

Florida Health Care Connections (FX)
MMIS Concept of Operations
(MMIS ConOps)

Version: 100
Last Modified: February 26, 2019

Document Number: Phase II EDW and IS/IP v100

TABLE OF CONTENTS

SECTION 1	INTRODUCTION.....	1
SECTION 2	REFERENCED DOCUMENTS	1
2.1	CURRENT SYSTEM.....	2
2.1.1	<i>Functional Description</i>	<i>2</i>
2.1.2	<i>User Community Description.....</i>	<i>3</i>
2.1.3	<i>Technical Architecture.....</i>	<i>4</i>
SECTION 3	GOALS, OBJECTIVES, AND RATIONALE FOR NEW OR SIGNIFICANTLY MODIFIED SYSTEM.....	6
3.1	PROJECT PURPOSE	6
3.2	SYSTEM GOALS AND OBJECTIVES	7
3.3	PROPOSED SYSTEM.....	8
3.3.1	<i>System Scope</i>	<i>9</i>
3.3.2	<i>Business Processes Supported</i>	<i>10</i>
3.3.3	<i>High Level Functional Requirements.....</i>	<i>11</i>
SECTION 4	SCENARIOS ANALYSIS.....	13
SECTION 5	FACTORS INFLUENCING TECHNICAL DESIGN	18
5.1	RELEVANT STANDARDS.....	18
5.2	ASSUMPTIONS, DEPENDENCIES AND CONSTRAINTS.....	18
5.3	AGENCY GOALS AND OBJECTIVES	21
5.4	DESIGN GOALS	22
SECTION 6	PROPOSED SYSTEM.....	23
6.1	TECHNICAL SOLUTION ALTERNATIVES.....	23
6.2	RATIONALE FOR SELECTION.....	23
6.3	RECOMMENDED TECHNICAL SOLUTION.....	24
6.4	PROPOSED SOLUTION DESCRIPTION.....	26
6.5	CONTEXT DIAGRAM.....	27
6.6	HIGH-LEVEL OPERATIONAL REQUIREMENTS AND CHARACTERISTICS.....	27
6.6.1	<i>User Community Description.....</i>	<i>27</i>
6.6.2	<i>Non-Functional Requirements</i>	<i>29</i>
6.7	HIGH LEVEL ARCHITECTURE & ALTERNATIVES ANALYSIS.....	34
6.7.1	<i>Application Architecture</i>	<i>37</i>
6.7.2	<i>Information Architecture.....</i>	<i>38</i>
6.7.3	<i>Interface Architecture</i>	<i>42</i>
6.7.4	<i>Technology Architecture.....</i>	<i>43</i>
6.7.5	<i>Security and Privacy Architecture</i>	<i>45</i>
SECTION 7	ANALYSIS OF THE PROPOSED SYSTEM.....	47
7.1	IMPACT ANALYSIS	47
7.1.1	<i>Operational Impacts.....</i>	<i>47</i>

7.1.2 *Organizational Impacts*..... 48
7.1.3 *Risks* 49
7.1.4 *Issues to Resolve* 53
7.1.5 *Critical Success Factors for Remainder of Project*..... 56
SECTION 8 GLOSSARY.....**57**
SECTION 9 APPENDICES.....**59**

LIST OF FIGURES

Figure 1: Medicaid Ecosystem.....	3
Figure 2: Current Conceptual Technical Architecture.....	5
Figure 3: FX Strategy Articulation	8
Figure 4: FX Modular Transformation	9
Figure 5: FX Transformation Model.....	13
Figure 6: Transformation Foundation.....	13
Figure 7: Project Portfolio Management.....	16
Figure 8: TSRG Standards Hierarchy Example.....	18
Figure 9: Context Diagram	27
Figure 10: Conceptual Technical Architecture Diagram	37
Figure 11: Multilayer Application Architecture Model.....	38
Figure 12: National Information Exchange Model	40
Figure 13: Conceptual Data Model Sample.....	41
Figure 14: Conceptual View of Multiple Environments.....	44
Figure 15: FX Security Description.....	47
Figure 16: Risk Management Process.....	50

LIST OF TABLES

Table 1: Supported Business Processes	11
Table 2: User Community Description	28
Table 3: Security and Privacy Standards	30
Table 4: System Availability Requirements	31
Table 5: Current Volumetric Capacity.....	32
Table 6: Performance Expectations	33
Table 7: Solution Design Alternatives	36
Table 8: MMIS Interfaces	43
Table 9: Risk Management Activities.....	52
Table 10: Solution-related Risks.....	53
Table 11: Issues and Action Items Roles and Responsibilities.....	54
Table 12: Critical Success Factors	56

SECTION 1 INTRODUCTION

The Florida Agency for Health Care Administration (AHCA or Agency) is continually looking to fulfill its Mission of providing “Better Health Care for all Floridians.” As part of this Mission, the Agency is transforming the Medicaid Enterprise System (MES), the group of systems that deliver Medicaid Program services. This initiative is known as the Florida Health Care Connections (FX). Unlike a typical system replacement where the implementation team implements the existing functionality into a new system, the Agency is developing an approach to transform the MES driven by strategic thinking about the future of healthcare delivery, innovation in Information Technology (IT), and delivery of the best and most efficient service to Florida’s providers and recipients. Transforming the MES into a modular environment allows the Agency to procure individual solutions that will best meet the needs of Floridians for years to come, while providing a solution that is flexible enough to meet the challenges and opportunities created by the ever-changing healthcare, policy, and technology landscapes.

As described in the FX Procurement Strategy, the Florida MES is defined as the business, data, services, technical processes, and systems necessary for the administration of the Florida Medicaid program. The Florida Medicaid Management Information System (FMMIS) has historically been a single integrated system of 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 current Florida MES includes the Medicaid Management Information System (MMIS) and separate systems that function to support Florida Medicaid and the Agency. Agency systems include, but are not limited to, the enrollment broker system, third party liability, pharmacy benefits management, fraud and abuse case tracking, prior authorization, home health electronic visit verification, provider data management system, and Health Quality Assurance (HQA) licensure systems. The Florida MES also includes interconnections and touch points with systems that reside outside the Agency such as systems hosted by the Department of Children and Families, Department of Health, including Vital Statistics, Department of Elder Affairs, Agency for Persons with Disabilities, Florida Healthy Kids, Department of Financial Services, Florida Department of Law Enforcement, and Department of Juvenile Justice.

SECTION 2 REFERENCED DOCUMENTS

The following documents were referenced in the development of the Florida MMIS Concept of Operations.

- Florida MES Procurement Strategy
- MES Approved Planning Advanced Planning Document (PAPD)
- EDW Project Partnership Understanding
- S-3: Enterprise Systems Strategic Plan
- S-4: Strategic Project Portfolio Management Plan
- MITA Concept of Operations
- P-1: Revised MITA State Self-Assessment and Update Process
- T-1: Data Management Strategy

- T-2: Information Architecture Documentation
- T-4: Technical Management Strategy
- T-5: Technical Architecture Documentation
- T-6: Technology Standards
- T-7: Design and Implementation Management Standards
- T-8: Enterprise Data Security Plan
- Draft Integration Services and Integration Platform Invitation to Negotiate
- Draft Enterprise Data Warehouse Invitation to Negotiate

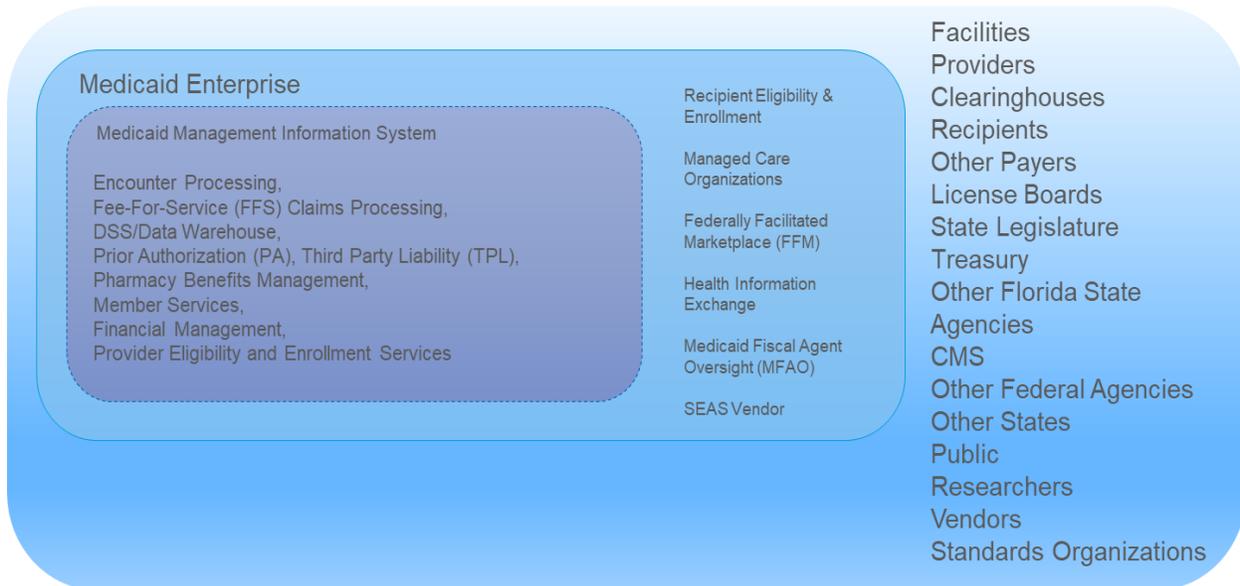
2.1 CURRENT SYSTEM

2.1.1 FUNCTIONAL DESCRIPTION

The Florida Medicaid Enterprise System is a collection of many systems each with its own platform, systems architecture, and proprietary data stores. The systems in the MES are islands of processing and information. Data exchange provides the bridge between these systems. The current Medicaid Enterprise uses the MMIS and multiple systems and functions integrated or interfacing with the MMIS, such as Automated Health Solution (AHS) HealthTrack system, the Health Information Exchange (HIE), the Federally Facilitated Marketplace (FFM), and care management organization systems. **Figure 1: Medicaid Ecosystem** summarizes Florida's MMIS which encompasses mission critical business systems upon which the Medicaid Enterprise and Medicaid ecosystem depend.

This current state can be categorized as follows:

- Providers, health plans, and Agency systems primarily submit information to MMIS through Electronic Data Interchange (EDI) and Secure File Transfer Protocol (SFTP) batch transmissions
- Pharmacy Benefits is operated by an outside vendor, Magellan
- The enrollment broker vendor is Automated Health Solutions. AHS operate both the Choice Counseling call center to enroll recipients in health plans and the Provider Network Verification (PNV) system to monitor health plan provider networks' adequacy
- Other Florida Agencies perform Medicaid processes using replicated Medicaid data; primarily using batch interfaces
- The Decision Support System (DSS) is the data warehouse that supports analytics, ad hoc inquiry and management, and administrative reporting
- The HIE system enables provider-to-provider exchange of information
- The system lacks a 360-degree view of recipient information or alerting of changes in social determinants of health data

MEDICAID ECOSYSTEM – Stakeholders and Other entities**Figure 1: Medicaid Ecosystem****2.1.2 USER COMMUNITY DESCRIPTION**

Listed below is the description of the user community:

- Agency staff access the MMIS to perform assigned daily activities. These include, but are not limited to, assisting members with questions about benefits and enrollment, billing issue resolution for Medicaid providers, enrollment for new providers into the Medicaid program, and creation of new accounts receivables and expenditures
- Other Agency staff access the MMIS and Decision Support System (DSS) to complete tasks such as researching Medicaid eligibility, assisting with system change requests, and gathering data for use in fraud and abuse determinations
- External organizations access the MMIS to update eligibility spans, submit claims, verify Medicaid eligibility, and identify potential fraud
- Providers access the MMIS for multiple reasons such as, enrolling as a Medicaid provider, verification of recipient eligibility, claims submission, and confirmation of claim payment status
- Billing Agents submit claims on behalf of Medicaid providers through various Clearinghouses for processing by MMIS
- Health plans access the MMIS to verify Medicaid eligibility, submit encounter transactions and to research encounter errors
- Agency staff use DSS and its components for data needs that include but are not limited to analyzing data for the impact of policy changes, forecasting, program performance, and reporting information to all stakeholders including CMS

- Other Agency staff access DSS to verify data integrity, research data issues, forecast program expenditures, and provide ad hoc data requests for other internal and external entities
- External organizations and community partners access DSS to obtain reports and datasets for a variety of research and/or litigations involving Medicaid membership

2.1.3 TECHNICAL ARCHITECTURE

The information technology that supports the operation of the Medicaid program is distributed across many state agencies, health plans, and provider systems. There are hundreds of state agency computer systems and thousands of provider systems that must work together to deliver healthcare services to the people of Florida. In this highly distributed technology landscape, there is substantial duplication and inconsistencies of information and processing across systems.

Currently 10 state agencies have direct responsibilities in processing or supporting the operation of the Medicaid program. Within the Agency alone, there are more than 140 computer systems or applications in operation. More than 80 of these systems play a direct role supporting the operation of the Medicaid program. A complete list of MMIS interfaces can be found in Appendix C.

The current Medicaid Enterprise contains several primary components including Electronic Data Interchange (EDI), the MMIS/DSS, interChange User Interface (UI), and the Prescription Benefits Management System (PBMS), all of which are built around Service Oriented Architecture (SOA) principles.

Electronic Data Interchange (EDI) manages the flow of the various X12 transactions into and out of the Medicaid Enterprise. EDI utilizes BizTalk and Simple Object Access Protocol (SOAP) servers, mapping X12 transactions into proprietary XML file structures for processing in the MMIS.

The largest system in the Medicaid Enterprise is the MMIS/DSS, currently operated by the fiscal agent, DXC / Enterprise Systems, LLC. The MMIS components of the system are comprised primarily of a collection of custom-built software applications used for processing Medicaid claims and encounter transactions. This processing includes the adjudication of claims and encounter transactions via batch processes and online submissions, the processing of financial transactions, producing and distributing payments, the storing and utilization of provider and recipient enrollment and demographic data, and the implementation of business rules and supporting reference data.

The DSS components of the system are comprised of a collection of Extract, Transform and Load (ETL) programs written in the C programming language, a set of Business Intelligence tools, and an Oracle database. The DSS provides the tools necessary for analytics and reporting.

The technologies utilized in the implementation of the MMIS/DSS include Windows, and HP-UX operating systems, Oracle and SQL Server databases; Commercial-off-the-Shelf (COTS) products such as Business Objects, Crystal Reports, SPSS, and ArcView GIS; programming languages

include C, C#, VB.NET, Javascript, Perl, VBScript, R and SAS. The MMIS/DSS system is hosted at a commercial data center in Orlando, Florida.

The interChange User Interface (UI) is a web-based solution developed with Microsoft.NET technologies. The UI allows highly detailed access to all Claims, Provider, Recipient, Financial and Reference data stored in the MMIS. Authorized users also have update capabilities to relevant data.

The Prescription Benefits Management System (PBMS) is a Point-of-Sale (POS) Pharmacy Claims processing system operated and maintained by Magellan Health Services. Currently the PBMS is comprised of proprietary software running on a UNIX platform with an Oracle Database from a data center in Maryland Heights, Missouri. This system receives and adjudicates Point-of-Sale NCPDP D.0 claims transactions which are subsequently transmitted via Secured File Transfer Protocol (SFTP) to the MMIS for payment. Users interact with pharmacy data via interChange or by means of FirstRx, a proprietary user interface operated by Magellan Health Services.

The number of agencies and systems that access and manage data used for healthcare delivery is likely to expand significantly. These agencies exert significant effort processing system-to-system interfaces to extract, load, and update information in one system with information from another system. Because of the many systems in operation, there is not a reliable “single source of truth” to make processing, reporting, policy analysis, investigation, or analytic decisions. Differences in data timeliness, data validation, data transformation, and application of policy within systems means reports and data analysis vary depending on which system performs the analysis.

Figure 2: Current Conceptual Technical Architecture provides a current state overview of the major components of the MMIS/DSS systems and interfaces with those systems.

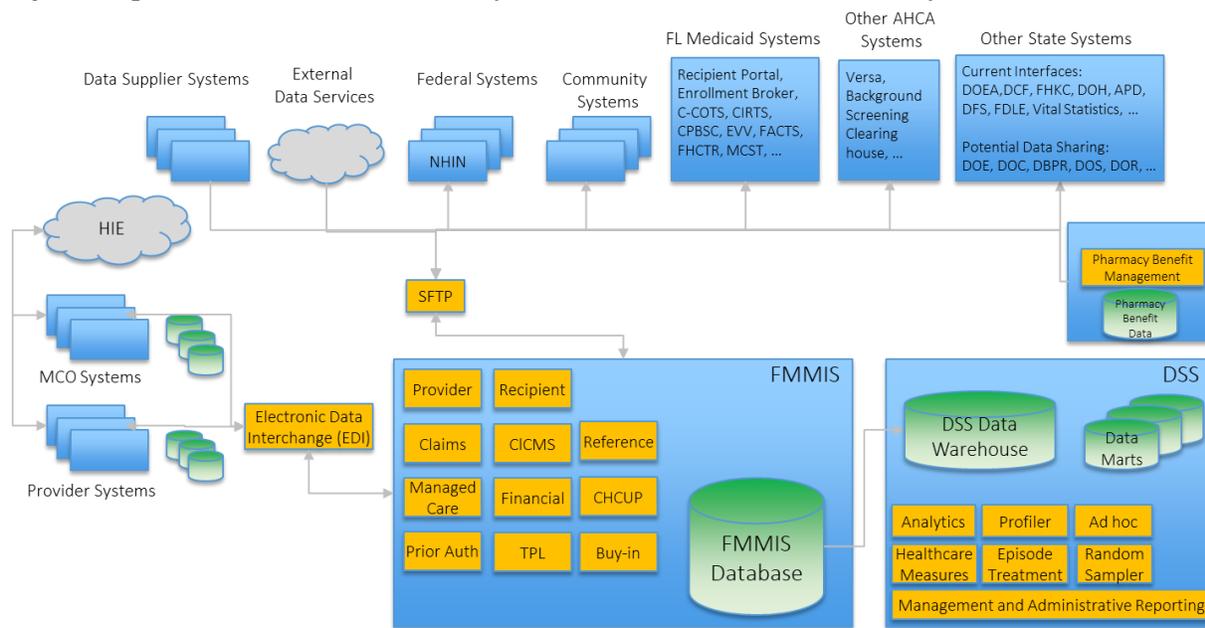


Figure 2: Current Conceptual Technical Architecture

SECTION 3 GOALS, OBJECTIVES, AND RATIONALE FOR NEW OR SIGNIFICANTLY MODIFIED SYSTEM

3.1 PROJECT PURPOSE

The objectives of Phase I of the FX were to procure a Strategic Enterprise Advisory Services (SEAS) Vendor and an Independent Verification and Validation (IV&V) vendor. Additional objectives of Phase I included operating an interim Project Management Office (PMO) using existing Agency resources in the Bureau of Medicaid Fiscal Agent Operations in advance of the SEAS Vendor, and extending the current fiscal agent contract beyond the current end date of June 30, 2018 to ensure the continued operation of the MMIS/DSS during the transition period of the MES.

The objectives of Phase II of the FX transformation program include procurement(s) of an Integration Services / Integration Platform (IS/IP) and an Enterprise Data Warehouse (EDW). The IS/IP will provide the technical expertise to ensure the integrity and interoperability of the FX transformation program by performing technical systems integration in coordination with multiple vendors providing the technology solutions. The IS/IP platform will provide a standards-based integration platform to connect diverse applications and enable a common information exchange process between systems.

The EDW will provide data warehousing and data integration capabilities for data to be shared across systems and will replace the current DSS. The Agency is designing a comprehensive EDW solution that is architected to provide greater reuse of information, broader and easier access, enhanced data integration, increased security and privacy, and strengthened query and analytic capability by building a unified data repository for reporting and analytics.

The objective of Phase III of the FX transformation program is to integrate services and systems within the Medicaid Enterprise through and under the direction of the IS/IP vendor. The systems that currently exist in the MES primarily interact through the exchange of data files, using Secured File Transfer Protocol (SFTP). These point-to-point interfaces become more complex and costlier as the number of systems and applications increase and are prone to data redundancy, information delays, and data incompatibility issues. To facilitate effective data flow, the IS/IP will act as the communication broker and web services orchestrator to provide data sharing and routing intelligence for the FX.

The objective of Phase IV of the FX transformation program is to procure modules to replace business processes within the MMIS that are interoperable with other systems within the MES, using open source solutions, COTS products, or other modular approaches that reduce the need for custom development. As Phase IV, Module Acquisitions, completes in approximately five (5) years, the functions that are currently performed in the fiscal agent contract, the MMIS, or the DSS, will be replaced with a modern group of modules that will provide a greater cost benefit and the flexibility of choice of vendors that will enhance the operations of the Medicaid Enterprise.

3.2 SYSTEM GOALS AND OBJECTIVES

Agency executives developed the FX Vision by tying the FX Strategy to the overall Mission, Vision, and Goals of the Agency. The Agency's Mission is "Better Health Care for all Floridians." The Agency's Vision and long-range goals support the Mission. The Agency's Vision is "A health care system that empowers consumers, that rewards personal responsibility and where patients, providers, and payers work for better outcomes at the best price."

Agency executives collaborated with the SEAS Vendor to create the FX Vision and supporting Guiding Principles. As a result, the FX Vision and Guiding Principles support the Agency's Mission, Vision, and Goals to effectively guide the Agency's investment decisions during the transition to a modular environment.

The Agency's FX Vision is to "Transform the Medicaid Enterprise to provide the greatest quality, the best experience, and the highest value in health care."

The Agency's FX Guiding Principles are the principles that must be adhered to if the FX Vision is to be achieved. They therefore support the FX Vision and are as follows:

- Enable high-quality and accessible data
- Improve healthcare outcomes
- Reduce complexity
- Use evidenced-based decision making
- Improve integration with partners
- Improve provider and recipient experience
- Provide good stewardship of Medicaid funds
- Enable holistic decision making rather than short-term focus

The FX Guiding Principles are, in turn, supported by Strategic Priorities which define the areas of practical importance to achieve the FX Vision. The FX Strategic Priorities are:

- Integration Components
- Provider Experience
- Recipient Experience
- Program Integrity
- Financials (and analytics)
- Value-Based Care
- Inter-agency Focus

Figure 3: FX Strategy Articulation depicts a single page view of the vision, guiding principles, and strategic priorities.

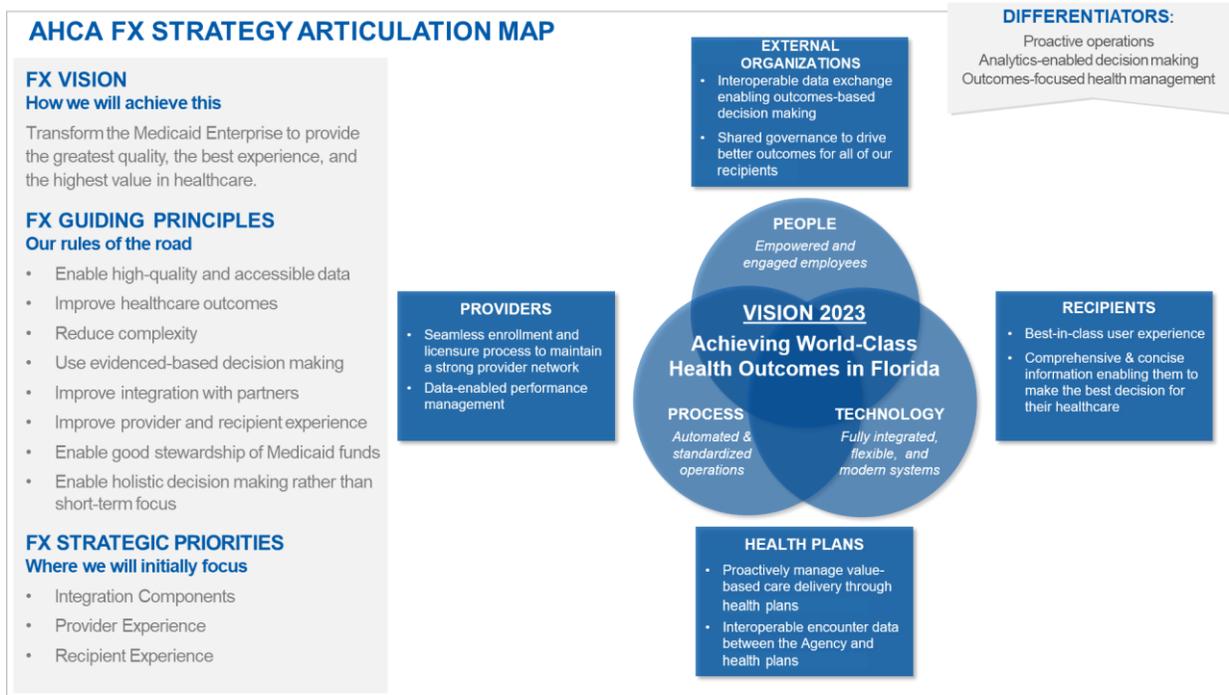


Figure 3: FX Strategy Articulation

The Centers for Medicare and Medicaid Services (CMS) Modularity Standard requires the Agency to move away from the current large, highly complex, and highly customized MMIS enterprise systems and towards smaller, less customized modules. To enable this modular environment, the Agency must deploy standards-based data exchange and information architecture to enable systems to communicate effectively with one another in an interchangeable manner. This will enable the Agency to improve consistency around system functionality and service by easily modifying systems independently of the rest of the enterprise.

