Part III – Technical Architecture

Chapter 6 – Technology Standards

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

MITA
Medicaid Information Technology Architecture

Table of Contents

PART III – TECHNICAL ARCHITECTURE 1

Chapter 6 – Technology Standards 1

- Introduction 3
  - Purpose 3
  - Scope 3
- Technology Standards Reference Model 4
  - Key Elements of the Standards Reference Model 5
  - Applicable Standards 6
  - Service Delivery and Service Support 9
  - Technology Readiness and Maturity 10
  - Key Elements of the Technology Readiness and Maturity 12
- Technology Standards Reference Guide 12
  - Architecture, Analysis and Design Standards 13
  - Service Interoperability Standards 16
  - Security and Privacy Standards 20
  - Business Enabling Technologies 24
  - Data and Information Standards 26
- Using Technology Standards 28

List of Figures

Figure 6-1. Standards Reference Model 4

Figure 6-2. Technology Readiness and the MITA Maturity Model 11

Figure 6-3. Technology and Standards Put into Context 20

List of Tables

Table 6-1. Architecture, Analysis and Design Standards 13

Table 6-2. Service Interoperability Standards 16

Table 6-3. Security and Privacy Standards 21

Table 6-4. Business Enabling Technologies 25

Table 6-5. Data and Information Standards 26

Introduction

This chapter presents the standards associated with target technologies that support the goals of the Medicaid Enterprise. The technologies that support the Medicaid IT Architecture (MITA) Technical Architecture (TA) continue to mature. For example, the Information Technology (IT) Industry has used Service-Oriented Architecture (SOA) principles and methodologies long enough for baseline standards to emerge that support proven enterprise solutions. The focus of the TA Technology Standards is to leverage these proven solutions by adopting and adapting them for the State Medicaid Agency (SMA). The TA selects technologies and standards that meet the MITA Framework requirements, identifies the functional components that apply to the State Medicaid Enterprise, as well as any gaps in the standards, and tailors them as necessary into robust solution sets. An important part of the maturity of the MITA Framework is to analyze available technology standards at regular intervals to ensure that the solution sets advocated by MITA remain current.

The topics covered in this chapter include:

- Technology Standards Reference Model
- Technology Standards Reference Guide

Purpose

The use of standards supports the reuse of solutions and facilitates Commercial Off-the-Shelf (COTS) integration. Technology standards identify target technologies that support MITA goals. The primary focus is on selecting standard technologies that meet the MITA mission, goals, and objectives, and provide a solid foundation for the MITA Framework.

Scope

MITA technology standards are quite dynamic and require a periodic review of the available technologies and definitions. MITA Framework classifies technology standards into three categories:

- **Ready –** Technology that is ready to use.
- **Emerging –** Technology that fits the needs of MITA over the next year.
- **Incubating –** Technology that is on a watch list as being nearly ready.

The emerging technologies and processes that have the most significant impact are those involved with creating and enabling the definition of a SOA and the creation of distributed components.

Many of the technologies recommended in the standards are mature in the IT Industry, but may be unfamiliar to the Medicaid community. The preference is to select open standards supported by two (2) or more vendors. Other criteria for selection are interoperability and data management features based on open standards and leveraged with similar initiatives within other federal and state government agencies.

Critical technologies to watch over in the near future include the maturing Security and Privacy (S&P), model-driven architecture, and implementation technologies. These technologies allow the full implementation of system model, configuration management, and dynamic configuration control of distributed services.

Technology Standards Reference Model

The Standards Reference Model (SRM) is a framework that identifies technical services. **Figure 6-1** shows the SRM, consisting of technical services shown as a series of horizontal layers and vertical slices. The horizontal layers represent six (6) separate areas of technology standards and evolving technology: user interface, message exchange, metadata repository, message transmission, data and information, and communication.

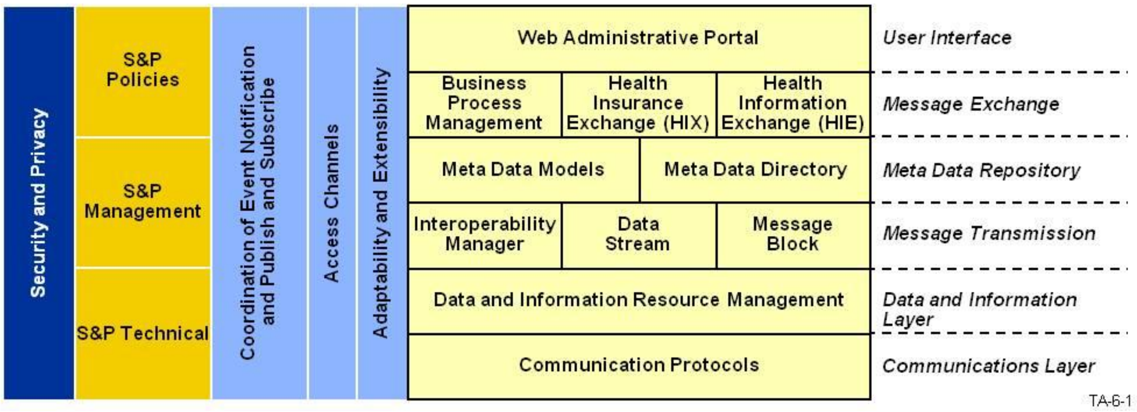

Figure 6-1. Standards Reference Model

The four (4) vertical slices of the SRM shown in **Figure 6-1** are:

