, or enrollment. More complex chatbots could be deployed to answer questions like provider requests for recipient eligibility, that helps to remediate a claim or encounter, or directs recipients to care options.

10.1.3 Behavioral Economic Based User Interfaces

Behavioral economics is the study of the effects of psychological, cognitive, emotional, cultural, and social factors on the economic decisions of individuals and institutions and how those decisions vary from those implied by classical economics theory. An assumption of classical economics is that people and organizations make decisions that create the most value for themselves. Behavior economic studies have found that often people and organizations make decisions that are not in their best interest. These studies attempt to identify and leverage decision making factors that are unanticipated to cause people to take actions that create desired behaviors. Often the presentation of information can suggest or nudge people to make decisions and taking actions that improve their situation. Because the above factors and social, influencer, personality style and other factors are different for each person or organization, it

may be necessary to present information to different audiences in different ways. Ongoing analysis of user actions and behaviors based on presentation that considers behavioral economic factors will identify opportunities to optimize user interface and content presentation to improve healthcare for Floridians.

10.1.4 Voice Assistant-Based User Interfaces

Use of voice assistants (e.g., SIRI, Amazon Alexa, Google Assistant, Cortana) as a user interface is increasing in the general population. Currently, interactions are primarily initiated by users to request information. Voice assistant-initiated communications of external events and behavioral suggestions are expected to increase in frequency, maturity, and sophistication for the next several years.

Recognizing the growing use of this user interaction channel, the Agency will consider solutions and data management strategies that support the expected increased use of voice assistants, especially for recipient communications.

10.2 Changes in Organizational Liability Related to Data Ownership, Possession or Access

Historically data is most organizations most precious asset. Data about recipients / customers, providers, internal processes, and employees has been a valuable asset that allows health plans and service providers to offer differentiated or *better* service. This data also provides competitive advantage to market to customers of competitors. While data has been an asset with minimal downside other than the cost of collection, a changing legal landscape is likely to alter the cost and liability of possessing or having access to data.

Organizational liability resulting from data ownership, possession, or access is expected to increase raising the cost of malpractice insurance and the costs from the practice of *defensive medicine*. Litigants will increasingly pursue awards and damages for a rising standard of care where simply possessing data increases expectations of accountability to act on the data or act on algorithm-based analysis of data that service providers have or have access to.

The increased liability from having access to information has been one barrier to electronic health records exchange. Other states have applied creative solutions to reduce the liability from collecting, possessing, and sharing information including limiting liability of information provided to Health Information Exchange (HIE) solutions.

The Agency will continue to monitor the impacts of changes in provider liability resulting from data ownership, possession, and access and seek to implement reasonable strategies to optimize delivery of health care for Floridians.

SECTION 11 APPENDIX A – FX SYSTEM UI STANDARDS

The FX System UI Standards document referenced in Section 3.2.6 is available as Attachment A to this document and located in the FXPR at FX Hub > Standards & Plans> Category: Technology > Technical Management Strategy (T-4).