3.3 PROPOSED SYSTEM

The FX transformation program proposes a phased approach to replace the current functions of the MMIS based on the CMS Standards and Conditions to ultimately transition to an interoperable and unified Medicaid Enterprise where individual processes, modules, sub-systems, and systems work together to support the Medicaid program. The FX transformation program will replace large, core aspects of the existing MMIS and fundamentally change Medicaid business processes for the better across multiple stakeholder groups encompassing recipients, providers, and Agency staff.

The recommended business solution for Phase I of the FX transformation program was to procure a SEAS Vendor to obtain the expertise needed to develop the framework for the Medicaid Enterprise in accordance with the CMS conditions and standards, including MITA 3.0, and facilitate the interoperability of business and technical services across the Medicaid Enterprise. The scope of work for the SEAS Vendor includes strategic, programmatic, and technical advisory services to support the phased approach to the FX transformation program. The Agency procured

the SEAS Vendor, and the contract was executed in September 2017. The Phase II business solution for the FX transformation program includes IS/IP and EDW procurements. The Phase III solution aims to integrate services and systems within the Medicaid Enterprise through the IS/IP vendor. The objective of Phase IV is to procure modules to replace business processes within the MMIS that are interoperable with other systems within the Medicaid Enterprise, using open source solutions, COTS products, or other modular approaches that reduce the need for custom development.

Figure 3: FX Strategy Articulation depicts the Medicaid Enterprise future state modular environment.

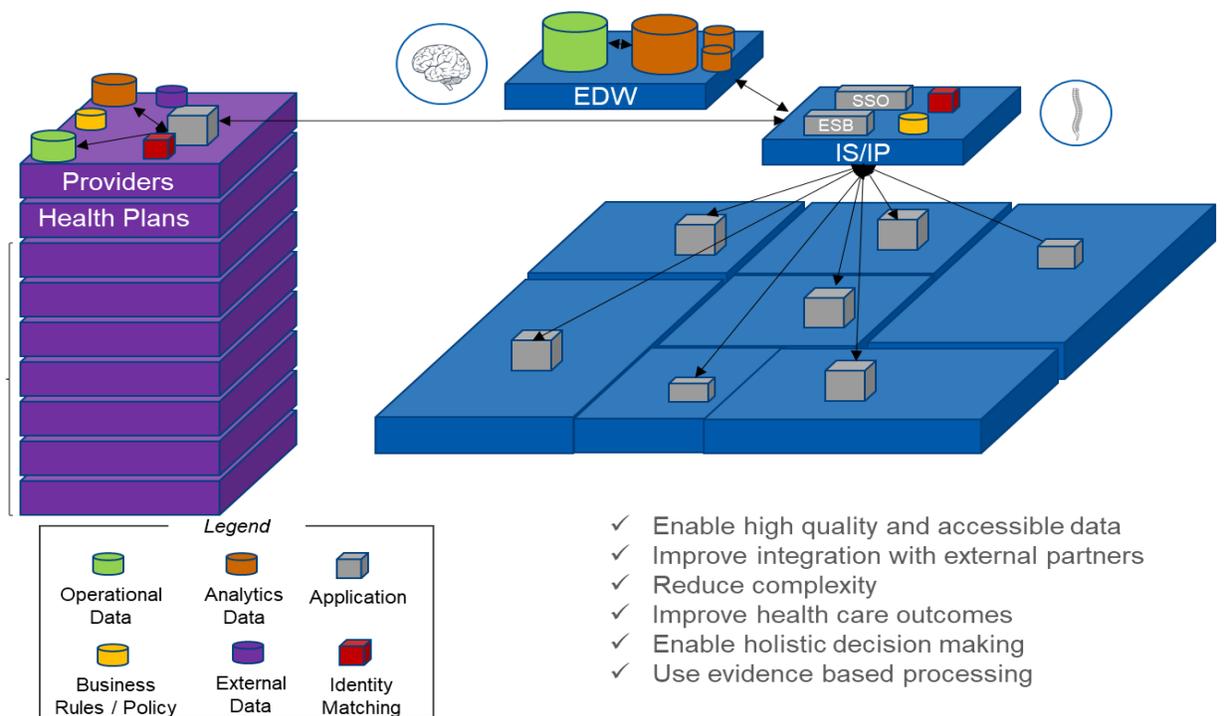


Figure 4: FX Modular Transformation

3.3.1 SYSTEM SCOPE

The proposed technical solution is to procure modules to replace business processes within the MMIS that are interoperable with other systems within the FX transformation program, using open source solutions, COTS products, or other modular approaches that reduce the need for custom development. Proposed solutions include the EDW and IS/IP, and may include modular procurements for Recipient Management, Provider Management, Financial Management, Encounter Processing, and Claims Processing.

The proposed solution supports the FX Data Management Vision which emphasizes six primary strategies that align with the overall FX strategic priorities:

- Improve data quality by operating from a single source of policy truth
- Evolve core processing with data validation at the point of business event data collection
- Provide seamless access to a real-time, 360-degree view of recipient and provider information
- Decouple data from proprietary systems and application stores
- Operate with business area and persona optimized data marts and data analysis tools
- Prepare to collect and manage recipient and provider experience and outcome data

3.3.2 BUSINESS PROCESSES SUPPORTED

The project was initially conceived as a MMIS replacement. However, through the strategic planning process the Agency determined that the Medicaid Enterprise required a comprehensive transformation to fulfill its mission of providing “Better Health Care for all Floridians” while meeting evolving federal requirements and standards and responding to a changing healthcare landscape. The FX transformation program is not only transformative for the Agency, but will improve how FX business process are conducted, thereby affecting Agency staff, other agencies, providers, plans, and recipients.

Through the 2014 State Self-Assessment (SS-A) development, the Agency along with consultants procured to assist with the process, conducted Requirement Analysis and Development sessions to completely describe the business process needs for the FX transformation program. The 2018 SS-A update focused on the business processes associated with the near-term strategic priorities of the EDW, IS/IP, and Provider Services, which drive progress towards the Agency’s goals of improving data quality, promoting modularity, and enhancing provider experience. While the SS-A captures high-level business process requirements, solicitation documents for module procurements and other projects will define the detailed requirements. **Table 1: Supported Business Processes** shows the business processes selected for reassessment in 2018.

ENTERPRISE DATA WAREHOUSE	PROVIDER MODULE
<ul style="list-style-type: none"> ▪ BR03 – Manage Business Relationship Information ▪ CM02 – Manage Case Information ▪ CO01 – Manage Contractor Information ▪ FM06 – Manage Accounts Receivable Information ▪ FM13 – Manage Accounts Payable Information ▪ FM17 – Manage Budget Information ▪ ME01 – Manage Member Information ▪ OM28 – Manage Data ▪ OM29 – Process Encounters ▪ PE03 – Manage Compliance Incident Information ▪ PL01 – Develop Agency Goals and Objectives ▪ PL04 – Manage Health Plan Information ▪ PL06 – Manage Health Benefit Information ▪ PL07 – Managed Reference Information ▪ PM01 – Manage Provider Information 	<ul style="list-style-type: none"> ▪ EE05 – Determine Provider Eligibility ▪ EE06 – Enroll Provider ▪ EE07 – Disenroll Provider ▪ EE08 – Inquire Provider Information ▪ PM01 – Manage Provider Information ▪ PM02 – Manage Provider Communication ▪ PM03 – Perform Provider Outreach ▪ PM07 – Manage Provider Grievances and Appeals ▪ PM08 – Terminate Provider

Table 1: Supported Business Processes

3.3.3 HIGH LEVEL FUNCTIONAL REQUIREMENTS

The Agency is pursuing a transformative approach to become a data-centric organization. Data has always been critical to the work the Agency, health plans, providers, and external organizations perform. The Agency is changing its treatment of data as an asset to the healthcare ecosystem. Historically, data was a component embedded within a specific system focused on specific business processes. Applications and data were tightly linked, often as isolated islands specific to a business unit or business process. When the Agency replaced applications or the vendors providing processing services, the process to convert or migrate data for use in a new system was complex and difficult.

The approach AHCA is pursuing in its vision is to change the relationship between data and systems. The Agency seeks to make healthcare data a permanent asset that is managed and retained regardless of systems or organizations using the data. The centralization of this important asset will provide a single source for consistent data validation and application of business policy. With this approach, the Agency expects better data quality, expanded use throughout the healthcare ecosystem and increased innovation from stakeholders and the vendor community to improve health care for all Floridians.

The EDW vision recognizes that there are currently—and will likely be ongoing—technical and organizational boundaries requiring data be kept in multiple data stores. The Agency is implementing an Integration Services / Integration Platform (IS/IP) solution to allow information to be stored in multiple data stores in a manner consistent with the Agency’s vision. The IS/IP solution will provide near real-time connectivity to external data sources allowing redundant

information to be accessed and presented in a cohesive view in near real-time. The use of integration services to assemble and consolidate data from multiple sources will help the Agency achieve some of the benefits of its vision as the operational data store grows, and duplicated data is reduced. Over time as operational data is decoupled from application systems, the expectation is the IS/IP platform will integrate fewer and fewer sources (only those external to the operational data store).

Industry technology trends aligned with the EDW vision (e.g. the use of Blockchain) anticipate that eventually all stakeholders in the healthcare ecosystem will contribute and access information from a secure single source. Therefore, the EDW vision contemplates that health plans, providers, and external organizations may ultimately operate from the single source of truth thus reducing internal duplication and processing delays.

The EDW System, as currently envisioned, is comprised of the Operational Data Store (ODS) and Content Management (CM) Repository, the Analytic Data Store, the Persona Optimized Analytics and Reporting (POAR) component, and Specialized Data Stores (SDS). Combined, these components will address the challenges presented by MES Current State.

By providing a single location for all transactional data and digital content retained by the Agency, the Operational Data Store and Content Management Repository strives to rectify the data inconsistencies and multiple versions of “truth” present in the current state.

The Analytic Data Store is comprised of the Reporting Data Store (RDS), the Analytics Data Store, and various Data Marts. These components will provide rapid and timely access to high quality data captured from the ODS via well-defined replication and Extract Transform Load (ETL) processes.

The Persona Optimized Analytics and Reporting component will provide a unified set of tools intended to create consistent analytical, modeling, and reporting processes thereby increasing confidence in the reports and models produced by and for the Agency.

The Specialized Data Stores round out the EDW Solution by providing the capability to efficiently produce data structures and data stores to meet specialized needs of the Agency, (e.g. data requests from external entities such as other state agencies, academic institutions, media outlets).

Together, these components form a cohesive and effective response to the Agency’s need for reliable, accurate, and timely data while also addressing the need for dependable analytics and predictive modeling and forecasting.

Figure 3: FX Strategy Articulation depicts the vision and conceptual design for the future state of the Medicaid Enterprise.

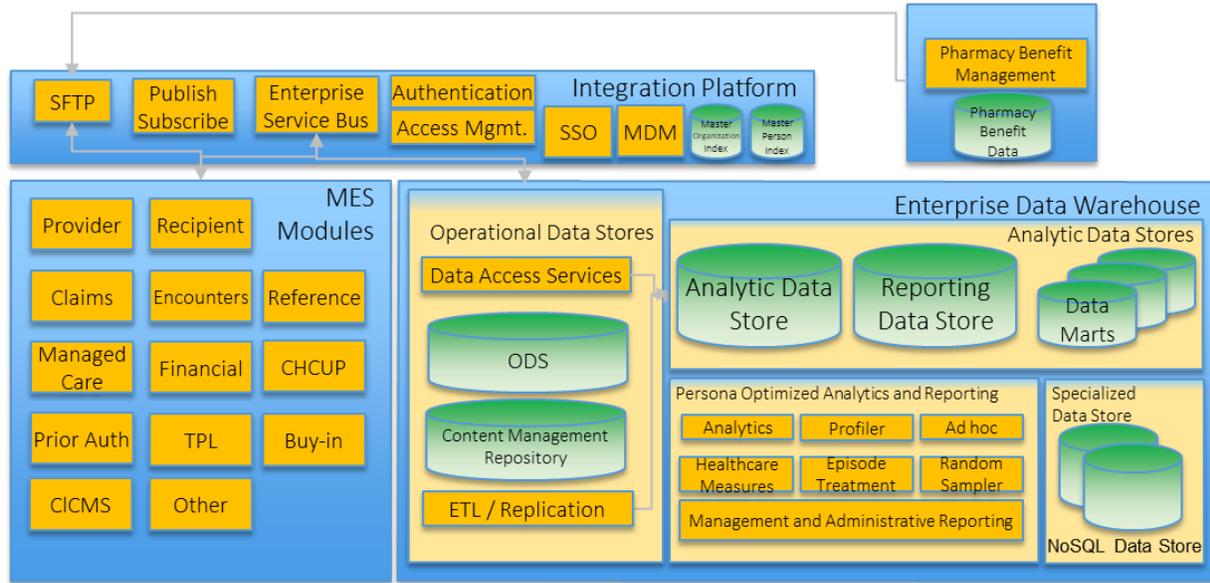


Figure 5: FX Transformation Model

SECTION 4 SCENARIOS ANALYSIS

The Agency’s approach focuses first on building the foundation for transformation through procurement of an Integration Services and Integration Platform vendor and Enterprise Data Warehouse services. The Integration Services and Integration Platform and Enterprise Data Warehouse procurements power the health of the Agency to live in a data driven healthcare ecosystem.

Figure 3: FX Strategy Articulation depicts the functions of the foundational IS/IP and EDW procurements.

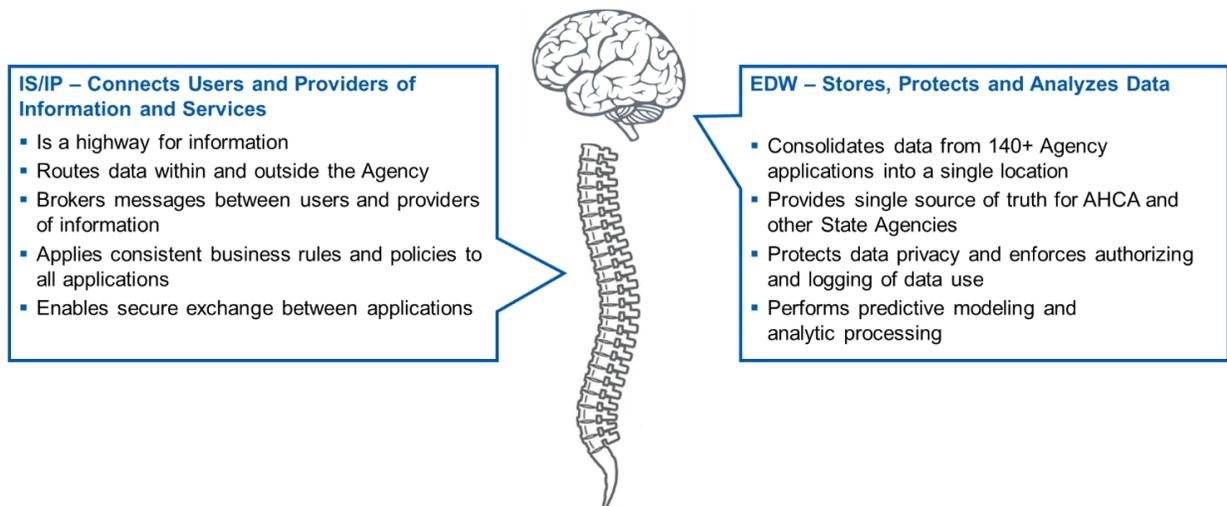


Figure 6: Transformation Foundation

The new IS/IP solution will enable people and systems within and outside the Agency to operate and act with the same information to accelerate service delivery. The Integration Platform consists of several components enabling new and existing systems to access and reuse data and processing across organization and system boundaries.

- Enterprise Service Bus - Validates, authorizes, and connects requestors and providers of data and processing services across the ecosystem
- Master Person/Organization Index - Links master records about a person or organization within or across systems so processing considers all relevant information
- Master User Interface - Provides pages to view and explore available information about a recipient, provider, or organization
- Single Sign-On - Provides internal and external users secure access to applications using a single id
- Enterprise Rules Engine - A repository and processing engine to make processing decisions (e.g. enrollment, pre-authorization, claim approval)
- Publish Subscribe Alerting - Allows systems to communicate information and events that are automatically shared with other organizations or systems

The EDW system will allow the Agency to become a data centric organization and improve data integrity and accuracy. The components of the Enterprise Data Warehouse solution decouple systems and data to make healthcare data available and consistent throughout the ecosystem.

- Operational Data Store - Single source of truth for all transactional information collected and used by systems
- Operational Data Services - Service that systems use to access operational data; standardizes authentication, logging, access controls, usage accounting
- Enterprise Data Warehouse - Data store optimized for analytical processing
- Reporting Data Store Services - Data store for dashboards, reports, and ad hoc users needing analytics of real time or near real time information
- Content Management Store - Store for specialized content types (e.g. documents, images, reports, blueprints, etc.)
- Data Marts - Data stores organized for analytical processing specific to a business unit or persona
- Specialized Data Marts - Data stores optimized for specialized types of analysis or special project

- Analytic Tools - Tools to perform reporting, analysis, predictive modeling and other types of analysis on health-related data

The Agency will leverage the Strategic Project Portfolio Management Plan to identify future FX projects or modules. The Strategic Project Portfolio Management Plan is used for identifying, categorizing, evaluating, and selecting outcome-driven FX projects. This is a phase-gate project selection and approval process meaning that entry and exit criteria are considered in each phase with approval through FX Governance. A project must meet the criteria of a given phase to advance to the next phase. This process integrates with the Enterprise Systems Governance Plan and the MITA business areas. For the MES maturity efforts, outcomes are essential. The outcome model in the plan defines programmatic and operational outcome categories to evaluate projects.

- Programmatic outcomes focus on the strategic mission which are “big picture” items such as improve healthcare outcomes, reduce complexity, and improve provider and recipient experience.
- Operational outcomes are those that focus on achieving desired operational objectives such as the costs of administering a program, technology costs, staff costs, compliance with regulations and law, reduction of data silos, improved data quality, and analytics for operational efficiencies.

A way to improve outcomes is by implementing projects that improve program operations. Therefore, the portfolio management approach will show and select projects with desired outcomes aligned to the Enterprise Systems Strategic Plan. To maximize outcome improvements, the approach is to pursue projects in the right sequence using an evaluation and phase-gate process to categorize, evaluate, and select projects that improve outcomes.

As the Agency continues to execute its Enterprise Systems Strategic Plan, the process will evaluate potential projects against the strategic guiding principles and desired outcomes. This evaluation against the desired outcomes model scores potential projects in the portfolio. **Figure 7: Project Portfolio Management** depicts the stages and gate reviews of the process.



Figure 7: Project Portfolio Management

The Project Gating Process helps the Agency efficiently evaluate and prioritize ideas and potential projects/modules named by subject matter experts and stakeholders. The intake and evaluation of potential project investments occur using a gated evaluation process.

The overall purpose of the phase gates is to:

- Support preliminary project assessments to gauge alignment with the future state FX strategy, goals, guiding principles, policies, and standards
- Develop a project score and preliminary assessment of the impact to the business and technical architecture
- Identify other project and stakeholder dependencies and intersections
- Identify implementation risks and estimates associated with each project
- Identify initial architecture assurance needs indicated by the complexity profile of the project

Key Considerations:

- Ensure the projects, modules, and services required to deliver the business imperatives are identified and validated with the Agency and FX strategic priorities
- Highlight opportunities for re-use
- Look to highlight any cross-capability and cross-release issues

- Since each project has a different profile, size, and scope, gates need to be flexible and scalable and adaptable
- A project may not fully align with the existing business or technical architecture, but may have a large business value and should therefore be considered for additional evaluation

Through the Portfolio Management process, future projects/modules will be evaluated for consideration. Business user scenarios will be identified through the Project Sequencing and Portfolio Management phase when assessment of business cases and outcomes are evaluated. As the process matures and projects are selected for execution, updates will be made to the MMIS ConOps to capture additional transformation scenarios. Additional user scenarios should be developed during use case or user story elaboration.

Future potential business user scenarios include but are not limited to:

- Separating claims and encounter processing
- Becoming the gateway to public sector social determinant of health data
- Enabling integrated health and human service delivery
- One-stop provider licensing enrollment and regulation
- Enabling coordinated communications for recipient and provider communications
- Real time policy-based validation of transactions prior to submission
- Supporting hybrid vertical and horizontal health care service delivery
- Recipient engagement in their own wellness
- Recipient engagement in validation and verification of service delivery
- Improving and automating capture and analysis of provider and recipient experience metrics
- Using telemedicine to expand accessibility, reduce disruption when recipients move or relocate

SECTION 5 FACTORS INFLUENCING TECHNICAL DESIGN

5.1 RELEVANT STANDARDS

A technology standard is an established norm or requirement for technical systems. Standards are usually a formal document that establishes uniform engineering or technical criteria, methods, processes, and practices. The Technology Standards Reference Guide (TSRG) is a collection of technology standards applicable to the administration and operation of the enterprise and the future state enterprise. A comprehensive list of the Technology Standards identified for this project is located in Appendix B.



Figure 8: TSRG Standards Hierarchy Example

Figure 8: TSRG Standards Hierarchy Example shows the types of organizations that are sources of relevant technology standards. Often standards of different organizations are aligned and consistent. Higher-level organizations may adopt lower-level standards or provide guidance that is more specific to the enterprise, organization, or system. In some cases, standards may conflict, or an organization may provide guidance that certain standards are waived or not applicable. The TSRG seeks to help stakeholders understand not only the universe of applicable standards, but also provides a framework and guidance to prioritize and resolve potential conflicting standards. A comprehensive list of the Technology Standards identified for this project is located in Appendix B.

5.2 ASSUMPTIONS, DEPENDENCIES AND CONSTRAINTS

The strategic plan and SS-A address the unique business requirements of the FX transformation program, including standards that affect the range of reasonable technical alternatives. On an enterprise level and on an individual project-by-project level, successful implementation of the technical, policy, and process alternatives identified through the project is contingent on assumptions and subject to constraints.