1. S&P services that include policy, management, and technical service elements.
2. Coordination of event notification and publish-and-subscribe.
3. Access channels.
4. Adaptability and extensibility services that operate with each of the layers to design and manage changes in a consistent manner.

The SRM provides the structure for categorizing the technology standards. It provides information about each standard that a state can use in its procurement specifications. The MITA team refines the SRM based on feedback from States and the vendor community. It selects standards for their strong focus on service integration that cross interstate and intrastate boundaries. These criteria encourage interfaces and data sharing standards that are consistent with the Nationwide Health Information Network (NwHIN).

The SRM provides an overview of the current taxonomy of standards and how they relate to different solution sets.

Key Elements of the Standards Reference Model

The six (6) layers in the SRM are as follows:

1. **User Interface** – Standards for user interaction with Medicaid systems that use a wide range of devices including desktops, laptops, tablets, smartphones, mobile phones, and others.
2. **Message Exchange** – Standards for message content exchanged between applications, including messages between and within Medicaid business processes, health clinical data, and health administration data.
3. **Metadata Repository Management** – Standards for metadata interchange among data warehousing, business intelligence, and portal applications that provide a common basis for meta models that bridge gaps between dissimilar meta models. Two (2) sets of standards exist in this layer: metadata models and metadata directory. Metadata management services find, access, and create virtual queries that span organization boundaries and support translations from two (2) aligned but different syntaxes using metadata transformation tools.
4. **Message Transmission** – Standards for message routing based on logical need. These standards use communication layer protocols for message transport over communications links and networks. The Electronic Data Interchange (EDI) Gateway and the Enterprise Service Bus (ESB) are primary elements within this level. It is vital to follow standards to ensure that service-oriented message delivery with World Wide Web Consortium (W3C) Extensible Markup Language (XML) capabilities are part of the external exchange between ESB and that the EDI Gateway is where the transmitting organization handles translation.
5. **Data and Information Resource Management Layer** – Standards through data management and services that can access structured data using the Structured Query Language (SQL), semi-structured data using XML-based queries (e.g., W3C XQuery), and unstructured data using content management and search tools that understand W3C Hypertext Markup Language (HTML) and the Dublin Core Metadata Initiative (DCMI).
6. **Communications Layer** – Standards for communications protocols used at the lowest four (4) layers defined in the Open Systems Interconnection (OSI) model (i.e., the physical, data link, network, and transport layers).

In addition to the standards of the six (6) layers described above, the reference model describes standards for four (4) additional areas that span multiple SRM layers:

- **S&P –** Provide a level of consistency focused on the tactical sharing of data.
- **Coordination of Event Notification and Publish-and-Subscribe** – Support information sharing and change management with process automation functions. They support an event-driven architecture for information exchange and service requests consistently within and across state boundaries.
- **Access Channels** – Enable transparent access among applications and between users of applications. Varieties of devices (e.g., tablets, smartphones, and Wi-Fi routers) interface with applications through special device managers.

- ❖ **Adaptability and Extensibility** – Define standards with technical features and parameters that change within each of the layers. Adaptability and extensibility allow the management of technological changes in an orderly manner.

Applicable Standards

This section presents currently defined standards for the technical services and capabilities.

USER INTERFACE LAYER STANDARDS

Web Administrative Portal – Focuses on the tools needed to adapt and manage the shared services. Tactical and strategic data access provides tools and manages control within limits set by the governance process. The Organization for the Advancement of Structured Information Standards (OASIS) Web Services for Remote Portlets (WSRP) standard is the basis of the portal. The operational and the administrative portals follow the same basic standards.

MESSAGE EXCHANGE LAYER STANDARDS

Business Process Management Standards – Used within the process automation service, enables the addition of new business areas or provides the ability to compose processes and link to COTS capabilities. Human interaction extension directs an Object Management Group (OMG) Unified Modeling Language (UML) model to a Web Services-Business Process Execution Language (WS-BPEL) to address workflow and business process automation. An alternative to the UML standard notation is the OMG Business Process Model and Notation (BPMN) Version 2.0 (previously known as Business Process Modeling Notation).