For the purposes of the project, assumptions are circumstances and events that need to occur for the project to be successful but are outside the total control of the project team. The following assumptions and constraints are identified:

- Agency and Vendor staff and other project stakeholders will be available and actively participate in the project activities and will respond to requests promptly
- Solicitations will result in the timely onboarding of the planned project consulting teams with minimal impact to the master project schedule critical path items
- The FX governance structure will provide timely decision making and project guidance to facilitate an integrated approach to the prioritization of time, resources, and budget across all Agency initiatives currently in progress and for any new initiatives over the life of the project
- MMIS Core Modules will use multi-layered application architecture in accordance with guidance provided by CMS
- Solutions must comply with federal and state security requirements to safeguard data and systems
- CMS Conditions and Standards must be met by FX solutions.
- MMIS activities will be ongoing during the FX transition; services to recipients must continue to be delivered.
- Buy-in is needed from external stakeholders such as the State Legislature, partner state agencies, providers, and members
- Business processes may need to be re-engineered to align with change enabled by the future MMIS
- Competitive and innovative vendors must be ready and able to support modularity
- Adherence to the following interoperability application design principles is required:
 - Standardized Contract – Expresses purpose, capability, and interface content quality to assure appropriate modularity and granularity
 - Loose Coupling – Contains dependencies between the contract, deployment, and customer
 - Abstraction – Hides as much of the details of the service to preserve loose coupling
 - Reusability – Positions services as enterprise resources with agnostic function content

- Autonomy – Design of the service logic and realization of environment impact reliability
 - Statelessness – Managing excessive state information can compromise availability
 - Discoverability – Avoid the accidental creation of redundant service or services that implement redundant logic
 - Composability – Complex service composition places demands on service design
- Existing MMIS portals are developed and owned by different vendors that may use different technology stacks, style guides, data stores, and APIs
 - Updating all MMIS portals to have a unified user interface may not be possible without altering source code of vendor portals
 - The state budget process requires a lead time of 12 to 18 months from the time funding is requested until funds can be accessed
 - The continued operations of the MMIS/DSS and fiscal agent operations are contingent upon execution of a contract extension beyond the current expiration date
 - Retire and replace scenarios must carefully consider current contract terms and scopes of work
 - Change in administration at the national and state level may impact funding, programs, and guidance
 - Standards are not consistently used when exchanging data with external agencies and contractors
 - To support a multi-year MMIS procurement and implementation, the Agency must address limited resource capacity and identify and dedicate resources with the necessary skill sets to the effort. Additionally, availability of state resources is critical for requirements and testing, while recognizing that data conversion is consistently the biggest time and resource consuming challenge. Multiple and overlapping implementations are taxing on state technical staff, so have a plan to adjust state resources as needed
 - The completion of the implementation of the FX modular components, and Fiscal Agent operations, is contingent upon certification by the Centers for Medicare and Medicaid Services
 - The Florida procurement process is a constraint relative to the overall project schedule

- The FX transformation program includes business processes and data transfers with outside agencies

5.3 AGENCY GOALS AND OBJECTIVES

Agency executives collaborated with the SEAS Vendor to create the FX Vision and supporting Guiding Principles during a Strategic Visioning Session held on December 13, 2017. During this session, the SEAS Vendor and Agency executives used the Agency's Mission, Vision, and Goals as guides to create the FX Vision and Guiding Principles. As a result, the FX Vision and Guiding Principles support the Agency's Mission, Vision, and Goals to effectively guide the Agency's investment decisions during the transition to a modular environment. The Agency's FX Vision is to "Transform the Medicaid Enterprise to provide the greatest quality, the best experience, and the highest value in health care."

- Goal #1 – Improve Data Quality
 - Objective #1 – Create reusable business and technical services that provide consistent data validation, edits, and transformation of data based on a single source of policy truth
 - Objective #2 – Enable use of business and technical services throughout the Agency that create, access, and maintain data consistently in a single source of data truth (e.g. Operational Data Store for transactional data and the Reporting Data Store, Enterprise Data Warehouse and Data Marts that derive from the Operational Data Store)
 - Objective #3 – Create business and technical services that perform real-time processing and enable real-time data access
- Goal # 2 – Improve Recipient and Provider Experience
 - Objective #1 – Enable processing consistency across system, program, and organization boundaries
 - Objective #2 – Enable complete and consistent experience data collection for MES business processes
 - Objective #3 – Enable no-wrong door processing to increase access and information timeliness and accuracy
- Goal #3 – Reduce MES Total Cost of Ownership (TCO)
 - Objective #1 – Reduce duplication of custom code embedded in applications that perform same business or technical processing
 - Objective #2 – Simplify testing of established services
 - Objective #3 – Enable service versioning to reduce change management complexity
- Goal #4 - Encourage Service Reuse
 - Objective #1 – Establish a registry that allows potential service consumers to identify existing or planned services that can be reused
 - Objective # 2 – Simplify the ability to identify, create, and reuse business and technical services

- Goal #5 – Develop, document, and implement the necessary processes to maintain and update the Technical Management Strategy, Technical Architecture documentation, FX Project Repository, and Technical Standards

5.4 DESIGN GOALS

Following a set of well-defined application development design principles improves the quality, consistency, and overall cost effectiveness of the FX application environment. The FX Application Architecture design principles are based on widely used standards and concepts currently used in building a sophisticated system to enable future expansion. The primary FX application design principles are:

Data Normalization – Because data duplication leads to errors, there is a strong incentive to establish Single Source of Truth (SSOT) entities to achieve the goal that each fact be a single non-decomposable unit, where these facts are independent of all other facts. When a data change occurs, the expectation is only one data location requires modification.

Factoring – This principle is similar to Data Normalization but refers to application code. Well-planned architectures segment specific code functions or behaviors. At runtime, these appear as separate groups or layers, where each of these layers represent a level of abstraction or domain.

Automatic Propagation – Entails the need to maintain accuracy and consistency through disseminating changes in data or code across a disparate environment. This means that when it is necessary for performance sake to duplicate data or application code to maintain consistency and correctness, the update of these facts is automatic at construction time.

Minimize Functionality – If an application component exists that meets requirements, reuse that component or service wherever possible. Doing so provides the benefits of needing less code to write, verify, and maintain. It can also reduce memory and runtime resources. To support widespread reuse, an Application Service Registry (ASR) will track the inventory of reusable components and services. The Application Service Registry will support search and registration activities. Managing change to reusable components and supporting concurrent use of versions services reduces the operational complexity of change to services and reusable components. Designers and developers use the ASR to conduct impact analysis across all development and production environments. Identifying both direct impacts and secondary impacts all the way to the Business Service level simplifies management of shared components reducing the coordination effort. Likewise, the ASR can help track use of previous service and component versions to reduce the overall maintenance efforts.

Construct Layers – To construct an extensible system, the construction process involves using intermediate layers, which can act on the data received from higher layers of the Application Architecture. These intermediate layers act like virtual machine engines that handle the processing of a specific function in a separate session. This allows data to define the specific functionality, which enables the layered components to be very reusable.

SECTION 6 PROPOSED SYSTEM

The proposed technical solution is to procure modules to replace business processes within the MMIS that are interoperable with other systems within the FX transformation program, using open source solutions, COTS products, or other modular approaches that reduce the need for custom development. Proposed solutions include the EDW and IS/IP, and may include modular procurements for Recipient Management, Provider Management, Financial Management, Encounter Processing, and Claims Processing.

The SEAS Vendor produced technical deliverables that defined the data management, technology, system design and implementation, and enterprise security management strategy for the program. Links to the various technical deliverables can be found in Appendix A.

6.1 TECHNICAL SOLUTION ALTERNATIVES

The evolution to modular applications decouples applications from proprietary data stores, leverages and provides reusable business and technical services, and uses enterprise integration platform services including security and business rule services. The Agency and the SEAS Vendor considered the following technical solution alternatives:

Project-based Modular Evolution and Consolidation – Modernize the Agency applications using a project-based evolution that facilitates the reorganization of existing systems into modular applications.

Current System Operations Procurement – Continue to use the existing system(s). Re-procure a vendor to perform ongoing operation of the current system as it currently operates.

Modular System Slice Replacement – Define the modular slices that in total equate to the current MMIS system. Procure vendor(s) to perform replacement or ongoing operation of one or more modular slices of the current system. This approach would result in processing responsibility split between multiple vendors allowing individual slices to evolve incrementally.

Big Bang / Third Party Administrator Replacement – Procure a single vendor to provide a MMIS system and Medicaid operations services. The vendor would implement the MMIS replacement as a big bang cut-over from the current Third-Party Administrator (TPA) vendor to the new vendor.

6.2 RATIONALE FOR SELECTION

The recommended technical solution is to use a project-based modular evolution and consolidation strategy. The rationale for this approach includes:

- Technology modernization investments are driven by value generated and direct impact on supporting the business
- The chosen solution best supports key recommendations of data management and

technology strategies in that it:

- Operates from a single source of truth for data
- Operates from a single source of truth for policy and business rules (e.g. data edits, validations, transformations, decision making)
- Performs data validations at the point of the business event to improve data quality
- Aligns with expected market evolution in data management (e.g. toward Blockchain-like distributed ubiquitous data management)
- Enables higher level of business agility and reduces costs to convert proprietary vendor data
- Reduces vendor lock-in and problems with vendors controlling access to Agency data

6.3 RECOMMENDED TECHNICAL SOLUTION

The FX Data Management Vision emphasizes six primary strategies that align with the overall FX strategic priorities and the recommended Technical Solution will be required to align with all six:

- Improve data quality by operating from a single source of policy truth
- Evolve core processing with data validation at the point of business event data collection
- Provide seamless access to a real-time, 360-degree view of recipient and provider information
- Decouple data from proprietary systems and application stores
- Operate with business area and persona optimized data marts and data analysis tools
- Prepare to collect and manage recipient and provider experience and outcome data

Improve data quality by operating from a single source of policy truth. Today, data edits, data validations, and data transformations are the electronic implementation of policy. The inconsistent application of data edits, validations, and transformations to the many different Agency data stores means there is no single source of policy truth which causes confusion and lack of trust in the data both within the Agency and with external consumers of Agency data. For example, data edit rules and policies are applied differently in the front-end of MMIS interChange when compared to the back-end processing resulting in claims rejections. Different business units and individuals implement policy by applying specific data edits, validations, and transformations to their own data sets to meet their needs or preferences. Often, separate systems support different versions of data validation and transformation. When each business area can claim common data is not right for the unit, this leads to many propagations of duplicated data and no true single source of the truth. The Agency's strategy is to centralize and standardize data edits, data validations, and data transformations applying the policy to a single source of truth data set. After consolidation, a single set of policies operationalized as system edits, validations, and transformations decreases the need for business unit or individual specific clones of data. After a single source of policy truth exists, health plans and providers can use the electronic implementation of this policy to validate information before submission to Agency systems reducing errors and rejects.

Evolve core processing with data validation at the point of business event data collection. Today, high-volume claims and encounter processing occurs in a single system that validates submissions in a complex, difficult to maintain claims processing engine. The current system is a

stable, reliable workhorse that is essential for timely and accurate payments to health providers in Florida. Naturally, there is reluctance to introduce risk to this critical processing engine because of the transaction volumes and State spending processed by the system. However, evolution of core claims and encounter processing is essential for the Agency to meet its mission and strategic priorities. The most significant improvements in provider experience, recipient experience, levels of fraud, and provider administrative costs depend on how core processing works. The Agency strategy is to evolve core processing by allowing health plans and providers to validate and verify claim and encounter data before submission to the Agency. Evolutions in core processing will reduce errors, rejected transactions, denied claims and encounters, and costs.

The Agency strategy to evolve core processing involves:

- Providing access to an electronic set of policy truth (e.g. implemented via rules engine)
- Providing health plans and providers with recipient, provider, and reference data needed for evaluation against the electronic set of policy truth
- Having health plans and providers validate and resolve errors before claim and encounter submission by validating data at the point of business event. This will be accomplished through services the Agency will expose to health plans and providers allowing them to validate data against edit rules and policies before submitting to the Agency
- Submitting validated claims and encounter records that can be accepted with minimal Agency processing

The Agency strategy of going beyond the boundaries of the Agency to fix data quality problems is foundational to address symptomatic and derivative issues that affect many business functions.

Provide seamless access to a real-time, 360° view of recipient information. Today, batch files drive most of Medicaid system processing. The Agency strategy is to use technology to assemble information in near real-time from all relevant sources to make processing decisions. The near real-time, 360° view of recipient information will eventually include information from other Medicaid stakeholder organizations providing access to comprehensive social determinants of care data. Access to current and complete recipient information will improve service authorization decisions, treatment, and enhance coordination of care by health plans and providers. The information will also help organizations in the community of care to deliver non-Medicaid services to recipients. Providers of education, child welfare, elder care, employment, and other services can be more effective by leveraging information and collaborating with other providers to benefit the recipient. For example, another state's analysis of behavioral issues in schools leading to class disruption, detention, suspension, and expensive behavioral services found the root cause often originates from health issues related to vision, hearing, and dental screenings. By sharing claim or encounter information with appropriate data privacy protections, educators may accommodate children, provide proper referrals, and confirm that appropriate screenings occur. Providing service providers with real-time access to a comprehensive view of recipient information should also help the Agency, health plans, and providers to identify if increased coordination of care is prudent and justified.

Decouple data from proprietary systems and application stores. Today, MMIS and most application systems use tightly coupled databases that contain information structured for use in an individual application. The Agency data management strategy is to manage data as a service. New

FX modular components operate using data access services that connect to an operational data store that is independent of specific systems or modules. The operational data store provides data to applications through service calls or application programming interfaces (APIs) by subject areas, which is a commonly used and supported technical pattern. Decoupling data from proprietary systems and databases helps operate from a single source of the truth and reduces data duplication. This strategy simplifies access, improves security, and enables business agility to replace or improve a new module. Decoupling will also simplify the future migration to emerging virtual data access technologies (e.g. Blockchain) that allow entire industry ecosystems to contribute data, access data and operate from a single secure information source.

Operate with business area and persona type optimized data marts and data analysis tools.

As it relates to data strategy, a persona categorizes and defines the data and analytic usage and processing characteristics for a person. The persona generalizes the types and breadth of data used and processed and the types of tools used to perform a role. In most organizations, there are 5-10 different personas. Currently, several hundred Agency personnel routinely develop and execute custom Structured Query Language (SQL) queries in roles as power users. The Agency's data strategy is to provide optimized data marts and tools that meet the needs of each combination of business area and data processing persona type. For example, users that perform advanced data scientist level analytics may need access to pull the data into more sophisticated software programs such as SAS to analyze the data more effectively. A data mart to support some personas would allow for a large download in a quick and efficient manner directly by the users themselves. This new strategy should reduce costs and improve responsiveness to business needs by rightsizing technology spend based on business persona need.

Prepare to collect and manage recipient and provider experience and outcome data. Today, the Agency and entire healthcare industry has limited visibility to comprehensive recipient and provider experience or health outcome data. Survey and sampling provide limited feedback mainly about recipient satisfaction with provider interactions. Across all industries, system and process improvements are raising expectations of recipients and providers. The Agency expects increased scrutiny on the overall costs, time spent, and quality of service interaction by recipients and providers in the delivery of healthcare services. For the Agency, health plans, and providers this means collecting, storing, and analyzing more data and new types of data with new dimensions of analysis. Collecting experience data efficiently also requires new applications and technology. Likewise, emerging advanced payment models (e.g. Diagnosis Related Grouping (DRG), Enhanced Ambulatory Patient Grouping (EAPG), bundled payments) introduce changes to core claims and encounter processing systems.

6.4 PROPOSED SOLUTION DESCRIPTION

The proposed solution is to procure the services of the SEAS Vendor to develop the strategic plan for the FX transformation program and identify solutions that meet the current and future business needs of the Medicaid Enterprise. An IS/IP vendor will be procured to provide the technical expertise to perform systems integration and ensure the integrity and interoperability of systems within the Medicaid Enterprise. Additionally, the IS/IP vendor will integrate services and

infrastructure within the Medicaid Enterprise without relying on a common platform or technology. The procurement of an Enterprise Data Warehouse will provide data warehousing and data integration capabilities, that will provide a unified data repository for reporting and analytics. Modules will be procured to replace business processes within the MMIS that are interoperable with other systems within the Enterprise.

6.5 CONTEXT DIAGRAM

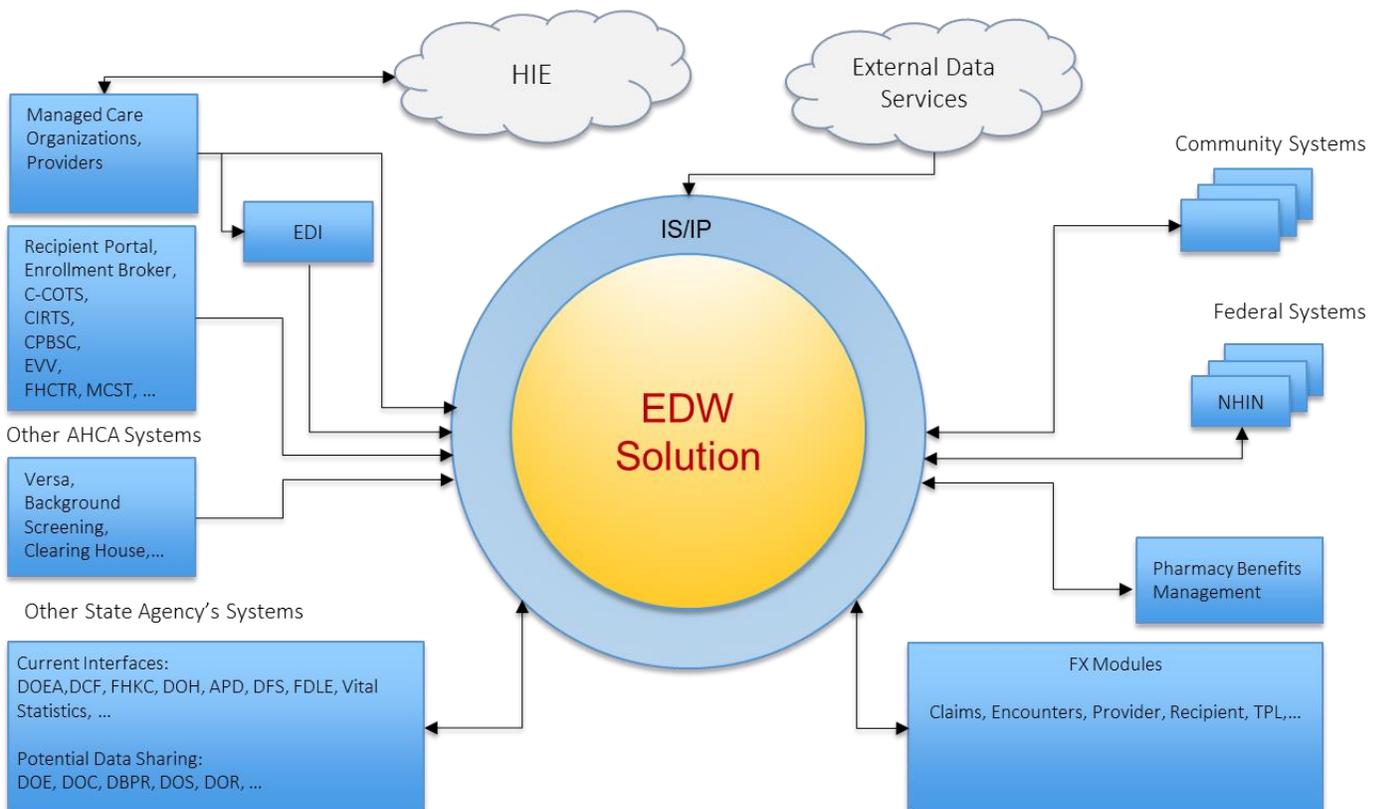


Figure 9: Context Diagram

6.6 HIGH-LEVEL OPERATIONAL REQUIREMENTS AND CHARACTERISTICS

6.6.1 USER COMMUNITY DESCRIPTION

- Recipients (including potential Recipients) – AHCA administers health coverage for vulnerable and underserved populations who might otherwise go without medical care for themselves and their children.
- Providers – The State is responsible for enabling access to covered services through a network of providers for which the State verifies credentials and licenses, including individual providers (i.e. doctors, nurses, social workers, dentists, and other ancillary

providers) and facilities (i.e. hospitals, ambulatory surgery centers, assisted living facilities, nursing homes, and home health agencies).

- Federal and State Agency Partners – The State partners with independent partner agencies for information and data exchange related to providing care, including the Centers for Medicare and Medicaid Services, Social Security Administration, Florida Department of Children and Families, Florida Department of Health, Florida Department of Elder Affairs, Florida Agency for Persons with Disabilities, and Office of the Attorney General Medicaid Control Fraud Unit (MFCU-OAG).
- Health Plans – The State carries out its mission through two models: Fee-For-Service (FFS), which directly manages care for members, and managed care through Statewide Medicaid Managed Care (SMMC), which manages an assigned group of members. Health plans are also responsible for credentialing their providers, managing the care delivered to members, and maintaining a network to provide adequate access to their covered members.
- Vendors – Many MMIS processes are contracted to outside vendors with contractual authority to perform various functions and interact with the core MMIS to send and retrieve current data.

User Group	Description / Expected Use of System	Type (Federal Employee, Contractor)	Geographic Location	Network Profile (LAN, WAN, External)	Total Users	Concurrent Users
Recipients	Access health benefits, verify coverage, change health plans or providers, track claims, communications	End User, Private Citizen	Statewide	External	Potentially over 3.8 million	Unknown
Providers	Verify coverage for recipients, submit and track claims, enroll as a Medicaid provider or a licensed/credentialed facility, correspondence	End User, usually a medical care provider or facility, or pharmacy	Statewide	External	Just under 150,000	Unknown
Centers for Medicare and Medicaid Services (CMS)	Exchange data on Medicare buy-in or disabled recipients	Federal		External		
Federally Facilitated Marketplace (FFM)	Verify Medicaid coverage for individuals applying for ACA coverage.	Federal		External		
Social Security Administration	Exchange data on Medicare buy-in or disabled recipients	Federal		External		
Department of Children and Families (DCF)	Determines eligibility for Medicaid recipients. Batch transmission of eligibility and enrollment files to the fiscal agent for plan assignment and coverage.	State Employee	Statewide	External		
Department of Health	Responsible for the regulation and licensing of health practitioners. Exchange data related to provider licensing.	State Employee	Statewide	External		
Department of Elder Affairs (DOEA)	Provides direct services through its Division of Statewide Community-Based Services and determines the level of care needed long term care recipients.	State Employee	Statewide	External		
Agency for Persons with Disabilities (APD)	Provides access to community-based services, treatment, and residential options for the developmentally disabled.	State Employee	Statewide	External		
Office of Attorney General Medicaid Fraud Control Unit (MFCU-OAG)	Investigates and prosecutes fraud involving providers that intentionally defraud the state's Medicaid program through fraudulent billing practices.	State Employee	Statewide	External		
Health Plans	Manage an assigned group of members. Health plans are also responsible for credentialing their providers, managing the care delivered to members, and maintaining a network to provide adequate access to their covered members.	Contractor	Statewide	External		
Vendors	A variety of vendors contract with the Agency to perform various functions (ex: pharmacy benefits, choice counseling, provider network verification, etc.) and interact with the MMIS to send and retrieve current data.	Contractor	Statewide	External		

Table 2: User Community Description

6.6.2 NON-FUNCTIONAL REQUIREMENTS

6.6.2.1 SECURITY AND PRIVACY CONSIDERATIONS

FMMIS maintains current and historical Protected Health Information (PHI) and Personally Identifiable Information (PII) for providers, recipients, and recipient households. Because this data may be shared with other entities within the state to support additional processing, it is vital the information is protected throughout the capture, processing, transmission, online usage, and storage of this data. Accordingly, all stakeholders accessing data within the new system in any manner will be required to go through proper security credential verification. The new system must comply with the following security and privacy standards:

NAME	DESCRIPTION	GOVERNING BODY	STATUTORY REFERENCE
Security Standards for the Protection of Electronic Protected Health Information	Commonly referred to as HIPAA Security Rule . Provides specific standards and safeguards for health information protection	Federal Government	45 CFR Part 164, Subpart C
Federal Information Security Modernization Act of 2014	Establishes the Secretary of Homeland Security as the responsible party to implement policies and practices to secure Federal information systems.	Federal Government (Department of Homeland Security)	S.2521 of the 113 th Congress to amend Chapter 35 of Title 44, United States Code
Federal Information Processing Standards	Sets the approved technical standards and guidelines for federal information systems	Federal Government (NIST)	S.1124 of the 104 th Congress – Information Technology Reform Act of 1996
Medicaid Information Technology Architecture (MITA) Framework	Provides authority for states to receive enhanced federal funding by developing highly interactive and interoperable MES platforms	Federal Government (Centers for Medicare and Medicaid Services (CMS))	Affordable Care Act: Medicaid Program: Federal Funding for Medicaid Eligibility Determination and Enrollment Activities (CFR Vol. 76, No. 75)
Florida Cybersecurity Standards	Establishes the Florida Cybersecurity Standards (FCS), the minimum standards for state agencies to secure IT resources. Uses the NIST CSF and Federal Information Security Management Act (FISMA) as guiding documents	State of Florida	Florida Administrative Code 74-2.001 through 74-2.006

NAME	DESCRIPTION	GOVERNING BODY	STATUTORY REFERENCE
Florida Technology Architecture Standards – Identity Management	Creates the Identity Management Services framework to provide secure, reliable, and interoperable mechanisms for authenticating the identity of devices, application services, and users that consume state information and application resources. This rule is modeled after the Identity Ecosystem Framework Baseline Functional Requirements v1.0	State of Florida	Florida Administrative Code 74-5.003
SEAS Contract	Authorizes Florida Agency for Health Care Administration to expend funds in support of developing the strategy and governance for the State’s MES transition	Florida Agency for Health Care Administration	SEAS Contract MED-191

Table 3: Security and Privacy Standards

By implementing a comprehensive and robust security scheme around the Medicaid Enterprise, the Agency avoids these risks:

- Unauthorized access to PHI and PII
- Monetary damages due to unauthorized access to PHI and PII
- Compromising data integrity
- Stakeholder dissatisfaction

6.6.2.2 AVAILABILITY REQUIREMENTS

System availability requirements are outlined in the table below:

System Availability Requirements	
Solution Availability	Excluding Agency-approved downtime for maintenance, the Solution shall be available, at a minimum, 99.982% of the time, twenty-four (24) hours per day, seven (7) days per week.
Approved Downtime	All Planned downtime and maintenance outages shall be coordinated with and approved by the Agency at least five (5) business days in advance and must occur after 10:00 PM ET and before 6:00 AM ET, unless a different time is approved by the Agency.
Notification	Agency staff shall be notified by email twelve (12) hours before

	any scheduled maintenance.
Recovery Time Objective (RTO) and Recovery Point Objective (RPO)	In the event of unscheduled system outage, the RTO shall be no more than 2 hours and RPO shall be no more than 15 minutes.