Clinical Health Exchange – Involves Health Level Seven International (HL7) standards for interoperability of health information technology and handles classes of event-based HL7 messages.

Health Administration Exchange – Includes Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related privacy services, as discussed in the HIPAA Exchange and Related Attachments.

METADATA REPOSITORY LAYER STANDARDS

Federated Data Management Engine – A registry or repository that creates virtual models and maps between data sets that States, providers, or federal agencies own and agree to share based on an access-control agreement. The federated component is a small central core of the virtual model or virtual schema that links to the related data elements. Stakeholders use it for short-term, focused problems as a transition strategy to tactical or strategic shared data. It also enables drill down to data from a subject-specific data mart. An International Organization for Standardization (ISO) XML-Related Specifications (XML/SQL) interface provides virtual data access.

Metadata – Data that provides one or more aspects of data. It integrates specific metadata elements of OMG Meta-Object Facility (MOF) Version 2.0 and Web Service (WS) Metadata Exchange, coupled with W3C XML Schemas.

MESSAGE TRANSMISSION LAYER STANDARDS

Interoperability Manager – Provides the management of new interfaces as stakeholders create new NwHIN gateways. Focus is on creating business agreements between organizations at the policy level, establishing specific information exchanges, and specific, permissible, fine-grained queries. This function manages the business interface agreements (e.g., formats, and security), monitors for compliance, and provides failover and recovery and flow management. The Interoperability Manager originates from OASIS Messaging Electronic Business XML (ebXML) and emerging business-centric interface management methodology. It uses channels and Endpoint Reference (EPR) based on W3C Web Services Addressing (WS-Addressing) and W3C Web Services Choreography Description Language (WS-CDL).

Data Stream – Reflects the use of XML-based protocol standards that cover message headers, enables the routing of messages to the right location based on logical need, and maps between logical and physical need based on the type of message received. Smart telecommunication switches and topic-based virtual communication channels are a key element of the Interface Integration Interoperability layer. It takes into account event-based detection and filtering, such as W3C Web Services Eventing (WS-Eventing) and OASIS WS Notification (WSN).

W3C Simple Object Access Protocol (SOAP) Message Exchange Patterns (MEP) – A set of message exchange enablers for SOAP 1.2 is operational. The MITA team considers new performance-enhanced forms of SOAP MEP based on standards enhancements such as Brief Treatment Outcomes Measure (BTOM) and other performance-based standards enhancements. The originating agent signs, selectively encrypts the messages, and ensures all messages have a label to designate the owner and the S&P policies.

SECURITY AND PRIVACY STANDARDS

S&P standards address policies, management procedures, and technical services that cover technical functions (e.g., authentication and authorization) and ensure the enforcement of security policies between services.

Typical S&P technical services include, but are not limited to, the following:

- **Authentication** - To verify the identity of a user, device, or other entity in a computer system positively, usually as a prerequisite to allow access to resources in a system.
- **Authorization –** To determine if a user has a specified access type to a system resource by evaluating applicable access control information. Usually, authorization is in the context of authentication. When the system authenticates a user, it grants authorization to perform different types of access.
- **Auditing -** A service that reliably and securely records security-related events producing an audit trail enabling the reconstruction and examination of a sequence of events. Security events could include authentication events, policy enforcement decisions, and others. Authorized users can access the resulting audit trail to confirm compliance with policy, deter abuse, detect attacks, or other purposes.
- **Credentialing** – Transferring data to establish a claimed principal identity.

- **Encryption -** The process of transforming meaningful information (cleartext) into coded language (ciphertext). Encryption transforms personal information into an unrecognizable string of characters, ensuring privacy of information before transmission over the Internet.
- **Provisioning** - Provides end-to-end identity management services for centralized user administration, password synchronization, password strength control, and web browser based self-service capabilities. Typical built in features are interoperability with metadirectory services and an open technical design to support integration with other components such as web access-control products.

COORDINATION OF EVENT NOTIFICATION AND PUBLISH-AND-SUBSCRIBE STANDARDS

These standards leverage the OASIS Web Services Notification (WSN) family of specifications that define standard interoperable protocols through which the WS disseminates as events. The WSN family includes the following:

- **Web Services Base Notification (WS-BaseNotification) Standard** - Defines the WS interfaces for notification producers and notification consumers. It includes standard message exchanges that service providers implement and the operational requirements expect. The other WSN specification documents depend on this base document.
- **Web Services Topics (WS-Topics) Standard** - Defines a mechanism to organize and categorize items of interest for subscriptions (known as topics). WS-BaseNotification specification combines the topics with the notification mechanism. WS-Topics specify an XML model for describing metadata associated with topics and defines topic expression dialects.
- **Web Services Brokered Notification (WS-BrokeredNotification) Standard** - Defines the WS interfaces for notification brokers. A notification broker is an intermediary that allows publication of messages from entities that are not service providers (e.g., service gateways, and information hub). It includes standard message exchanges service providers may implement along with operational requirements expected of service providers and requestors that participate in brokered notifications.