Table 4: System Availability Requirements

6.6.2.3 VOLUME AND PERFORMANCE EXPECTATIONS

The following capacity, performance, and availability expectations have influenced the technical design of the FX. System volume and performance expectations are depicted in the following tables:

Current Volumetric Capacity	
Volumetric Type	Volumes
Number of Systems/Applications	149
Total Number of Internal Users	8,815
Total Number of External Users	352,754
Number of Concurrent Users	1,983
Number of Outbound Interfaces	139
Number of Inbound Interfaces	126
Number of Databases Types	199
OLTP Database Size (TB)	32
Avg Volume of Transaction Per Day	11,261,530
Number of Real Application Clusters (RAC) Nodes	21,005
Avg Backup Size (GB)	30,127
Avg Yearly Data Growth (TB)	9
Number of Published Reports	2,679
Content Management Database Size (TB)	55
DSS Database Size (TB)	16
Number of DataMart's	11

Table 5: Current Volumetric Capacity

Performance Expectations	
Enterprise Data Warehouse Data Currency	The solution shall maintain a level of data currency in Enterprise Data Warehouse where committed source data is available based on intervals specified by the Agency; daily source data is available in the target system within 24 hours; Weekly, Monthly, Quarterly, Annual and Odd Cycle source data shall be available in the target system within 72 hours
Reporting Data Store Data Currency	The solution shall maintain a level of data currency in Reporting Data Store where committed real time source data is available within 5 minutes, committed delayed source data is available in the target system within 60 minutes, committed daily source data is available in the target system within 24 hours; Weekly, Monthly, Quarterly, Annual and Odd Cycle source data shall be available in the target system within 72 hours
Response Time - Data Service Request	The solution shall be capable of responding to simple data service requests in less than 125 ms (milliseconds), data service requests of medium complexity in less than 140 ms and complex data service requests in less than 170 ms
Response Time – Direct Access	The solution shall be capable of responding to simple direct access queries in less than 25 ms, direct access queries of medium complexity in less than 40 ms and complex direct access queries in less than 70 ms
Response Time – Reports	The solution has response times to simple reports within 1 second, reports of medium complexity within 2 seconds and complex reports within 3 seconds

Table 6: Performance Expectations

6.7 HIGH LEVEL ARCHITECTURE & ALTERNATIVES ANALYSIS

Alternative	Description	Pros	Cons	Rationale
Project-based Modular Evolution and Consolidation	Modernize the Agency applications using project-based evolution to consolidation existing systems into modular applications.	<p>Improved outcomes delivered faster</p> <p>Meets current CMS requirements</p> <p>Uses modern technologies and design patterns</p>	<p>More granular change than module</p> <p>May not align with module certification</p> <p>Ongoing Implementations</p> <p>Modular approach is an emerging technology that has yet to be fully implemented</p> <p>Period of parallel reuse of existing System</p>	<ul style="list-style-type: none"> • Technology modernization investments are driven by value generated and direct impact on supporting the business • The chosen solution operates from a single source of truth for data • Operates from a single source of truth for policy and business rules • Aligns with expected market evolution in data management • Enables higher level of business agility and reduces costs to convert proprietary vendor data

				<ul style="list-style-type: none"> Reduces vendor lock-in and problems with vendors controlling access to Agency data
Current System Operations Procurement	Continue to use the existing system(s). Re-procure a vendor to perform ongoing operation of the current system as it currently operates.	Shorter turnover time	<p>Systems will continue to constrain the service delivery</p> <p>Reduced ability to use newest technologies</p> <p>Continued silos of information and policy / rule implementation</p>	
Modular System Slice Replacement	Define the modular slices that in total equate to the current MMIS system. Procure vendor(s) to perform replacement or ongoing operation of one or more modular slices of the current system. This approach would result in processing responsibility split between multiple vendors allowing individual slices to evolve incrementally.	<p>Shorter turnover time</p> <p>Supports modularity and newer technologies</p>	<p>System capabilities likely to be similar to current</p> <p>May create even more silos of information and policy</p> <p>May require managing many different vendors simultaneously</p>	

<p>Big Bang / Third Party Administrator Replacement</p>	<p>Procure a single vendor to provide a MMIS system and Medicaid operations services. The vendor would implement the MMIS replacement as a big bang cut-over from the current TPA vendor to the new vendor.</p>	<p>Advances into newer technologies Fewer procurements</p>	<p>Risk to current operations May not attain full modularity Unlikely to consolidate and eliminate current silos of duplicated information and inconsistent policy Long time to achieve outcome improvements</p>	
---	---	---	---	--

Table 7: Solution Design Alternatives

6.7.1 APPLICATION ARCHITECTURE

The Application Architecture connects Business Services with Technical Services, as shown in

Figure 10:Conceptual Technical Architecture Diagram. The Agency tailors Business Services to environmental needs. The Application Architecture framework defines services from the abstract level to the design level, which allows the Agency to build service interfaces as standard interfaces without dialects caused by interpretations.

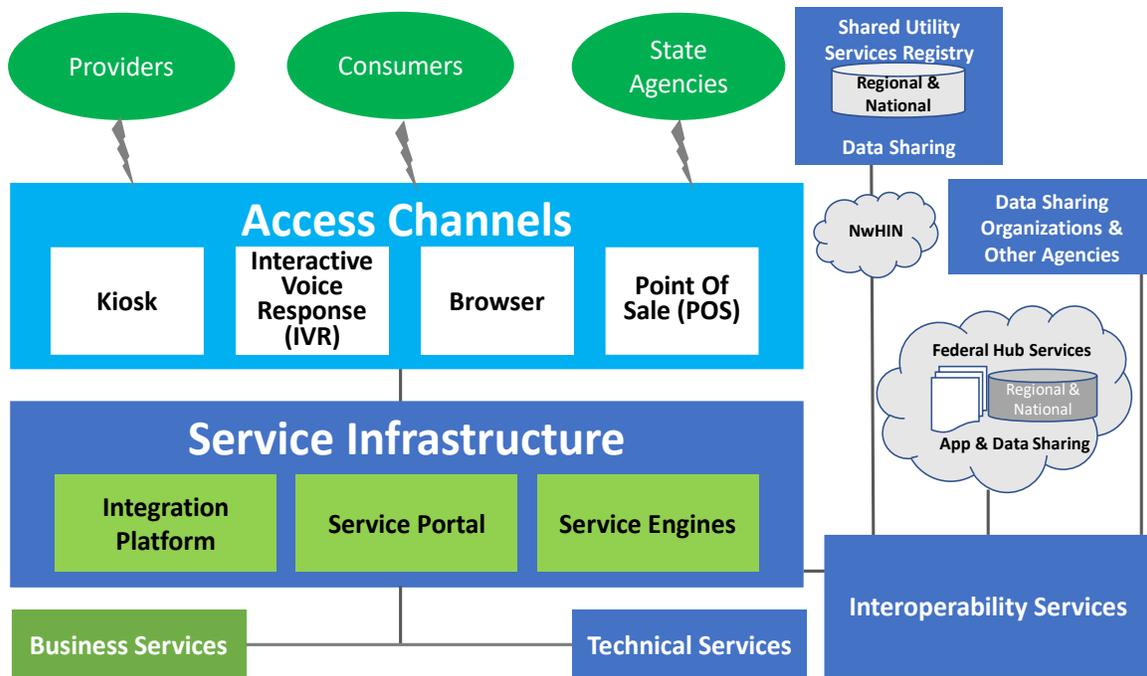


Figure 10:Conceptual Technical Architecture Diagram

The service infrastructure includes standards-based elements that use service-process integration and data sharing with other organizations and agencies. The Application Architecture framework is compatible with the Federal Health Architecture (FHA), the Nationwide Health Information Network (NwHIN), regional and national shared data sources, and the network on Regional Health Information Organizations (RHIOs). The Application Architecture framework defines a series of interoperability services based on Web Services (WS) and Extensible Markup Language (XML) message formats and protocols. The tools the Agency requires to establish interoperability, data capabilities, and other support requirements, are available to the Agency in groups using common facilities.

The following sections provide a description of the top-level Application Architecture Service Oriented Architecture (SOA). They describe fundamental infrastructure components, such as the Enterprise Service Bus (ESB), the Service Management Engine (SME), infrastructure services (e.g. external data-sharing and hubs), and provide references to industry standards.

A multilayer Application Architecture model represents a combination of applications and connections to deliver services to stakeholders, as shown in [Error! Reference source not found.](#) The four (4) levels are the Access Layer, Service Management Layer, Service Application Layer, and Platform Layer.

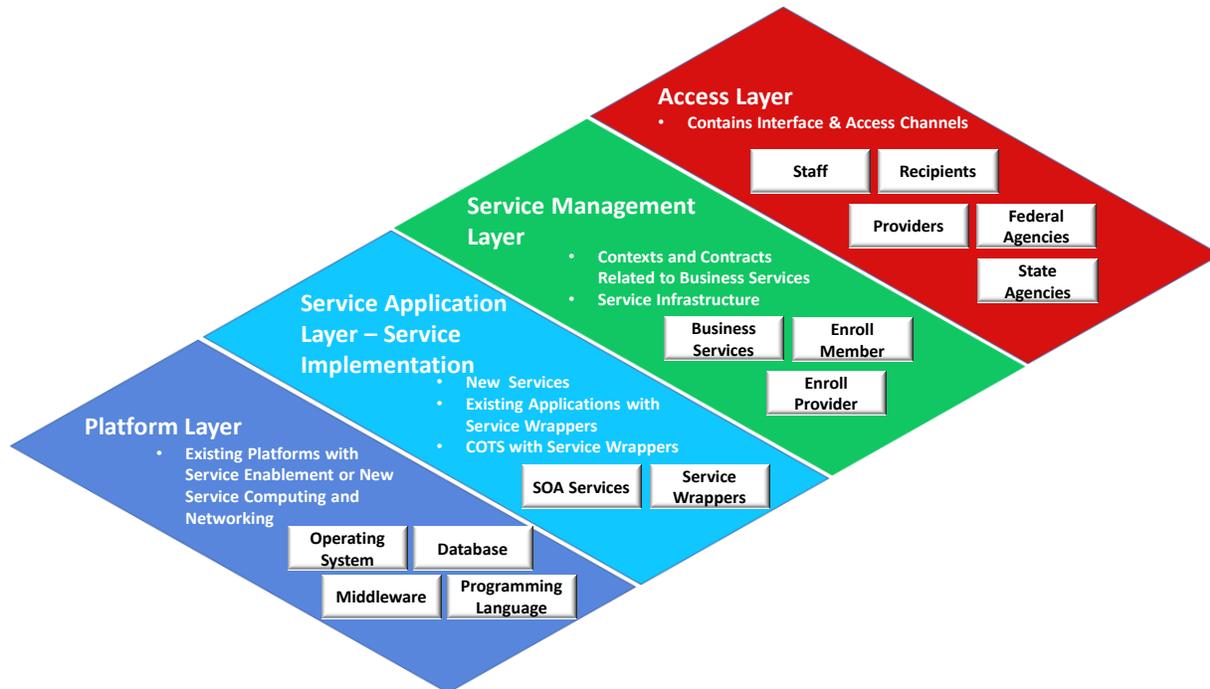


Figure 11: Multilayer Application Architecture Model

- **Access Layer** – This layer is where end users connect to the application. This is most likely through a user interface like a web page. Additionally, this could be via a web service or API accessed by an internal or external system.
- **Service Management Layer** – This layer consists of the service infrastructure, service contexts, and service contracts for each Business Service. All Business and Technical Services are exposed via this layer. The Service Management Layer links to the Service Application Layer, either directly or through service wrappers.
- **Service Application Layer** – This layer consists of Data and Business rule services. Although the Service Application Layer consists of services, those services might be new services, wrapped legacy applications, or wrapped-COTS products. The Service Application Layer evolves incrementally as new applications are added.
- **Platform Layer** – This layer includes the software that is necessary to support the execution of the Application Layer.

6.7.2 INFORMATION ARCHITECTURE

A conceptual data model (CDM) helps in identifying high-level key business and system entities and establishing the relationships existing between them. It also helps in defining the key issues

of business problems and opportunities for the system. It can address both digital and non-digital concepts. A conceptual data model can also help in closing the gaps between a solution model and requirements document.

The CDM has two levels, an enterprise conceptual data model (ECDM), containing all required data elements, and a MITA business process-specific set of CDMs for each business area. These are delivered as high-level data models, normalized to show “data classes” and “relationships” (associations between classes).

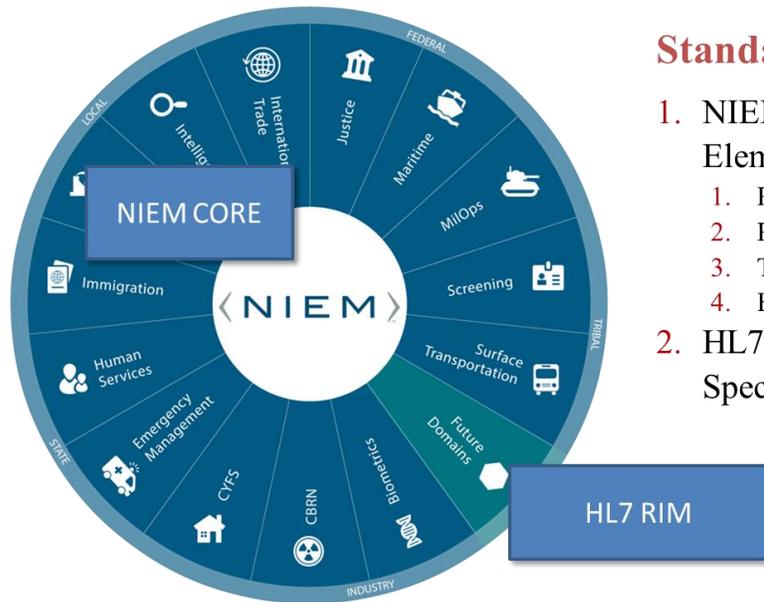
The FX Data Dimensions shows a general overview of the kinds of data each business area contains. This section of the deliverable will continue to develop and serve as the documentation for information architecture elements as they are conceived through the implementation of future module procurements.

The FX conceptual data models will follow and use applicable standards provided by national standards organizations, State, and CMS guidelines. The FX Conceptual Data Model will use applicable data classes and predefined names preferred by national naming standards:

- National Information Exchange Model (NIEM) version 4, for “core data” class names such as ORGANIZATION and PERSON, with ENTITY as the superclass for any business party; ACTIVITY to represent a business event; IDENTITY; LOCATION and ADDRESS
- Applicable data naming and data elements from other NIEM datasets
- Applicable data naming and data elements from Health Level 7 (HL7) Reference Information Model (RIM) datasets

Figure 12: National Information Exchange Model version 4 provides the basis for modeling information exchanged especially between government organizations. NIEM is a canonical model that is the standard for exchange of information between government information sources. The federal government mandates use of NIEM for exchange of information between federal government organizations. NIEM is also widely adopted for modeling and exchange of information between other government data.

The use of NIEM based modeling and data vocabulary is a change from existing healthcare vocabulary that will require communication and organizational change management to secure adoption. The direction to use NIEM supports the direction for MITA higher maturity levels to increase integration and use of information across program, agency, and state boundaries. Likewise, the direction to use social determinants of care to increase coordination of health care will integrate new information sources, data types and expand and change the vocabulary and perspective of the business. This evolution in vocabulary should be minor but will help particularly in communication with external organizations that already communicate with this vocabulary.



Standards Based:

1. NIEM Core for Enterprise Elements
 1. People
 2. Places
 3. Things
 4. Events
2. HL7 RIM for Healthcare Specific Elements

Figure 12:National Information Exchange Model

NIEM lacks data classes or elements defined for some of the healthcare specific data classes necessary for the Agency’s data model. Other federal agencies are transforming their models to NIEM. For these and other areas not supported by NIEM conventions, the data naming and formats will use standards from HL7 and Federal Health Information Model (FHIM). FHIM is a national program supported by the federal government that provides a community of users, tools, common terminology, governance, methodologies, and support that enables enterprise-wide information exchange.

Fast Healthcare Interoperability Resources (FHIR, pronounced fire) is a draft standard describing data formats and elements (known as resources) and an Application Programming Interface for exchanging Electronic health records. Exhibit 4-3: Sample MMIS Conceptual Data Model depicts an example of a fully defined conceptual data model reflecting the data that supports major MITA business area processing. The creation of an Agency-specific FX Conceptual Data Model optimized for Florida and the FX strategy will ultimately reflect data and relationships of all FX modernization implementations.

Figure 13:Conceptual Data Model Sample is illustrative of completeness and representative of alignment with MITA. This sample is too detailed for presentation to a C-suite in its complete form but could be presented in segments for executive consumption.

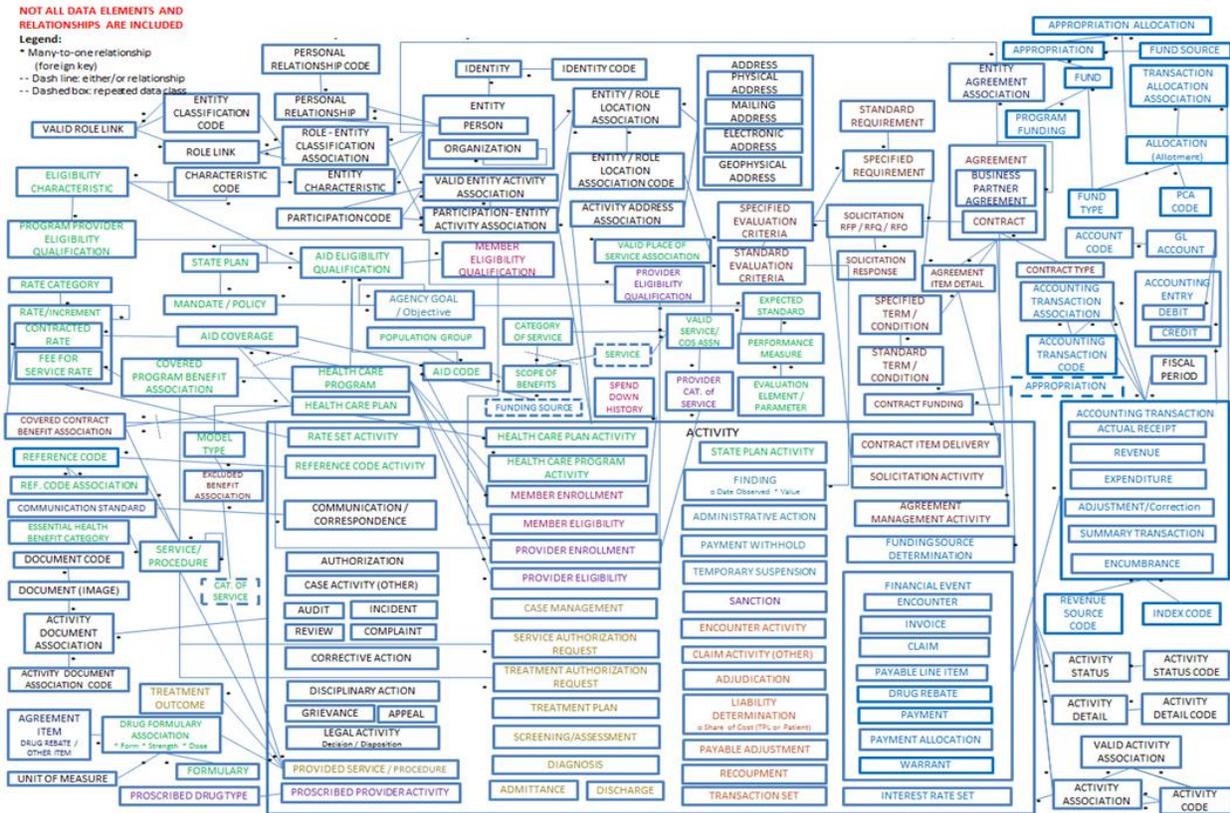


Figure 13: Conceptual Data Model Sample

The strategy to develop the FX Conceptual Data Model is to iteratively model the conceptual data and relationships relevant to FX Project implementations. This approach begins with a blank model and incrementally adds conceptual data model subjects for areas relevant to active FX Projects. This deliverable creates an initial FX CDM by projecting the data types used in FX Projects in the FX Infrastructure Phase of the FX Procurement Strategy. Specifically, this deliverable contains representative conceptual data modeling to support the anticipated processing of the Integration Services Integration Platform (IS/IP) Project. This iteration models the conceptual data relationships used in integration and information exchange processing:

- Entity - people and organizations used in Master Person Index, Master Organization Index and Master Data Management identity processing
- Integration Management – integration message information used in Enterprise Service Bus processing
- Security Management – system user identity credentials, authentication and access control information used in Single Sign-on processing

Following the selection of a specific IS/IP vendor and solution, the SEAS Vendor will update the FX CDM for these areas to reflect additional data types and relationships managed by the integration solution. As the FX Project defines, procures, and implements other FX Projects, the

SEAS Vendor will elaborate the FX CDM until the FX CDM reflects all data subjects and relationships.

6.7.3 INTERFACE ARCHITECTURE

The Agency’s preference for increased granularity of enterprise functionality and an API-centered approach to seamless interoperability places particular design and delivery considerations on the underlying technical and interface architectures and foundational technologies of the FX. This is especially true of technical design considerations targeting and enabling the desired business process improvements essential to achieving the Agency’s goals. Many of these anticipated improvements are to be made possible by the functional and technical innovations amplified by proven, advanced system integration techniques and technologies.

The Agency fully understands the necessity to transition to a more up-to-date and advanced form of system integration in response to growing healthcare industry recognition that many stakeholder experience and business process improvement benefits are tied to creating a distinct data layer. Benefits are derived from improving upon and scaling intra-enterprise information data interchange messaging and inter-agency and trading partner information exchange.

The State is being intentional in risk mitigation actions and technical and information architecture capabilities to be implemented to avoid the risks of modularity damaging data integrity, data quality, and stakeholder interaction experiences. This risk avoidance is particularly focused on early stages of FX implementation actions when the portfolio of functionality contains both new and legacy systems and modules.

The future MMIS will use new APIs and reuse existing APIs where possible and appropriate. All APIs will strictly follow Agency guidelines, governance, processes, and best practices. The development of individual APIs for each vendor and/or module will be designed following normative specifications. All API information will be maintained in an API inventory and registry.

Table 8 – MMIS Interface presents key interfaces required to support MMIS processing and reporting.

INFORMATION SHARED	INTERFACING APPLICATION	PURPOSE	INBOUND OR OUTBOUND?	BATCH OR NEAR REAL TIME?	DATA STORED PERSISTENTLY?
MMIS Transactional Data from Vendors	MMIS Vendor Modules will use APIs.	This is the data that is retrieved and/or sent from the Vendors’ systems modules. This data will end up in the ODS	Inbound/ Outbound	Batch / online real time	Yes
Federal and State	APIs designed for Federal	This is the data that is retrieved	Inbound/ Outbound	Batch / online	Yes

INFORMATION SHARED	INTERFACING APPLICATION	PURPOSE	INBOUND OR OUTBOUND?	BATCH OR NEAR REAL TIME?	DATA STORED PERSISTENTLY?
Transactional Data	and State Agencies	and/or sent from the State and Federal Agencies' systems modules. This data will end up in the ODS		real time	
MMIS Analytical Data	API designed for EDW interface	This is the data that is sent from MMIS. This data will end up in the EDW	Outbound	Batch / online real time	Yes

Table 8: MMIS Interfaces

6.7.4 TECHNOLOGY ARCHITECTURE

The technology architecture envisioned by the Agency and the SEAS Vendor will adhere to MITA principles, standards, and architecture configurations with a target of advancing MITA maturity levels. The following sections outline the future-state technology architecture as currently conceptualized, with several decisions still to be determined. The MMIS ConOps, along with the future-state system plan, shall be updated on an iterative basis as CMS provides new guidance, and as the Agency regularly assesses options and evaluates decisions.

6.7.4.1 PLATFORM

The Agency’s FX Platform will be designed to provide a transition from the current application systems into loosely coupled, API-focused modules. This platform will consist of standardized APIs for core shared services, shared tools and resources, and an operational data store. The core shared services will provide critical functionality to multiple modules, and it will allow reuse of functionality by exposing services from other modules. The Shared Tools will expose access to tool functionality through the platform and will allow access to the tools from multiple modules. The operational data store will track transactional data and additional information for reporting and querying. The platform will focus on the use of technical standards, COTS, and open source tools. In addition, the platform will be developed using industry standards and deployed in virtualized servers on high end server architecture.

6.7.4.2 SYSTEM HOSTING

The Agency will require the IS/IP and EDW vendors to develop and implement appropriate hosting environments capable of supporting all current and anticipated hosting and infrastructure

needs. The MMIS ConOps will be updated concerning this topic on an iterative basis as the available options become more apparent, and a direction is solidified.

6.7.4.3 CONNECTIVITY REQUIREMENTS

The Agency will use its existing network infrastructure in conjunction with network infrastructure provided by the IS/IP and EDW vendors to address the anticipated connectivity requirements. The MMIS ConOps will be updated concerning this topic on an iterative basis as the available options become more apparent, and a direction is solidified.

6.7.4.4 MODES OF OPERATIONS

The IS/IP vendor will be responsible for designing the hosting infrastructure along with the various environments necessary for development, testing, and operation of the Integration Platform. As illustrated in **Figure 14: Conceptual View of Multiple Environments**, supporting the Integration Platform will require a multi-environment strategy.

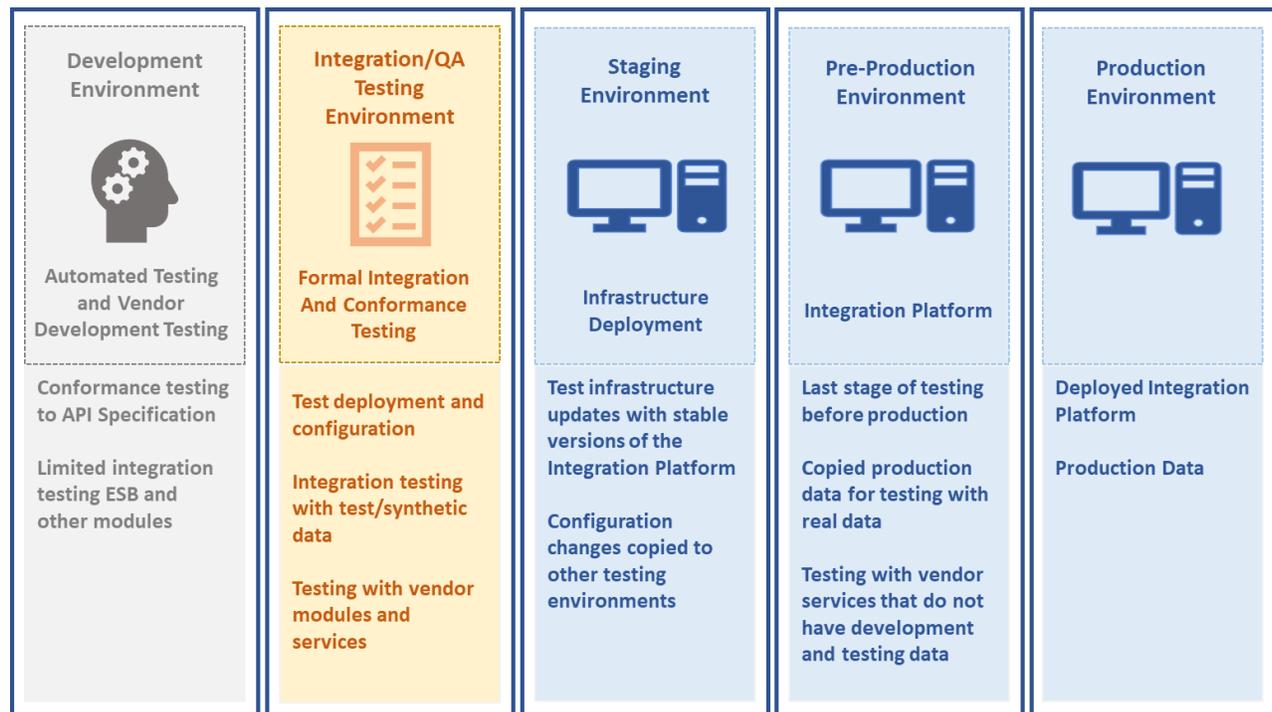


Figure 14: Conceptual View of Multiple Environments

The Development Environment runs the latest code and configuration from development through automated testing to identify deployment issues as early as possible. Deployment and configuration of the integration platform and APIs will be performed in the Integration/QA/Test Environment. Vendor Development and Integration/QA/Test Environment connectivity is only possible with test data. Some vendors may only be able to test with production data and unable to participate in testing in these environments. Verification of infrastructure updates will be tested in the Staging Environment before the last stage of testing in the Pre-Production Environment with real data.

6.7.5 SECURITY AND PRIVACY ARCHITECTURE

An Integration Services/Integration Platform (IS/IP) solution will be implemented for FX, including both the technical means for authorized users to authenticate to the system and policies and procedures to support user vetting, credentialing, and identity lifecycle management. Existing user roles and the system access available in the current solution will be used as a starting point for establishing roles, privileges, and permissions. The Integration Services/Integration Platform will provide the authentication, authorization and encryption components of the Integration Platform which encompasses the following capabilities:

- Single sign-on - The capability to authenticate once and be subsequently and automatically authenticated when accessing various target systems.
- Identity and access control - Enables the right individuals to access the right resources at the right times for the right reasons.
- Federated identity management - Enables identity information to be developed and shared among several entities and across trust domains.
- Data anonymization - Tools and processes to sanitize information and protect privacy.

These security capabilities are to provide application or module level authentication. The goal is to provide role and content-based access control for information exchanged using the Integration Platform that will include controls at page, action, and field level within applications or modules.

The solution will support external systems such as FX modular components which use custom access control strategies within each system or module and shall include enabling an encrypted bi-directional interface between the authentication service and the authorization service, allowing user information to flow between the two (2) components. The authorization product shall provide federated integration with organization specific Active Directories of authorization information. Consent management is a possible future Integration Platform capability currently under consideration.

6.7.5.1 AUTHENTICATION

The IS/IP solution will authenticate all users accessing FX through a stakeholder Single Sign-On portal or system API interfaces. Security protocols and standards which follow NIST 800-53 profile for “moderate impact systems” with additions and applicable state and agency standards and requirements are outlined in the MITA 3.0 security requirement document.

Vendors will require APIs to send or receive data from FX. Any vendor hosting their own solution will be required to submit and follow a security plan that adheres to the NIST 800-53 profile for “moderate impact systems” with additions and applicable state and agency standards and requirements.

6.7.5.2 AUTHORIZATION

The Agency will require any vendor to provide an authentication and the authorization scheme which follows NIST 800-53 profile for “moderate impact systems” with additions and applicable state and agency standards and requirements for user access to authorized functions and systems.

6.7.5.3 ENCRYPTION

Due to the nature of the information and associated business risks, all Protected Health Information (PHI) and Personal Identifying Information (PII) will be encrypted for system receipt or handoff. Furthermore, all transmissions of data to the data warehouse will be encrypted. The following encryption standards will be implemented within MMIS regarding email, backup tapes, WEB interactions, and server interactions:

- Secure Socket Layers (SSL)
- AES-256 (Advanced Encryption Standard) encryption
- NIST approve transmission protocol
- WEB Certifications / bit key 256

The Agency requires vendors to obtain third party security assessment reports annually and submit them to the Agency for evaluation at which point the Agency will either recertify or require security system updates or changes according to a remediation plan.

Additional encryption requirements are as follows:

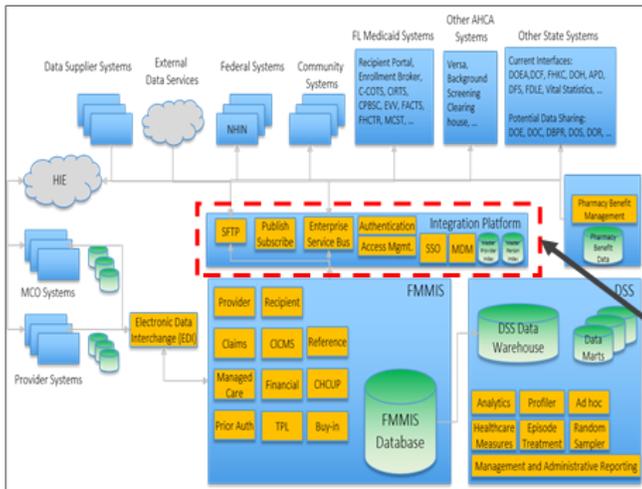
FIPS Encryption: Federal Information Processing Standard (FIPS) 140-2 level 1 encryption used on HNC data connections between sites.

Data-at-Rest Encryption: All Virtual Private Cloud and Traditional Backup and Restore (BUR) storage compartments will be provisioned with “data at rest” encryption enabled.

Conversion/Development/Testing Data: The database and application tiers for development, testing, and conversion will be separated to ensure that appropriate levels of access are granted. Development and testing areas that may be used by offshore developers and testers will be well-defined, compartmented and use only de-identified data, using Agency-approved security protocols.

Data-In-motion Encryption: Any inbound and outbound data transmissions must adhere to the FIPS Encryption noted above, this includes data across individual connections, used by Agency stakeholders.

Remote Access: All Virtual Private Network (VPN) remote access methods to the network compartments use SSL encryption.



AHCA is procuring the IS/IP, which includes the Enterprise Service Bus, System Integrator, and Enterprise Information Management. The IS/IP will enable secure real-time, or near real-time information exchange between systems while migration to data services occurs. This allows for implementation of modular capabilities that interact with legacy systems and other modular capabilities.

This implementation will also enable integration of non-Medicaid data sources and system integrations with MMIS business processing. Integrations between MMIS modular capabilities and non-Medicaid data sources and information types will use the integration services indefinitely.

To allow for future data types and decisions, the Agency is designing the IS/IP to be as flexible and scalable as possible.

This state is categorized by the following:

- Real-time, or near real-time, data sharing and reuse through the IS/IP is routine
- Identify duplicate recipient and provider links, link identified records across systems through Master Person and Master Provider Indexes
- Single sign-on, authorization, and access controls to support sharing data and processing services across systems and modular processing
- Improved secure file transfer capabilities
- An ability to send select real-time transaction data to the data warehouse to support real-time analytics and reporting

Figure 15: FX Security Description

SECTION 7 ANALYSIS OF THE PROPOSED SYSTEM

7.1 IMPACT ANALYSIS

7.1.1 OPERATIONAL IMPACTS

The enterprise integration capabilities of the IS/IP solution will allow Agency systems to be much more efficient in sharing data and services between systems within AHCA and with other agencies. Two major goals of the integration platform are (1) reduced duplication of data across systems, and (2) improved data consistency and communication of data changes between systems when there is a business need for data to be duplicated.

The IS/IP, will enable:

- Near real-time data, processing access and sharing between different organizations and systems, reducing the propagation of duplicated and inconsistent data
- A 360-degree view of information by linking data about recipients and providers
- Application of consistent business rules and policy
- Single sign-on and data protections

The enterprise data service and analytic capabilities of the Enterprise Data Warehouse Solution will provide Agency stakeholders with enhanced data management and analytics capabilities. The EDW creates a model that promotes having a “single source of truth” for applications to provide and access data from this central source (rather than keeping data within each application). The EDW Project decouples systems and data to make data available and consistent throughout the

ecosystem, which will improve data quality, consistency, and tools for operational data use and analytic processing. The EDW Solution will enable:

- A single source of truth to improve data quality, accuracy, and accessibility
- Improved timeliness and consistency of data
- Improved analytic data processing with holistic business unit and persona optimized data marts and tools
- System innovation and simplified system implementation
- The ability to eliminate inconsistent data and processing
- Reduction in duplicated data

The use of modular processing systems and service capabilities using the real or near real-time data provided by the EDW Solution, applying consistent business rules will reshape the application landscape, reducing duplicated applications and inconsistent processing. The implementation of Modular Systems Future State will:

- Retain and improve mature working operational business processing capabilities
- Standardize business processing (e.g. enrollment, case management) to improve recipient and provider experience
- Add new processing capabilities without the capacity constraints of a single vendor
- Enable use of processing services by external organizations and systems
- Enable high quality and accessible data
- Improve integration with external partners
- Reduce complexity
- Improve healthcare outcomes
- Enable holistic decision making
- Use evidence-based processing

7.1.2 ORGANIZATIONAL IMPACTS

The implementation of improved technologies will enable organizational change to improve the delivery of healthcare services. The foundational technologies and improved systems will reduce duplication, data inconsistency and processing delays. Within the Medicaid Enterprise Agencies reorganization, restructure, and consolidation will be possible to optimize business agility and service delivery. External to State Agencies, healthcare providers, and health plans may change organizational size and structure following improvements in efficiency and increased use of data for coordination of care. Specific future impacts are unknown. Anticipated changes include:

- Consolidation of policy administration and policy implementation within systems
- Consolidation of recipient, provider, and health plan interaction center (e.g. call center) operations
- A hybrid vertical and horizontal segmentation of service delivery by delivery model, claim type, advanced payment model, or recipient categorization

7.1.3 RISKS

The purpose of Risk Management is to address project risk in a controlled and intentional manner to realize the anticipated value of the project while balancing risk and reward. Formal risk management aims to identify and manage risks that are not addressed by other project management processes.

The SEAS Management Plan, outlines the processes used to identify, analyze, plan responses, and monitor and control risks associated with the project. The process will facilitate the development of action plans to reduce the probability of occurrence and contingency plans as appropriate to minimize the impact of a realized risk event on the project.

To be successful, Risk Management must be an ongoing process throughout the life of the project. The process begins with identifying and assessing significant risks, then developing appropriate response plans. It continues with regular risk monitoring, ongoing new risk identification, and timely plan implementation. Risks are communicated through the management structure as defined by the escalation process. As part of the risk response plan, the Risk Owner will determine which additional project stakeholders should be aware of potential risks throughout the project lifecycle.

The following set of key principles will guide the Risk Management Processes for the project:

- A risk has a cause, and if it eventually occurs, a consequence. As such, a risk is an uncertain event or condition which if it occurs, may result in a negative impact on the project objectives. Risk Management is the systematic process of identifying, assessing, responding, and controlling risks
- The probability of success for any project can be significantly increased through a formal, proactive, and iterative Risk Management approach. It is important risks are quickly identified, and appropriate steps are taken to address them
- Risk management is an iterative process which needs to occur throughout the project. As the project progresses, the project team becomes more knowledgeable and better equipped to identify and manage project risks. Additionally, risks evolve and change

Risk management includes the processes for conducting risk management planning, identification, analysis, response planning, response implementation, and monitoring risk on a project. The object of the risk management plan should be to increase the probability and/or impact of positive risks and to decrease the probability and/or impact of negative risks to ensure the chance of project success. An effective risk management process should include the following:

- Risks are reported and tracked in the project status report
- Risk Owner or designee reviews the risk description for completeness and accuracy
- Project Risks are logged with a unique identifier, categorized for impact and tolerance and linked to associated Issues, Action Items, and Decisions
- Risks are assigned an owner, a risk probability, impact, priority and a response strategy

- Risk response plans for risks with a high-risk score have been developed, have an owner and are being monitored and updated according to the risk response plan
- Risk Owners will conduct appropriate quantitative analysis as it is needed to assist in the decision-making process
- Risk Triggers are identified and monitored with status updated on a bi-weekly basis

This Risk Management Process addresses identified risks requiring visibility at the highest levels of the project. The Risk Management Process involves identifying and categorizing project risks (Identify), validating and logging the risk (Validate / Log), assessing and prioritizing the risks so they are manageable (Analyze), developing a response strategy and assigning responsibility (Plan), tracking the risks by reviewing them at key project milestones (Monitor/Track), and most importantly, communicating the risks and strategies on an ongoing basis throughout the life of the project (Communicate). Risk management processes address internal risks (those under the control or influence of the project team, such as quality of deliverables, cost, schedule, or technical risks) and external risks (those outside the control of the project team such as governmental legislation or force majeure).

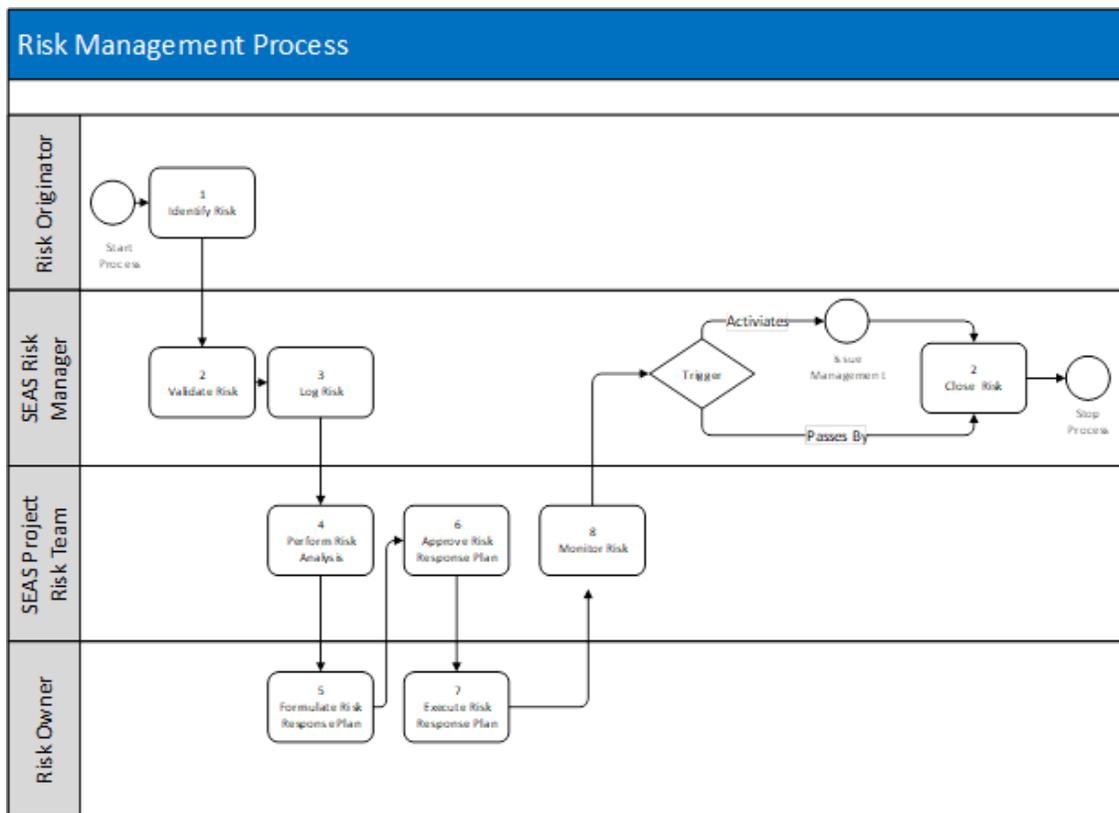


Figure 16: Risk Management Process

The table below lists the key project Risk Management activities:

ACTIVITY	APPROACH	PURPOSE
1 Identify Risk	<ul style="list-style-type: none"> ▪ Create a list of project risks; gather risks from stakeholders using brainstorming, predefined lists, and/or completion of risk form 	<ul style="list-style-type: none"> ▪ Identifies project risks before they become problems; helps to set expectations and provide a vehicle for reaching consensus – unknown risks cannot be managed
2 Validate Risk	<ul style="list-style-type: none"> ▪ Discuss all newly identified risks with the SEAS Project Risk Team, SEAS Director, FX Director, and affected stakeholders to establish credibility of the risk 	<ul style="list-style-type: none"> ▪ To ensure the information is complete, the identified risk is valid and not a duplicate
3 Log Risk	<ul style="list-style-type: none"> ▪ Log the risk in the Risk Log located on the FX Project Repository (MPR) 	<ul style="list-style-type: none"> ▪ To ensure the risk is thoroughly documented
4 Perform Risk Analysis	<ul style="list-style-type: none"> ▪ Determine the consequence of risks listed (probability and impact) and calculate the risk tolerance 	<ul style="list-style-type: none"> ▪ Transforms the risk data into decision-making information
5 Formulate Risk Response Plan	<ul style="list-style-type: none"> ▪ Determine desired risk strategies and actions, and assign responsibility 	<ul style="list-style-type: none"> ▪ Translates the risk information into strategies and mitigation actions
6 Approve Risk Response Plan	<ul style="list-style-type: none"> ▪ Gather consensus on risk strategies and actions and approve their assignment to an owner(s) 	<ul style="list-style-type: none"> ▪ Assigns accountability to Risk Owner
7 Execute Risk Response Plan	<ul style="list-style-type: none"> ▪ Mobilize action plans 	<ul style="list-style-type: none"> ▪ Risk Response actions are executed such that the probability of the risk occurring, and the impact are minimized

ACTIVITY	APPROACH	PURPOSE
8 Monitor Risk	<ul style="list-style-type: none"> ▪ Review and re-examine risks when the project situation changes or key milestones are achieved. Discuss and review project risks and plans in project status, or other scheduled meetings, when the project situation changes or key milestones are achieved 	<ul style="list-style-type: none"> ▪ Monitors risk indicators and risk response actions
9 Close Risk	<ul style="list-style-type: none"> ▪ As part of risk monitoring, when the SEAS Project Risk Team, SEAS Director, or FX Director agrees the risk can no longer occur, the probability of the risk will be changed to zero and the status will be set to “Closed” 	<ul style="list-style-type: none"> ▪ Enables the SEAS Project Risk Team to remain focused on active risks which have a potential to affect the project

Table 9: Risk Management Activities

Risks to the project reflect risks to the FX solution and any additional risks identified in the future will be incorporated into the complete list of project risk.

Potential risks to the solution itself have been identified and collected in the table that follows. These risks, while not affecting projects related to the development of various ITNs should be considered when moving forward.

RISK DESCRIPTION	PREFERRED ALTERNATIVE ADDRESSES	PREFERRED ALTERNATIVE DOES NOT RESOLVE
Failed, inaccurate or untimely replication processes between the current MMIS and EDW may affect recipient services, payments to providers, and may have the potential to expose the system to fraud and abuse.	Y	Y
Implementing a system of the scale and complexity envisioned presents the challenge of employing potentially unproven technologies and architectural concepts.		Y

RISK DESCRIPTION	PREFERRED ALTERNATIVE ADDRESSES	PREFERRED ALTERNATIVE DOES NOT RESOLVE
The current inconsistent application of data edits, validations, and transformations to the many different Agency data stores means there is no single source of truth which causes confusion and lack of trust in the data.		Y
Poor analytic processing response times	Y	
Inconsistency in use of analytics, predictive modeling, and reporting capabilities	Y	Y

Table 10: Solution-related Risks

7.1.4 ISSUES TO RESOLVE

Risks may develop into Issues and ultimately result in Action Items which will provide resolution. Disciplined management of Issues and Action Items enables a project team to effectively resolve the issues and complete action items promptly and keep a project on track. A formal Issue / Action Item Management process provides the mechanism throughout the lifecycle of the project to bring issues and action items to resolution.

- **Issue** - An Issue is an existing constraint negatively impacting project timeliness, quality, resources, or cost. Issues requiring attention from another level or area within the project governance structure will be subject to the formal issue escalation process.
- **Action Item** - An Action is a proactive task identified by the SEAS Project Team to address a known problem or situation. Actions may also come from a risk or issue item. Incomplete or overdue action items may create issues.

The first step in creating an effective Issue/Action Item management process is defining how the process should work. The following table describes the SEAS Project Team’s roles and responsibilities for reporting issues and action items.

ROLE	RESPONSIBILITY
Issue/Action Item Originator	Anyone can originate an issue or action item. Responsibilities include: <ul style="list-style-type: none"> ▪ Identify an issue requiring resolution in accordance with the Issue/Action Item documented processes ▪ Define the issue/action item as required ▪ Review and approve action plan/resolution to ensure issue as originally defined will be resolved

ROLE	RESPONSIBILITY
SEAS Risk Manager	<ul style="list-style-type: none"> ▪ Log action items identified during the project ▪ Facilitate the identification of issues and action items at project meetings ▪ Perform analysis on issues ▪ Assist Issue/Action Item Originators with defining and documenting risks and presenting new issues and action items to the FX EPMO Team ▪ Identify and assign an Issue/Action Item Owner for each issue or action item ▪ Ensure identified issues are analyzed and issue action plans are approved and implemented as required ▪ Periodically review issues and action items with Issue/Action Item Owners ▪ Provide effective communication ▪ Ensure issues and action items are recorded in the risk log
Issue/Action Item Owner	<p>The Issue/Action Item Owner can be found at any level within the project organizational structure. The Issue/Action Item Owner’s responsibilities include:</p> <ul style="list-style-type: none"> ▪ Collaborate with the SEAS Project Team regarding the status of the issue or action item until it is closed ▪ Participate in discussions with the Issue/Action Item Originator to fully understand the issue or action item ▪ Research and draft the Action plan/resolution ▪ Attend bi-weekly status meetings to discuss/report on a complex issue (on an as needed basis) ▪ Drive the issue/action item to resolution and closure

Table 11: Issues and Action Items Roles and Responsibilities

Issue or Action Item submission provides the first step in the issue and action item management process and starts with the Issue/Action Item Originator who identifies a project issue or action. The SEAS Risk Manager should review the issue and or action items in the tracking log to make sure the issue/action item has not already been reported and possibly resolved.

The Issue/Action Item Originator must describe the issue/action item and include any other information which could be helpful to whoever is assigned the issue/action item for resolution.

An issue may be identified in any number of ways. For example:

- A problem which is negatively impacting the project for which there is no apparent answer
- A current situation or event which could or is negatively impacting the project and cannot be answered immediately but requires some research and analysis to provide insight into actions which should be taken

- An inability of two project entities or functional groups to come to an agreement on an item or process
- An Action Item with a late due date which, if not completed, will negatively impact the project
- The need for information external to the project inhibits or stops the development of the project objectives, deliverables, and/or solution until resolved
- A trigger, as defined in the Risk Log, has been activated for a currently identified risk

An Action Item is a discrete project activity or group of activities with planned start and end dates and project resources allocated to the activities. Action items contribute to the completion of project deliverables and/or the resolution of project threats, opportunities, issues, and corrective action plans.

Action Items are tracked at the project level as a part of the project management execution and monitoring and controlling processes for managing the completion of project schedule work streams.

Project level action items are typically the result of and tied to risk response plans, issue action plans, and escalated project team action items and are tracked in the Action Item Log.

Project team level action items are typically the result of project team meetings and are documented in project Meeting Minutes and tracked at the project team level.

Once the issue or action item has been documented and assigned, the Issue/Action Item Owner will analyze the Issue/Action Item and develop a plan for resolution which describes the activities which need to be completed to close the item.

Project issues and action items not resolved within a reasonable timeframe or deemed to cause project delay will need to be escalated within the SEAS Project Leadership Team () in the following manner:

- Escalation Level 1: FX Domain Leads and SEAS Domain Project Managers
- Escalation Level 2: FX SEAS Contract Manager and SEAS Contract Manager
- Escalation Level 3: FX Director and SEAS Director

In the event the issue is unable to be resolved with the SEAS Project Leadership Team, it will need to be escalated to the next level in the governance structure.

Exhausting all options for resolution at the current level can also be considered a reason to escalate. The SEAS Project Risk Team and the SEAS Risk Manager will agree to escalate the given issue or issues at each level before escalation. Escalated issues and action items documented on the FX Project Repository, should indicate “Escalated” under the Status column, and the appropriate name of the assigned new owner is entered under the Assigned to column.

Example criteria for escalating issues include:

- An issue or action item with a priority of high whose resolution is more than seven calendar days past due
- An issue or action item with a priority of medium whose resolution is more than fourteen calendar days past due
- An issue has reached an impasse and cannot be resolved within the current level
- An agreement cannot be reached on the severity of an issue
- An issue or action item is not making adequate progress toward resolution or completion and is determined by the FX EPMO or SEAS Project Risk Teams will have a negative impact on the project

If an issue is significant and an impact analysis reveals the resolution would impact cost, scope, or the schedule critical path, then the issue should be escalated according to the escalation process defined in the Scope Management Plan. The current list of issues can be found at: [FX Issue Log](#)

7.1.5 CRITICAL SUCCESS FACTORS FOR REMAINDER OF PROJECT

#	Description of Success Factors	How will the Criteria be measured/assessed?
1	Completion of CMS milestone reviews throughout the Medicaid Enterprise Certification Life Cycle using the current Medicaid Enterprise Certification Toolkit (MECT), achievement of CMS certification for Medicaid Enterprise System, and approval for enhanced FFP.	Measured and assessed by CMS through the CMS-prescribed certification process
2	Architecture enables enhanced data: integrity, reliability, single source of truth, availability in real-time, analytics and analysis.	Assessed by the Agency’s SEAS management team and designated Agency Subject Matter Experts
3	Enhanced Provider Experience improving all areas where the provider interacts with the Agency, which will include the following: enrollment, claims process, and, reimbursement, among others.	Assessed by the Agency’s SEAS management team and designated Agency Subject Matter Experts
4	Improved Program Integrity which provides the Agency the ability to more accurately identify improper payments and discrepancies.	Assessed by the Agency’s SEAS management team and designated Agency Subject Matter Experts
5	Improved Recipient Experience and Health Outcomes.	Measured through Healthcare Effectiveness Data and Information Set (HEDIS) and Consumer Assessment of Healthcare Providers and Systems (CAHPS) quality indicators

Table 12: Critical Success Factors

SECTION 8 GLOSSARY

Term / Acronym	Definition
AES	Advanced Encryption Standards
Agency	Florida Agency for Health Care Administration
AHCA	Florida Agency for Health Care Administration
AHS	Automated Health Solutions
APD	Agency for Persons with Disabilities
API	Application Programming Interface
ASR	Application Service Registry
BUR	Backup and Restore
CAHPS	Consumer Assessment of Healthcare Providers and Systems
C-COTS	Claims Complaint Oversight System
CDM	Conceptual Data Model
CHCUP	Child Health Checkup
CIRTS	Client Information and Registration Tracking System
CMS	Centers for Medicare and Medicaid Services
CM	Content Management
COTS	Commercial-Off-The-Shelf
CPBSC	Care Provider Background Screening Clearinghouse
DCF	Department of Children and Families
DFS	Department of Financial Services
DJJ	Department of Juvenile Justice
DOEA	Department of Elder Affairs
DOH	Department of Health
DRG	Diagnosis Related Grouping
DSS	Decision Support System
EAPG	Enhanced Ambulatory Patient Grouping
ECDM	Enterprise Conceptual Data Model
EDI	Electronic Data Interchange
EDW	Enterprise Data Warehouse
ESB	Enterprise Service Bus
ETL	Extract Transform Load
EVV	Electronic Visit Verification
FCS	Florida Cybersecurity Standards
FDLE	Florida Department of Law Enforcement
FFM	Federally Facilitated Marketplace
FFP	Federal Financial Participation
FFS	Fee for Service
FHA	Federal Health Architecture
FHCTR	Fair Hearing Case Tracking and Reporting
FHIM	Federal Health Information Model
FHIR	Fast Healthcare Interoperability Resources

FHKC	Florida Healthy Kids Corporation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act or Federal Information Security Modernization Act
FMMIS	Florida Medicaid Management Information System
FTP	File Transfer Protocol
FX	Florida Health Care Connection
HEDIS	Healthcare Effectiveness Data and Information Set
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HL7 RIM	Health Level 7 Reference Information Model
HQA	Health Quality Assurance
IS/IP	Integration Services and Integration Platform
IT	Information Technology
ITN	Invitation to Negotiate
IV&V	Independent Verification and Validation
IVR	Interactive Voice Response System
LBR	Legislative Budget Request
MCST	Managed Care Survey Tool
MDM	Master Data Management
MECT	Medicaid Enterprise Certification Toolkit
MES	Medicaid Enterprise System
MFA	Medicaid Fiscal Agent
MFAO	Medicaid Fiscal Agent Operations
MFCU-OAG	Medicaid Fraud Control Unit - Office of the Attorney General
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MOI	Master Organization Index
MPI	Master Person Index
MPR	Medicaid Enterprise Project Repository
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NwHIN	Nationwide Health Information Network
ODS	Operational Data Store
ONC	Office of National Coordinator for Health Information Technology
PA	Prior Authorization
PBM	Pharmacy Benefit Management
PBMS	Prescription Benefit Management System
PHI	Protected Health Information
PII	Personal Identifying Information
PMO	Project Management Office
PNV	Provider Network Verification
POAR	Persona Optimized Analytics and Reporting

POS	Point of Sale
QA	Quality Assurance
RDS	Reporting Data Store
RHIO	Regional Health Information Organizations
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDS	Specialized Data Store
SEAS	Strategic Enterprise Advisory Services
SFTP	Secured File Transfer Protocol
SME	Service Management Engine
SMMC	Statewide Medicaid Managed Care
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SQL	Structured Query Language
SS-A	MITA State Self-Assessment
SSL	Secure Socket Layers
SSO	Single Sign-On
SSOT	Single Source of Truth
TCO	Total Cost of Ownership
TPL	Third Party Liability
TSRG	Technology Standards Reference Guide
UI	User Interface
VPN	Virtual Private Network
WS	Web Services
XML	Extensible Markup Language

SECTION 9 APPENDICES

[Appendix A – Technology Deliverables](#)

[Appendix B – Technology Standards](#)

[Appendix C – Inbound and Outbound Interfaces](#)

APPENDIX A: TECHNOLOGY DELIVERABLES

Technology Deliverable	Source
T-1 Data Management Strategy	T-1: Data Management Strategy
T-2 Information Architecture	T-2: Information Architecture
T-3 Data Standards	T-3: Data Standards
T-4 Technical Management Strategy	T-4: Technical Management Strategy
T-5 Technical Architecture	T-5: Technical Architecture
T-6 Technology Standards	T-6: Technology Standards
T-7 Design Implementation Management Strategy	T-7: Design Implementation Management Strategy
T-8 Enterprise Data Security	T-8: Enterprise Data Security

APPENDIX B: TECHNOLOGY STANDARDS

Category	Standard Name	Objective	Source
Project Documentation	Florida Information Technology Project Management and Oversight Standards	This is AST rule 74-1 which establishes project management standards when implementing information technology (IT) projects. State Agencies must comply with these standards when implementing all IT projects. Cabinet Agencies must comply with these standards when implementing IT projects that have a total cost of \$25 million or more and that impact one or more other agencies (pursuant to Section 282.0051(15)(a), F.S.). For all other IT projects, Cabinet Agencies are required to either adopt these standards or adopt alternative standards based on best practices and industry standards (See Section 282.00515, F.S.). These standards are documented in Rule 74-1.001 through 74-1.008, F.A.C.	Florida IT AST Rule 74-1
Design	Business Process and Rules Management Plan	The Business Process and Rules Management Plan provides the processes for managing the business requirements, business rules, user requirements, and functional / nonfunctional requirements for the project. It may also contain use case scenarios to help clarify the process required for the project.	FX Business Process and Rules Management Plan Template
Requirements	Requirements Management Plan	This Integrated System Requirements Management Plan (RM Plan) describes in detail the system requirements, including the vision, global design requirements, and business requirements for guidance and use during the development of the FX <project name>.	FX Requirements Management Plan Template
Design	Systems Impact Analysis Management Plan	The Systems Impact Analysis Management Plan is to communicate all possible inputs and outputs from the system for all potential actions whether they are internal to the system or transparent to system users. This plan helps ensure	FX Systems Impact Analysis Management Plan Template

		compatibility between system segments and components.	
Development	Configuration Management Plan	This Configuration Management (CM) Plan establishes the technical and administrative direction and surveillance for the management of configuration items (i.e. software, hardware, and documentation) associated with the <Project Name (Acronym)> that are to be placed under configuration control.	FX Configuration Management Plan Template
Requirements	(System) Change Management Plan	Provide a high-level overview of the project and a description of how the <Project Name> change management activities are processed in accordance with the Integrated Change Control Process defined in the FX P2: Project Management Plan, specifically the Interim PMO – Scope Change Management Plan.	FX Change Management Plan Template
Testing	Testing Management Plan	The Testing Management Plan describes the overall technical and management approach, resources, and schedule for all intended test activities associated with development, validation, implementation, and operational testing.	FX Testing Management Plan Template
Maintenance	Software Problem Resolution Standards and Procedures Plan	This Software Problem Resolution Standards and Procedures Plan (SPR Plan) describes the approach for continued software development process improvement during the life cycle of the <Project Name (Acronym)>. The document identifies the specific actions that will be taken to improve the software process and outlines the plans for implementing those actions.	FX Software Problem Resolution Standards and Procedures Plan Template
Maintenance	Integrated System Implementation Management Plan	This Integrated System Implementation Management Plan (IM Plan) describes how the automated system/application or IT situation will be installed, deployed and transitioned into an operational system or situation.	FX Integrated System Implementation Management Plan Template

Maintenance	Integrated Program Operations and Maintenance Planning/Deployment Plan	The Integrated Program Operations and Maintenance Planning/Deployment Plan (O&M Plan) is the guide for those who maintain, support and/or use the system in a day-to-day operations environment.	FX Integrated Program Operations and Maintenance Planning/Deployment Plan Template
Maintenance	Post Implementation Evaluation Plan	The Post Implementation Evaluation Plan is an internal evaluation to confirm that a system is operating according to design and that users are satisfied with the performance of the system. This plan represents the transition from design and implementation stage to the operations stage and signals the start of monitoring metrics established for the system.	FX Post Implementation Evaluation Plan Template
Testing	Quality Management Plan	The Quality Management Plan documents the necessary information for planning, managing, and controlling project and product quality to meet FX objectives. It defines the project's quality policies, procedures, areas of application and associated criteria, and roles and responsibilities.	FX Quality Management Plan Template
Maintenance	CMS Contingency Planning Standards	CMS is reliant on its information systems for mission fulfillment. Information systems are susceptible to a wide variety of events and threats that may affect their ability to process, store and transmit raw data and information. Contingency planning is one method of reducing risk to CMS' operations by providing prioritized, efficient, and cost-effective recovery strategies and procedures for the organizations' Information Technology (IT) infrastructure. The CMS Contingency Planning Standard is consistent with the guidance of the National Institute of Standards and Technology (NIST) and most specifically with NIST Special Publication (SP) 800-34 revision 1, <i>Contingency Planning Guide for Federal Information Systems</i> 2 dated May 2010. Effective	CMS Contingency Planning Standard

		<p>contingency planning requires clear and concise:</p> <ul style="list-style-type: none"> · Disaster declaration criteria, and · Recovery prioritization. <p>These, in turn, require:</p> <ul style="list-style-type: none"> · Accurate identification of functions performed by the system, · Accurately mapping any functions that rely on other systems, · Determining impact to the organization for loss of any or all functions (and thereby determine functional recovery prioritization). 	
Maintenance	Disaster Recovery Plan	The Disaster Recovery (DR) Plan provides step-by-step procedures to identify, address, and recover from disaster events. It also emphasizes the need to minimize negative impacts to the project and resume normal operations.	FX Disaster Recovery Plan Template
Maintenance	NIST IT Contingency Planning Guide	<p>NIST Special Publication 800-34, Rev. 1, <i>Contingency Planning Guide for Federal Information Systems</i>, provides instructions, recommendations, and considerations for federal information system contingency planning. Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods. This guide addresses specific contingency planning recommendations for three platform types and provides strategies and techniques common to all systems. Client/server systems Telecommunications systems Mainframe systems</p> <p>This guide defines the following seven-step contingency planning process that an organization may apply to develop and maintain a viable contingency planning program for their information systems.</p>	NIST SP 800-34, Revision 1

Architecture, Analysis and Design Standards	Database Naming Standards	These are the database naming standards of the MMIS system.	Database Naming Standard
Architecture, Analysis and Design Standards	Reporting Implementation Procedures	The purpose of this document is to identify and communicate the report promotion procedures within the Agency to achieve data validity, security, efficiency, and conformity.	Reporting Standards
Architecture, Analysis and Design Standards	Continuity of Care Record (CCR)	CCR is a core data set of relevant administrative, demographic, and clinical information facts about a patient’s health care, covering one or more encounters. It provides a communication method between practitioner, system, or setting and aggregates the pertinent data. There are three core components, the CCR Header, the CCR Body, and the CCR Footer.	Continuity of Care Record Standard
Data Standards	Current Dental Terminology (CDT)	CDT is a code set with descriptive terms developed and updated by the American Dental Association (ADA) for reporting dental services and procedures to dental benefits plans.	Dental Terminology Code Set
Architecture, Analysis and Design Standards	Digital Imaging Communications in Medicine (DICOM)	DICOM standards enable stakeholders to retrieve images and associated diagnostic information, transfer them from various manufacturers’ devices and medical workstations.	DICOM Standards
Architecture, Analysis and Design Standards	Logical Observation Identifiers Names and Codes (LOINC)	LOINC is a database and universal standard for identifying medical laboratory observations, developed and maintained by the Regenstrief Institute. The creation of LOINC was in response to the demand for an electronic database, for clinical care and management. It is publicly available at no cost.	LOINC Standards
Architecture, Analysis and Design Standards	Public Health Information Network (PHIN)	Public Health Information Network (<i>PHIN</i>) is a national initiative to increase the capacity of public health agencies to electronically exchange data and information across organizations and jurisdictions.	PHIN

Architecture, Analysis and Design Standards	Systematized Nomenclature of Medicine – Clinical Terms (SNOMED CT)	This is the most comprehensive set of multilingual clinical healthcare terminology. Its aim is to improve patient care through the development of standardized clinical terminology regardless of language.	SNOMED CT
Architecture, Analysis and Design Standards	Unified Medical Language System (UMLS)	This is a set of files and software collections from health and biomedical vocabularies and standards to enable interoperability between systems.	UMLS Standards
Service Interoperability	Open Data Protocol (OData)	OData, short for Open Data Protocol, is an open protocol to allow the creation and consumption of queryable and interoperable RESTful APIs in a simple and standard way.	OData Standards
Data Standards	Current Procedural Terminology, Fourth Edition (CPT-4)	A listing of descriptive terms and identifying codes for reporting medical services and procedures. Covers physician services, physical therapy, occupational therapy, radiology, medical diagnostic procedures, hearing, vision, and medical transportation.	CPT-4 Standards
Data Standards	Diagnosis Related Group (DRG)	System to classify hospital cases into groups expected to have similar hospital resource use.	DRG
Data Standards	Healthcare Common Procedure Coding System (HCPCS)	Set of healthcare procedure codes based on the American Medical Association's Current Procedural Terminology (CPT) which are used to provide healthcare claims that are managed consistently and in an orderly manner.	HCPCS
Data Standards	ICD-10	The 10th revision of a medical classification list by the World Health Organization (WHO) which contains codes for diseases, signs and symptoms, abnormal findings, complaints, social circumstances, and external causes of injury or diseases.	ICD-10

Data Standards	National Drug Codes (NDC)	The National Drug Code is a unique product identifier used in the United States for drugs intended for human use. The Drug Listing Act of 1972 requires registered drug establishments to provide the Food and Drug Administration (FDA) with a current list of all drugs manufactured, prepared, propagated, compounded, or processed by it for commercial distribution.	NDC
Data Standards	Global Trade Identification Number (GTN)	GTN is an identifier for trade items, developed by GS1, used to look up product information in a database which may belong to a retailer, manufacturer, collector, researcher, or other entity.	GTN
Data Standards	Health Industry Bar Code – Labeler Identification Code (HIBC-LIC)	Establishes and maintains unique identifiers and labeling standards for medical equipment, supplies, and devices.	HIBC-LIC
Data Standards	Arden Syntax	The Arden Syntax is a formalism for representing procedural clinical knowledge to facilitate the sharing of computerized health knowledge bases among personnel, information systems and institutions.	Arden Syntax
Data Standards	Clinical Context Object Workgroup, Management Specification (CCOW)	HL7 Standard protocol designed to enable disparate applications to synchronize in real time, and at the user-interface level. CCOW serves as the basis for ensuring secure and consistent access to patient information from heterogeneous sources.	CCOW
Data Standards	Clinical Document Architecture (CDA)	HL7 XML-based markup standard intended to specify the encoding, structure and semantics of clinical documents for exchange.	CDA
Data Standards	IEEE 1073	Medical / health device communication standards enable communication between medical, healthcare and wellness devices and with external computer systems.	IEEE 1073

Data Standards	Abstract Syntax Notation One (ASN.1)	Data syntax and constraint language that describes rules and structures for representing, encoding, transmitting, and decoding data in telecommunications and computer networking.	ASN.1
Data Standards	ebXML Business Process Specification Schema (BPSS)	ebXML specification schema provides a standard framework to configure business systems to support business transactions.	ebXML BPSS
Data Standards	ebXML Collaboration-Protocol Profile and Agreement Specification	Standard for two or more business partners to engage in business transactions based on each party's message exchange capabilities as described in a Collaboration Protocol Profile (CPP) and agreed to in a Collaboration Protocol Agreement (CPA).	ebXML Collaboration-Protocol
Data Standards	ebXML Message Service Specification (EbMS)	Defines the message envelope and header schema used to transfer ebXML messages over a communications protocol (e.g. HTTP or SMTP) and the behavior of software sending and receiving ebXML messages.	EbMS
Data Standards	International Organization for Standardization: Information Technology — Metadata Repository Standard (ISO 11179)	ANSI standard that supports registration of data regardless of syntax, naming and definition conventions, and registry interoperability.	ISO 11179
Data Standards	International Organization for Standardization: Protocol for Information Search and Retrieval (ISO 23950)	Standard client–server, application layer communications protocol for searching and retrieving information from a database over a TCP/IP computer network.	ISO 23950
Data Standards	Object Constraint Language (OCL)	UML-based standard for specifying the refinements of artifacts based on models that are essential for documenting collaboration profiles.	OCL Standards

Data Standards	Federal Health Information Model (FHIM)	A model of healthcare data developed for the FHA partner agencies seeking to develop a common Logical Information Model or Computationally Independent Model (CIM).	FHIM Standards
Data Standards	X12 Companion Guide (834)	Companion Guide for ASC X12 Benefit Enrollment and Maintenance (834) transaction type.	X12 834 Companion Guide
Data Standards	X12 Companion Guide (837P)	Companion Guide for ASC X12 Professional Health Care Claim (837P) transaction type.	X12 837P Companion Guide
Data Standards	X12 Companion Guide (278)	Companion Guide for ASC X12 Health Care Services Review (278) transaction type.	X12 278 Companion Guide
Data Standards	X12 Companion Guide (835)	Companion Guide for ASC X12 Health Care Claim Payment and Remittance (835) transaction type.	X12 835 Companion Guide
Data Standards	X12 Companion Guide (837I)	Companion Guide for ASC X12 Institutional Health Care Claim (837I) transaction type.	X12 837I Companion Guide
Data Standards	X12 Companion Guide (837D)	Companion Guide for ASC X12 Dental Health Care Claim (837D) transaction type.	X12 837D Companion Guide
Data Standards	X12 Companion Guide (820)	Companion Guide for ASC X12 Health Care Premium Payment (820) transaction type.	X12 820 Companion Guide
Data Standards	X12 Companion Guide (277U)	Companion Guide for ASC X12 Health Care Payer Unsolicited Claim Status (277U) transaction type	X12 277U Companion Guide
Data Standards	X12 Companion Guide (276/277)	Companion Guide for ASC X12 Health Care Claim Status Request and Response (276/277) transaction type	X12 276/277 Companion Guide
Data Standards	X12 Companion Guide (270/271)	Companion Guide for ASC X12 Health Care Eligibility Inquiry and Response (270/271) transaction type	X12 270/271 Companion Guide
Data Standards	Database Object Naming	Centers for Medicare & Medicaid Services (CMS) standard for database object naming.	CMS Database Object Naming Standards
Data Standards	UML Modeling	UML Modeling Specification for the design of persistent data.	UML Modeling Specification Version 2.5.1

Data Standards	Web Services Metadata Exchange	Specification that defines how metadata associated with a web service can be represented as WS-Transfer resources or HTTP resources, how metadata can be embedded in WS-Addressing endpoint references, how metadata could be retrieved from a metadata resource, and how metadata associated with implicit features can be advertised.	Web Services Metadata Exchange
Data Standards	International Organization for Standardization: Information Technology — Statistical Data and Metadata Exchange Standard (ISO 17369)	ANSI standard that provides an integrated approach to facilitating Statistical Data and Metadata Exchange (SDMX), enabling interoperable implementations within and between systems concerned with the exchange, reporting and dissemination of statistical data and related metadata.	ISO 17369
Business Enabling Technologies	Data Visualization Tool	Tableau is the AHCA tool standard for data visualization	Tableau Data Visualization Tool
Data Standards	Data Archiving	Standards for the archival and storage of data in any form (e.g. electronic, paper).	
Data Standards	Data Purging Standards	Standards for the permanent destruction of data in any form (e.g. electronic, paper).	
Data Standards	Records Retention	Standards for the retention of information in any form (e.g. electronic, paper)	
Data Standards	Data Standards for Eligibility	Data format standards for eligibility (e.g. always keep first data instance).	
Data Standards	Record Locking Patterns	Standard patterns for record locking (e.g. original value, time stamping).	
Architecture, Analysis and Design Standards	Information Logging	Standards for information logging across application portfolios including log categorization and archiving of logs.	
Architecture, Analysis and Design Standards	Code Repository Management	Standards for how code is managed in the code repository including patterns for check in, check out, labeling, branching, and merging.	

Architecture, Analysis and Design Standards	Service Versioning	Standards and patterns for how services are versioned.	
Data Standards	Data Monetization	Standards for generating measurable economic benefit from available data sources.	
Data Standards	Geographic Information System (GIS) Data Standards	Standards for the collection, storage, and use of Global Information System (GIS) data.	
Data Standards	Data Ownership Standards	Standards for data ownership.	
Data Standards	Content Management Data Storage	Standards for content management storage.	
Data Standards	Data Normalization	Standards for the normalization of data.	
Data Standards	Metadata Standards	Standards for the level of granularity and storage of metadata.	
Data Standards	Data Redaction	Data redaction standards for the protection of sensitive information.	
Data Standards	Records Retention	General Records Schedule GS-1 for State and Local Government	Florida DOS General Records Schedule GS1-SL
Data Standards	Records Retention	Records Retention schedule of the Centers for Medicare and Medicaid Services (CMS)	CMS Records Retention Guidance
Project Documentation	Document Naming Standards	USGS S&L Medicaid Implementation Services Documentation Procedures and Standards How to Documents FL MMIS	USGS S&L MMIS Documentation Procedures and Naming Standards
Security and Privacy	Liberty Alliance – Federated Approach	Federated network identity is the key to reducing the friction between the need to share, the desire for autonomy, and the need for clear identity without centralized control. A federated network identity model will ensure that appropriate parties use critical private information. Liberty Identity Federation Framework (ID-FF) offers a viable approach for implementing such as single sign-on and federated identities.	Project Liberty

<p>Security and Privacy</p>	<p>Security Assertion Markup Language (SAML)</p>	<p>SAML defines a framework for exchanging security information between online business partners. SAML defines a common Extensible Markup Language (XML) framework for exchanging assertions between entities to define, enhance, and maintain a standard XML-based framework for creating and exchanging authentication and authorization information. SAML requires agreements between source and destination sites about information such as Uniform Resource Locators (URLs), source and destination IDs, certification and keys, and other information in the form of metadata. This standard captures the metadata in a standard format as attributes used by SAML entities. The entities define Identity Providers, Service Providers, Attribute Authorities, Attribute Consumers, Authorization Decision Authorities, and Affiliate Members.</p>	<p>SAML Standards</p>
<p>Security and Privacy</p>	<p>Enterprise Privacy Authorization Language (EPAL) – W3C</p>	<p>EPAL goes beyond an application and lays out a standard to protect customers’ and citizens’ private information enterprise-wide. Customer and citizen information should be private and secure based on a global enterprise-wide privacy policy. The enterprise privacy policy defines a set of rules where each rule can allow a set of data users to perform an action in a set of actions on a category in a set of categories for any purpose(s).</p>	<p>EPAL W3C</p>
<p>Security and Privacy</p>	<p>WS-Trust Model</p>	<p>This standard takes the Liberty Alliance Trust Guidance reviewed by a broader, more inclusive community. Most concepts are the same as the earlier Liberty Alliance Trust Guidelines.</p>	<p>WS-Trust Model</p>
<p>Security and Privacy</p>	<p>eAuthentication and use of services Object Management Group (OMG) initiative</p>	<p>The OMG initiative is an additional security team with FEA SPP. This team is considering extending and adding additional security and privacy services. The United States Department of Agriculture (USDA)</p>	<p>The OMG Initiative</p>

		has established an eAuthentication setup. Organization for the Advancement of Structured Information Standards (OASIS) tested and proved the E-Gov eAuthentication initiative using WS-* standards.	
Security and Privacy	Public Key Infrastructure (PKI)	This standard describes how communities share policies and authorization schemes based on sharing attributes known as proxy credentials. It enables entity A to grant entity B the authorization right with others as if it were A. This profile allows limited proxy by providing a framework for carrying policies in Proxy Certificates. X.509 Public Key Infrastructure (X.509) started in 1988. Since that time, several Requests for Comments (RFC) exist for the X.509 standard specifying formats for public key certificates, certificate revocation lists, attribute certificates, and certification path validation algorithm. RFC 3820 is the most popular.	Public Key Infrastructure
Security and Privacy	Health Security	ISO/International Electrotechnical Commission (IEC) 27002:2013 “Code of practice for information security controls”. Standards and Certification Criteria for Electronic Health Records (EHR). Metadata Standards to Support Nationwide Electronic Health Information Exchange.	ISO Health Security Standards
Security and Privacy	Unified Modeling Language (UMLsec) and Security Engineering Profiles	UMLsec is an extension to the Unified Modelling Language for integrating security related information in UML specifications. This information can be used for model-based security engineering. Efforts to create new security stereotypes to integrate them with the UML 2.0 activity diagrams along with other formal Message Sequence Chart extensions.	Presenting the Profile to the Object Modeling Group

Security and Privacy	Security and Privacy Data Content Labeling and XML Access Authorization	Oracle Labeling Security has strong appeal, and there is extensive background information on distributed labeling (e.g. the work at Cornell by Andrew Meyers, et al). This is necessary for cross-line of business security and privacy control.	Security and Privacy Data Content Labeling
Security and Privacy	Consumer Health Informatics (CHI) Initiatives	CHI is a Kaiser Foundation Model that assists in minimizing the gap between patients and health resources. HITECH and other initiatives have grown from this model. There are a variety of sources for standards: <ul style="list-style-type: none"> · Electronic Health Records Systems (EHR-S) · NwHIN 	CHI Initiatives
Security and Privacy	Identity Management	The purpose of the Identity Management rule is to ensure that Identity Management Services provide secure, reliable and interoperable mechanisms for authenticating the identity of devices, application services, and Users that consume state information and application resources. This rule is modeled after the Identity Ecosystem Framework Baseline Functional Requirements v1.0, October 15, 2015.	Florida Security Rules
Security and Privacy	Federal Information Processing Standards (FIPS) 140-2	U.S. Government standard to approve cryptographic modules, functions, and algorithms that defines four levels of security: Level 1 - Basic security with one approved algorithm or function and no physical security mechanism Level 2 - Enhanced physical and tamper detection requirements Level 3 - Tamper resistant and mitigation requirements for Critical Security Parameters (CSP) to detect and respond to attempted access or modification of cryptographic modules Level 4 - Provides complete tamper and physical protection. Intended for cryptographic operation in open or uncontrolled environments with	FIPS 140-2

		protection features for environmental and operational fluctuations	
Security and Privacy	Physical Access and Security	The purpose of this rule development is to provide operational management and oversight regarding the state data center.	Florida Rules on Physical Security
Security and Privacy	Web Security Best Practices	The purpose of this document is to ensure that the applications developed in-house or bought off-the-shelf adhere to and enforce the security requirements needed to make the application function in a secure manner and free from flaws that could be exploited.	Web Security
Security and Privacy	SSO Access Controls Standards and Procedures	The purpose of this document is to ensure adherence to CJIS Security Policy and regulate user access to data and the extent of each user's access.	SSO Access Control Standards
Security and Privacy	NIST Framework to HIPAA Security	This crosswalk document identifies “mappings” between NIST’s Framework for Improving Critical Infrastructure Cybersecurity and the HIPAA Security Rule.	NIST Framework for HIPAA
Security and Privacy	Public Key Infrastructure (PKI)	x.509 Certification Standard	PKI x.509 Certification Standards
Security and Privacy	Universal 2nd Factor (U2F)	The FIDO U2F protocol enables relying parties to offer a strong cryptographic 2nd factor option for end user security. The relying party's dependence on passwords is reduced. The password can even be simplified to a 4-digit PIN.	FIDO U2F

Security and Privacy	Security Assertion Markup Language 4 (SAML)	This specification defines the syntax and semantics for XML-encoded assertions about authentication, attributes, and authorization, and for the protocols that convey this information.	SAML 4
Service Interoperability	Kerberos Network Authentication Service	This document describes the concepts and model upon which the Kerberos network authentication system is based. It also specifies Version 5 of the Kerberos protocol.	Kerberos Network Authentication Service
Service Interoperability	OAuth 2.0 authorization framework	The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.	OAuth 2.0 Framework
Service Interoperability	UAF	The FIDO UAF strong authentication framework enables online services and websites, whether on the open Internet or within enterprises, to transparently leverage native security features of end-user computing devices for strong user authentication and to reduce the problems associated with creating and remembering many online credentials. The FIDO UAF Reference Architecture describes the components, protocols, and interfaces that make up the FIDO UAF strong authentication ecosystem.	FIDO UAF
Security and Privacy	WS-Security Rights Expression Language (REL) Token Profile	This document describes how to use ISO/IEC 21000-5 Rights Expressions with the Web Services Security (WSS) specification. This document integrates specific error corrections or editorial changes to the preceding specification, within the scope of the Web Services Security and this TC. This document introduces a third digit in the numbering convention where the third digit represents a consolidation	WS-Security REL Token Profile

		of error corrections, bug fixes or editorial formatting changes (e.g. 1.1.1); it does not add any new features beyond those of the base specifications (e.g. 1.1).	
Security and Privacy	WS-Security Policy	This document indicates the policy assertions for use with [WS-Policy] which apply to WSS: SOAP Message Security [WSS10, WSS11], [WS-Trust] and [WS-Secure Conversation]. This document incorporates Approved Errata approved by the Technical Committee on 25 April 2012.	WS-Security Policy
Security and Privacy	WS-Trust	WS-Trust 1.4 defines extensions that build on [WS-Security] to provide a framework for requesting and issuing security tokens, and to broker trust relationships. This document incorporates errata approved by the Technical Committee on 25 April 2012.	WS-Trust
Security and Privacy	Secure Sockets Layer (SSL) Protocol	This document specifies version 3.0 of the Secure Sockets Layer (SSL 3.0) protocol, a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.	SSL Protocol
Security and Privacy	Transport Layer Security (TLS)	This memo describes how to use TLS to secure HTTP connections over the Internet. Current practice is to layer HTTP over SSL (the predecessor to TLS), distinguishing secured traffic from insecure traffic by the use of a different server port. This document documents that practice using TLS. A companion document describes a method for using HTTP/TLS over the same port as normal HTTP.	Transport Layer Security

<p>Security and Privacy</p>	<p>Florida Cybersecurity Standards (FCS).</p>	<p>This rule establishes cybersecurity standards for information technology (IT) resources. These standards are documented in Rules 74-2. State Agencies must comply with these standards in the management and operation of state IT resources. This rule is modeled after the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.</p>	<p>Florida Cybersecurity Standards</p>
<p>Security and Privacy</p>	<p>Health Information Portability and Accountability Act (HIPAA) Security Rule</p>	<p>Regulation developed by the U.S. Health and Human Services to protect the privacy and security of personal health information (PHI). (45 C.F.R. Subpart C, Part 164).</p>	<p>HIPAA Security Rule on Government Publishing Office</p>
<p>Security and Privacy</p>	<p>Federal Information Security Modernization Act (FISMA) of 2014</p>	<p>Establishes Secretary of Homeland Security as the responsible party to implement policies and practices to secure Federal Information Systems. (44 U.S.C. §2521)</p>	<p>FISMA 2014 on Government Publishing Office</p>
<p>Architecture, Analysis and Design Standards</p>	<p>National Institute of Standards and Technology Cybersecurity Framework for Critical Infrastructure</p>	<p>Voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risk. Developed in accordance with Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" and the Cybersecurity Enhancement Act of 2014 (15 U.S.C. §7421) to maintain efficient, innovative secure, and resilient Federal Information Systems.</p>	<p>NIST Cybersecurity Framework (CSF)</p>
<p>Security and Privacy</p>	<p>Florida Information Protection Act of 2014</p>	<p>A security law that requires covered entities to notify and disclose information breaches to Personally Identifiable Information (PII) of Florida Residents. (F.S. §501.171)</p>	<p>Florida Information Protection Act of 2014</p>
<p>Architecture, Analysis and Design Standards</p>	<p>Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS)</p>	<p>An open source standard that defines classification tiers, based on the communications and information patterns of the application, and provides lists of application security configurations and tests available to architects, designers, testers, and analysts. The controls defined within the framework enable a standardized evaluation of module application</p>	<p>OWASP 3.0 ASVS Landing Page</p>

		security and risk management related to application vulnerabilities.	
Data Standards	Data Encryption	Standards for the encryption and protection of information.	
Security and Privacy	Business Associate Agreement	Provisions constitute a business associate agreement for purposes of complying with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Is applicable if the Vendor is a business associate within the meaning of the Privacy and Security Regulations, 45 C.F.R. 160 and 164.	Business Associate Agreement
Security and Privacy	Sharing of PHI & PII	Any confidential personal identity information (PII) and individually identifiable health information (PHI) is not transported outside the United States in all vendor or their subcontractors' related business processes.	
Architecture, Analysis and Design Standards	SAMM (Software Assurance Maturity Model)	The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.	OWASP SAMM
Development	CWE (Common Weakness Enumeration)	CWE™ is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.	CWE
Security and Privacy	NVD (National Vulnerability Database)	The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes	NVD

		databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.	
Service Interoperability	Security Content Automation Protocol (SCAP)	The Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans. This publication, along with its annex (NIST Special Publication 800-126A) and a set of schemas, collectively define the technical composition of SCAP version 1.3 in terms of its component specifications, their interrelationships and interoperation, and the requirements for SCAP content.	SCAP
Testing	OWASP Testing Guide	This project's goal is to create a "best practices" web application penetration testing framework which users can implement in their own organizations and a "low level" web application penetration testing guide that describes how to find certain issues.	OWASP Testing Guide
Security and Privacy	National Institute of Standards and Technology (NIST) Initiatives	NIST has a variety of initiatives to address IT standards. Some of these initiatives include: <ul style="list-style-type: none"> · Computer Security · Cloud Computing · Biometrics · Data and Informatics · Health IT · Information Delivery 	NIST Initiatives
Service Interoperability	Accredited Standards Committee X12 (ASC X12)	ASC X12, chartered by the American National Standards Institute, develops and maintains Electronic Data Interchange (EDI) and Context Inspired Component Architecture (CICA) standards along with Extensible Markup Language	ASC X12

		(XML) schemas that drive business processes globally.	
Architecture, Analysis and Design Standards	Health Level 7 (HL7)	Health Level Seven International (HL7) is the global authority on standards for interoperability of health information technology with members in over 55 countries.	HL& Standards
Service Interoperability	National Council for Prescription Drug Programs (NCPDP)	National Council for Prescription Drug Programs (NCPDP) standards applies to ordering drugs from retail pharmacies. They standardize information between healthcare providers and pharmacies.	NCPDP Standards
Service Interoperability	National Information Exchange Model (NIEM)	This is a national program supported by the Federal Government that provides a community of users, tools, common terminology, governance, methodologies, and support that enablers enterprise-wide information exchange.	NIEM Standard
Architecture, Analysis and Design Standards	American Dental Association (ADA)	Works with others to develop and maintain the Code on Dental Procedures and Nomenclature (CDT)	ADA Nomenclature
Data Standards	National Committee on Vital and Health Statistics (NCVHS)	Acts as the public advisory body to Department of Health and Human Services (HHS) for health data and statistics. The NCVHS Standards Subcommittee focuses on healthcare standards.	NCVHS
Data Standards	Workgroup for Electronic Data Interchange (WEDI)	The Workgroup for Electronic Data Interchange (WEDI) is the leading authority on the use of Health IT to improve healthcare information exchange to enhance the quality of care, improve efficiency and to reduce costs of the American healthcare system.	WEDI
Data Standards	Dental Content Committee of the ADA (DeCC)	A committee of the ADA that sets standards for dental claim data content and maintains the Current Dental Terminology (CDT) Codes.	DeCC of the ADA

Data Standards	National Uniform Billing Committee (NUBC)	Formed in 1975 to develop and maintain a single billing form and standard data set to be used nationwide by institutional, private and public providers and payers for handling healthcare claims.	NUBC
Data Standards	National Uniform Claim Committee (NUCC)	Committee chaired by the American Medical Association (AMA) in partnership with CMS. Membership includes state and national level representatives from Medicaid (including CMS and National Association of Medicaid Directors (NAMD)) and public health representatives. Maintain the data set for the professional claim.	NUCC
Data Standards	American National Standards Institute (ANSI)	Serves as the U.S. member to the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), coordinating the U.S. position in the development of standards.	ANSI Standards
Data Standards	Organization for the Advancement of Structured Information Standards (OASIS)	Produces worldwide standards for security, Web services, XML conformance, business transactions, electronic publishing, topic maps, and interoperability within and between marketplaces.	OASIS
Data Standards	Office of the National Coordinator for Health Information Technology (ONC)	Federal entity responsible for the nationwide coordination efforts to implement and use state of the art health information technology. Charged with responsibility to coordinate electronic exchange of health information.	ONC
Data Standards	Public Health Data Standards Consortium (PHDSC)	Non-profit membership-based organization of federal, state and local health agencies; professional associations; academia; public and private sector organizations; international members; and individuals whose goal is to empower the healthcare and public health communities with health information technology standards to improve individual and community health.	PHDSC

Data Standards	Committee E31 on Healthcare Informatics (ASTM 31)	Develops standards related to the architecture, content, storage, security, confidentiality, functionality, and communication of information used within health care.	ASTM 31
Service Interoperability	Object Management Group (OMG)	The Object Management Group (OMG) is an international, open membership, not-for-profit technology standards consortium, founded in 1989. OMG standards are driven by vendors, end-users, academic institutions and government agencies. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries.	OMG Standards
Architecture, Analysis and Design Standards	Unified Modeling Language (UML) Profiles	This standard addresses business specific needs and technologies. The profiles include: Platform Independent Model (PIM), Platform Specific Model (PSM), CORBA Component Model (CCM), Enterprise Application Integration (EAI), Enterprise Distributed Object Computing (EDOC), Modeling Quality of Service (QoS) and Fault Tolerance Characteristics and Mechanisms, Schedule ability, Performance and Time	UML Profiles
Architecture, Analysis and Design Standards	Meta-Object Facility (MOF)	This standard provides an environment where models can export from one application, import into another, transport across a network, store in a repository and then stakeholders can retrieve and render it into different formats.	OMG Meta-Object Facility
Architecture, Analysis and Design Standards	Model Driven Architecture (MDA)	This standard unifies development from a PIM to a PSM. Object Management Group (OMG) MOF-enabled transformations are the basis of this standard.	OMG Model Driven Architecture
Architecture, Analysis and Design Standards	Business Process Definition Metamodel (BPDM)	This standard provides the ability to model business process with standard language and metadata.	OMG Business Process Definition Metamodel
Architecture, Analysis and	UML Enterprise Distributed Object	This standard simplifies development of component-based	OMG EDOC

Design Standards	Computing (EDOC)	systems using a modeling framework in UML.	
Architecture, Analysis and Design Standards	Web Ontology Language (OWL-S)	Applications that process content of information rather than presenting information to humans use this standard. It facilitates machine interpretability of web content.	Web Ontology Languages
Architecture, Analysis and Design Standards	Web Service Description Language (WSDL)	WSDL is an Extensible Markup Language (XML) format that describes services as endpoints. It abstractly describes the operations and messages bound by concrete protocols	WSDL
Architecture, Analysis and Design Standards	Universal Business Language (UBL)	UBL is a normative set of XML schema design rules and naming conventions that coincide with Electronic Business XML (ebXML) Core Components Technical Specifications	UBL
Architecture, Analysis and Design Standards	WS-Composite Application Models (WS-CAF)	WS-CAF defines a generic and open framework for applications containing multiple services.	OASIS
Architecture, Analysis and Design Standards	Representation State Transfer (REST) Architecture - Web Services	A RESTful web service (also called a RESTful web API) is a simple web service implemented using HTTP and the principles of REST. The REST Web is the subset of the WWW (based on HTTP) in which agents provide uniform interface semantics – essentially create, retrieve, update and delete – rather than arbitrary or application-specific interfaces, and manipulate resources only by the exchange of representations. Furthermore, the REST interactions are "stateless" in the sense that the meaning of a message does not depend on the state of the conversation.	REST Web Services
Architecture, Analysis and Design Standards	Web Services Modeling Ontology (WSMO)	WSMO describes aspects of a Semantic Web with four main elements: <ul style="list-style-type: none"> · Ontology's for terminology · Intention goals · Web service descriptions · Mediators 	WSMO

Architecture, Analysis and Design Standards	National Human Service Interoperability Architecture (NHSIA)	The National Human Services Interoperability Architecture (NHSIA) proposes a framework to facilitate information sharing, improve service delivery, prevent fraud, and provide better outcomes for children and families.	NHSIA
Service Interoperability	Extensible Markup Language (XML)	XML is a simple, flexible text format derived from Standard Generalized Markup Language (SGML). This standard provides a variety of associated standards, such as: <ul style="list-style-type: none"> · Associating Schemas · XQuery · Efficient XML Interchange · Extensible Stylesheet Language (XSL) Transformations (XSLT) – document transformation and presentation, XSL Formatting Objects (XSL-FO) and eXtended Memory Specification (XMS) Path Language 	XML
Service Interoperability	Simple Object Access Protocol (SOAP)	This is a protocol for the exchange of information. It does not define application semantics, but a simple mechanism for expressing application semantics.	W3C
Service Interoperability	SOAP with attachments-Message Transmission Optimization Mechanism (MTOM)	SOAP with attachments allows a message to contain attachments and provides rules for Uniform Resource Identifier (URI) references	SOAP
Service Interoperability	Universal Description, Discovery, and Integration (UDDI)	UDDI is a platform independent extensible markup language registry. Originally, proposed as a core web service standard, it interrogates SOAP messages to provide WSDL protocol bindings and message formats.	UDDI
Service Interoperability	Hypertext Transfer Protocol (HTTP)	Networking protocol for distributed, information systems. The Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) develop these standards. HTTP is a request-response protocol for client-server models.	HTTP

Service Interoperability	Hypertext Transfer Protocol – Secure (HTTPS)	HTTPS combines HTTP with Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol to provide encrypted communications and secure identification.	HTTPS
Service Interoperability	Web Services Description Language (WSDL)	This is a messaging standard in XML format for describing network services as endpoints. The messages are either document-oriented or procedure-oriented information. The messages bind to the concrete network protocol.	WSDL
Security and Privacy	Electronic Business XML (ebXML) Registry	This standard provides interoperable registries and repositories with an interface that enables submission, query, and retrieval.	ebXML
Service Interoperability	WS-Policy	The WS-Policy provides a general-purpose model and corresponding syntax to describe and communicate the policies of a web service. WS-Policy defines a base set of constructs used and extended by other web services specifications to describe a broad range of service requirements, preferences, and capabilities.	WS-Policy
Service Interoperability	WS-Agreement	Standards are at varying levels of maturity. Some standards are ready for use today, some are emerging, and others are in a stage referred to as “incubating.” The term incubating describes a standard that is developing convergence and may require 3 to 5 years before finalization and adoption.	WS-Agreement
Service Interoperability	WS-Addressing	This is a key element in the definition of a complete process flow. Middleware and service-delivery companies have an interest in this standard because it is one of the key elements for adding more resource definition information to the URI points. It currently consists of three major pieces: · Core · SOAP binding · WSDL binding with WSDL 2.0	WS-Addressing

Service Interoperability	WS-Reliability	WS-Reliability is a SOAP-based protocol for exchanging SOAP messages with guaranteed delivery, no duplicates, and guaranteed message ordering. WS-Reliability is SOAP message header extensions and is independent of the underlying protocol. It includes a binding to HTTP. The focus is on Business-to-Business (B2B) reliable message delivery. The specification borrows from previous work in messaging (e.g. ebXML) and transports and applies to WS services.	WS-Reliability
Service Interoperability	Structured Query Language (SQL)	A database computer declarative language designed for managing data in relational database management systems.	ANSI SQL
Service Interoperability	XML Schema	Other developers who are building their own special-purpose application use these sets of standard application elements.	W3C XML Schema
Service Interoperability	Service Level Agreement Language (SLAng)	SLAng records a common understanding about services, priorities, responsibilities, and other contractual items. The SLAng contains segments for address, service definitions, performance, problem management, customer duties, warranties, disaster recovery, and agreement termination. Specific examples include Web Service Level Agreement Language for Collaborations (WSLA+), Cloud Computing, and Backbone Internet providers.	SLAng
Service Interoperability	Web Service Distribution Management (WSDM)	WSDM is a web service standard for managing and monitoring the status of other services. It contains two specifications: <ul style="list-style-type: none"> · Management Using Web Services (MUWS) defines a basic set of manageability capabilities. · Management of Web Services (MOWS) defines how to manage web services as resources. 	WSDM
Service Interoperability	WS-Reliable Messaging (WSRM)	A protocol that allows reliable delivery of SOAP messages to	WSRM

		distributed applications.	
Service Interoperability	IT Infrastructure Library (ITIL) – IT Service Management Capabilities Level	This is an IT management standardization effort to understand and compare the IT resource utilization and to improve the effectiveness and efficiency of the infrastructure used.	ITIL
Service Interoperability	Distributed Management Task Force (DMTF)	DMTF worked on infrastructure management and has developed a series of standards that are gaining acceptance in the system management industry segment.	DMTF
Service Interoperability	Common Information Model (CIM)	CIM is an object-oriented model that describes the conceptual framework for describing management data. CIM messages are in XML format and over HTTP. CIM messages are well-defined request or response data packets used to exchange information between CIM products.	DMTF CIM
Security and Privacy	Federal Enterprise Architecture Security and Privacy Profile (FEA SPP)	FEA SPP is a scalable and repeatable methodology for addressing information security and privacy from a business-centric perspective. The documentation is at a high level. It does not replace other security and privacy standards but seeks to work across the enterprise.	FEA SPP
Security and Privacy	HIPAA Security and Privacy Rule	The HIPAA Privacy Rule establishes national standards to protect health information. It requires specific safeguards, establishes personal health information and sets limits and conditions on the disclosure of information.	HIPAA Security and Privacy Rule
Security and Privacy	WS-Security – WS-I Security Profile	The standard enhances the SOAP messaging to provide message integrity and confidentiality. This supports a variety of security models and encryption technologies. It provides a general approach of associating a security token allowing support for multiple token formats. It describes how to encode binary security tokens and describe the tokens associated with a message.	WS-I Security Profile

<p>Business Enabling Technologies</p>	<p>Business Process Model and Notation (BPMN) previously known as Business Process Modeling Notation Business Motivation Model (BMM)</p>	<p>The computer industry consolidated all Business Process Model (BPM) activities under Object Management Group (OMG). The BPMN is a standard for business process modeling that provides a graphical notation for specifying business processes. The BMM specification provides a scheme for developing, communicating, and managing business plans; while BPMN provides a formal mechanism that maps business process to appropriate execution format (BPM).</p>	<p>OMG BPMN and BMM</p>
<p>Business Enabling Technologies</p>	<p>Extensible Markup Language (XML) Forms (XForms)</p>	<p>XForms is an XML application that integrates into other markup languages. XForms gathers and processes XML data using an architecture that separates presentation, purpose, and content. XForms accommodates form component reuse, fosters strong data type validation, eliminates unnecessary round-trips to the server, and offers device independence.</p>	<p>XML Forms</p>
<p>Business Enabling Technologies</p>	<p>Rule Markup Language (RuleML) Initiative</p>	<p>This is an international non-profit organization covering all aspects of web rules and their interoperation. There are Structure and Technical Groups that focus on RuleML specifications, tools and application development.</p>	<p>RuleML</p>
<p>Business Enabling Technologies</p>	<p>Workflow Management Coalition (WfMC)</p>	<p>WfMC is a global organization that contributes to process related standards and educates users. Wf-XML and XPDL are leading process definition languages. The coalition also works to provide process simulation and optimization standards.</p>	<p>WfMC</p>
<p>Business Enabling Technologies</p>	<p>Customer Relationship Management (CRM) Extended Relationship Management (xRM)</p>	<p>xRM is the principle and practice of applying CRM and is a standardized interchangeable relationship for services.</p>	

Architecture, Analysis and Design Standards	Technical Document Naming Standards	The Technical Documentation Standards describe the standards that need to be adhered to for documenting Pages, Panels, Reports, etc.	FL MMIS Technical Document Naming Standards
Architecture, Analysis and Design Standards	AUTOSYS Design and Documentation Standards	MMIS Design and Documentation Standards for the AUTOSYS job scheduler.	FL MMIS AUTOSYS Design and Documentation Standards
Architecture, Analysis and Design Standards	Technical Design Documentation	Part of a developer’s processes and procedures for MMIS	FL MMIS Technical Design Documentation
Architecture, Analysis and Design Standards	C Programming Standards	MMIS document setting standards for developers	FL MMIS C Programming Standards
Architecture, Analysis and Design Standards	C Programming	A general-purpose, imperative computer programming language, supporting structured programming, lexical variable scope and recursion, while a static type system prevents many unintended operations.	C Programming
Architecture, Analysis and Design Standards	.NET Programming Standards	MMIS .Net Programming Standards	FL MMIS .Net Programming Standards
Architecture, Analysis and Design Standards	.NET Programming Standards	This is the .NET Programming Standards and guidelines.	.NET Programming Standards
Project Documentation	Defect Documentation Standards	Standards for documenting defects	FL MMIS Defect Tracking Standards
Service Interoperability	Integration Standards	Proposed integration standards being developed by AST will modify FS 74.5.	
Architecture, Analysis and Design Standards	. Net Framework Coding Standards	The purpose of this document is to identify net framework coding standards that should be followed for all .net applications that are developed by (IT) staff and augmented staff.	AHCA .NET Programming Standards

Architecture, Analysis and Design Standards	C# programming Standards	The purpose of this document is to provide coding style standards for the development of source code written in C sharp. Adhering to a coding style standard is an industry proven best practice for making team development more efficient and application maintenance more cost effective. These guidelines represent the minimum level of standardization expected in the source code of all projects written in C sharp.	C# Programming Standards
Architecture, Analysis and Design Standards	Application Patches Testing Standards	The purpose of this document is to provide a core set of standards and principles that can be used to maintain an effective patch/update test management program in a systematic way.	AHCA Application Testing Standards
Architecture, Analysis and Design Standards	Application Code Review and Promotion Procedures	The purpose of this document is to document the code review process for any application/reports/web service developed or maintained within AHCA. A code review consists of a review of an application’s design, functionality, connections, and code.	AHCA Code Review and Promotion Procedures
Architecture, Analysis and Design Standards	Web Forms Standards	The purpose of this document is to provide a guide that illustrates step by step instructions to create web forms.	Web Forms Standards
Architecture, Analysis and Design Standards	SQL Server Standards	The purpose of this document is to identify SQL coding standards that should be followed for all SQL applications that are developed by (IT) staff and augmented staff. Source code location and version information must be documented and maintained in Visual Studios T.F.S	AHCA SQL Server Standards
Architecture, Analysis and Design Standards	SharePoint Standards and Procedures	The purpose of this document is to ensure that the system is managed and used in accordance with the design and intent to avoid creating an unusable and unmanaged system.	AHCA SharePoint Standards
Architecture, Analysis and Design Standards	.Net Development Servers	The purpose of this document is to ensure all developers are aware that the old servers are now obsolete. All .net development servers have been	.NET Development Servers

		migrated to the cloud.	
Architecture, Analysis and Design Standards	CRM Standards and Procedures	The purpose of this document is to ensure that the system is managed and used in accordance with the design and intent to avoid creating an unusable and unmanageable system. This document should be read by all people that use, support, and enforce the system.	CRM Standards and Procedures
Architecture, Analysis and Design Standards	AHCA SSRS Report Writing Standards and Procedures	The purpose of this document is to ensure that the SSRS report writing process is managed in accordance with the vision's intent to avoid creating an unusable and manageable process while following Agency policy and development best practices.	AHCA SSRS Report Writing Standards
Architecture, Analysis and Design Standards	Name Checker	The Name Checker Utility is a tool which performs data name translation and data name compliance analysis. These two functions implement the CMS Data Administration Standards, Guidelines, and Operating Procedures as they apply to forming valid names of data entities, data attributes, database tables, and database columns. The tool employs the CMS Data Administration Glossary of Standard Terms and Abbreviations.	CMS Name Checker Utility
Service Interoperability	Simple Object Access Protocol (SOAP)	Soap Version 1.2 Framework	FL Rules SOAP
Service Interoperability	WS-Policy	The Web service specifications (WS*) are designed to be composed with each other to provide a rich set of tools for secure, reliable, and/or transacted Web services. WS-Policy by itself does not provide a negotiation solution for Web services. WS-Policy is a building block that is used in conjunction with other Web service and application-specific protocols to accommodate a wide variety of policy exchange models.	WS-Policy

Service Interoperability	WS-SecureConversation	This specification defines extensions to allow security context establishment and sharing, and session key derivation. This allows contexts to be established and potentially more efficient keys or new key material to be exchanged, thereby increasing the overall performance and security of the subsequent exchanges.	WS-SecureConversation
Service Interoperability	JavaScript Object Notation (JSON)	JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is easy for humans to read and write. It is easy for machines to parse and generate. It is based on a subset of the JavaScript Programming Language.	JSON
Service Interoperability	Hypertext Transfer Protocol (HTTP)	The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypertext information systems.	HTTP
Service Interoperability	Secure Shell (SSH) Transport Layer Protocol	The Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network. This document describes the SSH transport layer protocol, which typically runs on top of TCP/IP. The protocol can be used as a basis for secure network services. It provides strong encryption, server authentication, and integrity protection. It may also provide compression.	SSH Transport Layer Protocol
Service Interoperability	Domain Name System (DNS) Protocol	The goal of domain names is to provide a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internets, and administrative organizations.	DNS Protocol

<p>Service Interoperability</p>	<p>XML Configuration Access Protocol (XCAP)</p>	<p>This specification defines the Extensible Markup Language (XML) Configuration Access Protocol (XCAP). XCAP allows a client to read, write, and modify application configuration data stored in XML format on a server. XCAP maps XML document sub-trees and element attributes to HTTP URIs, so that these components can be directly accessed by HTTP.</p>	<p>XCAP</p>
<p>Architecture, Analysis and Design Standards</p>	<p>Uniform Resource Identifier (URI)</p>	<p>A Uniform Resource Identifier (URI) is a compact sequence of characters that identifies an abstract or physical resource. This specification defines the generic URI syntax and a process for resolving URI references that might be in relative form, along with guidelines and security considerations for the use of URIs on the Internet. The URI syntax defines a grammar that is a superset of all valid URIs, allowing an implementation to parse the common components of a URI reference without knowing the scheme-specific requirements of every possible identifier. This specification does not define a generative grammar for URIs; that task is performed by the individual specifications of each URI scheme.</p>	<p>URI Standard</p>
<p>Service Interoperability</p>	<p>Resource Description Format (RDF)</p>	<p>The Resource Description Framework (RDF) is a framework for representing information in the Web. RDF Concepts and Abstract Syntax defines an abstract syntax on which RDF is based, and which serves to link its concrete syntax to its formal semantics. It also includes discussion of design goals, key concepts, datatyping, character normalization and handling of URI references.</p>	<p>Resource Description Framework</p>

<p>Service Interoperability</p>	<p>Web Application Description Language (WADL)</p>	<p>This specification describes the Web Application Description Language (WADL). An increasing number of Web-based enterprises (Google, Yahoo, Amazon, Flickr to name but a few) are developing HTTP-based applications that provide programmatic access to their internal data. Typically, these applications are described using textual documentation that is sometimes supplemented with more formal specifications such as XML schema for XML-based data formats. WADL is designed to provide a machine process-able description of such HTTP-based Web applications.</p>	<p>WADL</p>
<p>Architecture, Analysis and Design Standards</p>	<p>Data Center Usage Agency Limitations</p>	<p>(5) AGENCY LIMITATIONS.— (a) Unless exempt from data center consolidation pursuant to this section or authorized by the Legislature or as provided in paragraph (b), a state agency may not: 1. Create a new agency computing facility or data center, or expand the capability to support additional computer equipment in an existing agency computing facility or data center; 2. Spend funds before the state agency's scheduled consolidation into the state data center to purchase or modify hardware or operations software that does not comply with standards established by the Agency for State Technology pursuant to s. 282.0051; 3. Transfer existing computer services to any data center other than the state data center; 4. Terminate services with the state data center without giving written notice of intent to terminate services 180 days before such termination; or 5. Initiate a new computer service except with the state data center.</p>	<p>Florida Statue 282.201</p>

APPENDIX C: INBOUND AND OUTBOUND INTERFACES

INBOUND INTERFACES FMMIS/DSS

<p>Agency for Health Care Administration</p> <p>Provider Rate file, Mandatory Assignment and enrollment data from AHS, Recipient HIV AIDS data, Recipient SMI data, Disease Management Recipient File, Updated capitation rates, Nursing Home rate file, Intermediate Care Facility rate file, Hospice rate file, Provider rate file, Provider DRG rate file, ASC rate file, KICK rate file, LEIE Monthly Updates</p>	<p>Electronic Data Interchange</p> <p>FHK 270/271 Match files with Reports, X12 837 5010 Claims institutional encounters, X12 837 5010 Claims dental encounters, X12 837 5010 Claims professional encounters, X12 837 5010 Claims institutional, X12 270 5010 Health Care Eligibility request, X12 276 5010 Claim Status request, X12 837 5010 Claims dental, X12 837 5010 Claims professional</p>	<p>Health Quality Assurance</p> <p>HQA License file update the Facility provider license information, HQA Modifier file match providers to valid license numbers, HQA Status Code file, HQA Address Type Codes, HQA Client Codes, HQA Ownership Codes, HQA modifier Codes</p>	<p>Centers for Medicare & Medicaid Services</p> <p>COBA response files from CMS, Medicare Part D data, EDB database of CMS-oriented recipients (Medicare A/B/D and Medicare Buy-In), Medicare Part A billing information, Medicare Part B billing information, Medicare Part D enrollment information, CMS (HCFA) file used to update CLIA table record types 1, 3 and 5, NCCI Interface Professional NCCI edits, NCCI Interface Hospital NCCI edits, MUE Interface Professional MUE edits, MUE Interface DME MUE edits, HCPCS Interface HCPCS procedure codes, ICD10 interface add/update ICD10 Diagnosis and Procedure codes</p>
<p>Automated Health Systems Provider Plan Network File</p>	<p>EQ Health</p> <p>Home Health Prior Authorization, Inpatient Prior Authorization, PPEC Prior Authorization, Professional Therapy Prior Authorization, Outpatient Therapy Prior Authorization, DME Prior Authorization, Dental Prior Authorization, Vision Prior Authorization, Hearing Prior Authorization, Physician Prior Authorization, Inpatient Psychiatric Prior Authorization, SIPP Inpatient Psychiatric Prior Authorization, Outpatient Prior Authorization</p>	<p>Magellan</p> <p>Prior authorization data for drug claims, Magellan sends contact information, Magellan sends adjudicated claims, Magellan Formulary coverage for drugs, Magellan State determined Maximum Allowable Cost (SMAC) drugs, Magellan Formulary Extract for Drug Rebate, Magellan SMAC Interface, Magellan Formulary drug termination date, UPC Interface used to add/update UPC codes</p>	<p>Department of Juvenile Justice – DJJ incarceration information</p>
<p>Agency for Persons with Disabilities APD Gatekeeper Prior Authorization</p>	<p>NPPES Monthly Master file, NPPES Monthly Deactivation file, NPPES Weekly Updates</p>	<p>Other Inbound Interfaces</p> <p>IRS CP2100 tape Provider B notice created Maximus data from Florida Healthy Kids Maximus Monthly MEC 834 Eligibility file FHK MEUPS PIN Letter file MFAO Physician Fee Schedule rate update MFAO DRG rate update SDX Resource file SSA data file System for Award Management Daily Updates Link Provider add members to Provider Group Wells Fargo Cleared Checks (interChange)</p>	<p>Department of Health</p> <p>DOH License File, Claims using external interface file from Healthy Start, Data files from Florida Bureau of Vital Statistics, DOH Immunization Registry</p>
<p>First Data Bank Update reference configuration data</p>	<p>TPL Vendor Resource file, TPL Vendor Manage adjustments, TPL Vendor Voided claims</p>		<p>Florida Department of Law Enforcement FDLE incarceration information, LiveScan input file</p>

OUTBOUND INTERFACES FMMIS/DSS

<p>Agency for Health Care Administration</p> <p>Drug claims paid for Prepaid Mental Health Plan recipients, Appropriations report generated out of the weekly financial cycle.</p>	<p>Centers for Medicare & Medicaid Services</p> <p>EDB Finder File listing of recipients, Medicare Part A accretions, deletions and demographic changes, Medicare Part B accretions, deletions and demographic changes, COBA monthly extract, Pharmacy Claims file for CMS MMA Plans</p>	<p>EQ Health</p> <p>Extract of professional claims, Extract of UB92 claims, Extract of dental claims, Extract of pharmacy claims, Extract of professional encounter claims, Extract of UB92 encounter claims, Extract of dental encounter claims, Extract of pharmacy encounter claims, Extract of recipient data, Home Health Prior Authorization, Inpatient Prior Authorization, PPEC Prior Authorization, Professional Therapy Prior Authorization, Outpatient Therapy Prior Authorization, DME Prior Authorization, Dental Prior Authorization, Vision Prior Authorization, Hearing Prior Authorization, Physician Prior Authorization, Inpatient Psychiatric Prior Authorization, SIPP Inpatient Psychiatric Prior Authorization, Outpatient Prior Authorization, Provider extract new providers/updates</p>	<p>HMS (TPL Vendor)</p> <p>Resource file from FMMIS/DSS, Carrier file from FMMIS/DSS, Recipient eligibility file from FMMIS/DSS, Lead letter data file from FMMIS/DSS, Pharmacy claims file from FMMIS/DSS, Provider Medicare to Medicaid cross-reference file, Provider file from FMMIS/DSS, Paid dental claims file from FMMIS/DSS, Drug code file from FMMIS/DSS, Procedure code file from FMMIS/DSS, Diagnosis code file, Institutional claim file, Physician claims file from FMMIS/DSS</p>	<p>SAS Extract of recipient data to SAS, Extract new providers or updates, Provider Owner SAS extract file</p> <p>Web Portal Provider Master Listing Extract, Pending Provider Listing Extract e</p>
<p>Automated Health Systems</p> <p>File for determining eligible recipients in reform counties, Recipient data to AHS Choice Counseling, Managed Care data to Enrollment Broker</p>	<p>Department of Children and Families</p> <p>Terminated SDX recipients extract, Recipient FLORIDA Update Error Report & FLORIDA Match Error Report, Carrier data for FLORIDA eligibility, Home Safe Net recipients</p>	<p>Providers/Managed Care Organizations</p> <p>X12 271 5010 Health Care Eligibility, Unsolicited X12 271 5010 HC Eligibility, X12 277 5010 Claim Status response, X12 277U 5010 response from Financial or Claims when information is missing, X12 835 5010 HC Claim Payment Advice, MCO capitations paid enrolled recipients, X12 999 5010 report errors or acknowledge error-free transaction set, X12 997 5010 report errors or acknowledge error-free transaction set</p>	<p>Magellan</p> <p>Recipient data for MMA/TPL information, Pharmacy Claim voids, Claim RetroDUR processing, HPE to Unisys Drug Claims Drug Rebate, HPE to Unisys Drug Extract Drug Rebate, HPE to Unisys Physician UB Claims Drug Rebate, Pharmacy Provider extract First Health 4 files - Address, Panel, On Review, NPI, Header and Trailer records to extract file FLM_PanelData.dat, Header and Trailer records to extract file FLM_PorData_Update.dat, License base and alias files, License address file, License specialty file, Provider License alias file updates</p>	<p>Other Outbound Interfaces</p> <p>MFAO - Provider Type '35' and Specialty '71', '72', '73', '74', '88' Conduent - Receive file from CMS (monthly) and send to TPL vendor CPS - ID Card extract DOH - Extract of HIV recipients DOT - Extract of recipient data First Health - Resource file Healthy Start MomCare Network - HS enrollment data of newly eligible Healthy Start recipients HPE Banking Dept. - Checks issued weekly financial cycle HPE LG Team - Recipient info used for 1095-B forms MCO's - Rosters to MCOs Maximus - Error response file Molina - Monthly Pharmacy Encounter Claim extract Tirion - Providers terminated lock access to web portal or providers need a pin letter or pin reset Unity One - Extract recipient data USF - Delta file SMMC MMA Managed Care recipients and SMMC plans all active MMA enrolled recipients</p>
<p>Agency for Person with Disabilities</p> <p>Extract for new providers or updates, DS Waiver Paid Claims for recipients care plans within APD Gatekeeper Matrix, DS Waiver Denied claims for recipients care plans within APD Gatekeeper Matrix, Weekly claim extract for all paid claims with S9122 TJ procedure code billed, Weekly claim extract for all voided claims with S9122 TJ procedure code billed, Gatekeeper Prior Authorization Interface, Gatekeeper Prior Authorization Summary Report, Gatekeeper Prior Authorization Transaction Listing Report, Interface for EQ Health PA with Procedure code S9122TJ</p>	<p>Department of Elder Affairs</p> <p>All DOEA recipients delimited data file, Monthly Capitation extract, Monthly MP enrollments active as of first of the next month</p>			
<p>Beacon Health</p> <p>Provider Extract for Beacon Extract of recipient data</p>	<p>Medtel</p> <p>Extract of recipient data to MEDTEL, Provider extract for Med_Tel Call Center, Active Providers for Med_Tel</p>			