The ESB provides the service-oriented infrastructure to address request and response style messages in addition to event-based message exchanges.

ACCESS CHANNEL STANDARDS

Smartphones and web portals are two major types of access mechanisms. Smartphones use a web browser that is compliant with W3C eXtensible Hypertext Markup Language (XHTML) and W3C Cascading Style Sheets 2 (CSS2) specifications. Access channel standards include Infrared Data Association (IrDA), along with Transmission Control Protocol/Internet Protocol (TCP/IP), and Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPsec), and Secure Shell (SSH). The industry defines other access channels as others identify the needs.

ADAPTABILITY AND EXTENSIBILITY STANDARDS

TA identifies three (3) levels of standards:

1. Standards that involve defining user needs and the variety of elements that the users access. These include services the user needs to perform a task and the related message exchanges, transmissions, and permitted message-exchange patterns. Only research and proprietary activities comprise service management models. The standards use the OASIS Web Services Coordination (WS-Coordination) and Distributed Management Task Force (DMTF) Web Services for Management (WS-Management) protocols in a selective manner.
2. Standards such as the OASIS Web Services Distributed Management (WSDM) and changes within enterprise management address service orientation. The managed service environment responds to changes in user needs and preferences, support the evolution of services in phased sets of service collations or epochs, and react to the addition, deletion, or temporary changes of resources.
3. MITA Framework integrates Resource management into the OASIS WS-Resource Framework (WSRF). The standards define service groups and their directory, a standard method of defining the properties of WS resources, their lifetime management, and their ability to handle faults in a consistent manner. The WSN defined under the Coordination or Reliable Messaging, Event-Notification, and Publish-and-Subscribe standards identifies and brokers changes to appropriate service groups.

Service Delivery and Service Support

Similar IT Service Management capabilities complement the SRM to address the service delivery and service support functions. The MITA Framework addresses IT services from both the service provider and service client perspective. Many Medicaid providers work in multiple States and expect similar services and interactions. Beneficiaries who move from state to state or into different systems within the same state expect the same service. MITA Framework defines IT Service Management requirements for quality, service delivery, and support service based on emerging standards such as ITSqc eSourcing Capabilities Model for Service Providers (eSCM-SP), ITSqc eSourcing Capability Model for Client Organizations (eSCM-CL), and other best practices for IT Service Management.

Service delivery covers the processes required for the planning and delivery of quality IT services and longer term processes associated with improving the quality of delivered IT services. The State Medicaid Enterprise should address and support Service delivery in the following areas:

- Service Level Management (SLM) negotiates documents, agrees to, and reviews business service requirements and targets within service level requirements and agreements. These pertain to the measurement, reporting, and reviewing of the quality of services IT delivers to the business. The SLM process also negotiates and agrees to support targets contained in operational level agreements with the support team.
- Capacity Management processes ensure that adequate capacity is available at all times to meet the requirements of the business by balancing business demand with IT supply. Capacity plan connects closely to the business strategy and includes application sizing and modeling, as well as performance, workload, and demand management.

- IT Service Continuity Management produces recovery plans designed to ensure that IT services continue at an agreed level and within an agreed schedule following any major incident that disrupts or might disrupt service. It is a component of a business continuity planning process.
- Financial Management for IT Services provides the basis for running IT as a business within a business and for developing a cost-conscious and cost-effective organization.
- Availability Management is responsible for ensuring that services meet or exceed their availability targets and proactively improves on an ongoing basis.

Service support describes the processes associated with providing IT services, especially in the following areas:

- Configuration Management is the foundation for successful IT Service Management and supports every other process.
- Problem Management minimizes adverse impacts from incidents and problems in the business, assists incident management, and seeks to prevent incidents and problems.
- Change Management supports the efficient and effective management of changes through the complete system development life cycle. It focuses on the forward scheduling of changes throughout the organization based on business impact and urgency.
- Service Desk provides a single, central point of contact for all IT users in an organization and handles all incidents, queries, and requests. It provides an interface for all other service-support processes.
- Release Management takes a holistic view of changes to IT services, considering all technical and nontechnical aspects of release planning.
- Incident Management manages all incidents, from detection and recording through resolution and closure. Incident management seeks to restore normal services as soon as possible and with minimal disruption to the business.

Technology Readiness and Maturity

As shown in **Figure 6-2** below, technology readiness and the MITA Maturity Model (MMM) provide an invaluable resource for the SMA to use in planning and coordinating its technology acquisition to foster innovations during a long procurement cycle. Technology readiness operates in tandem with the annual technology review.

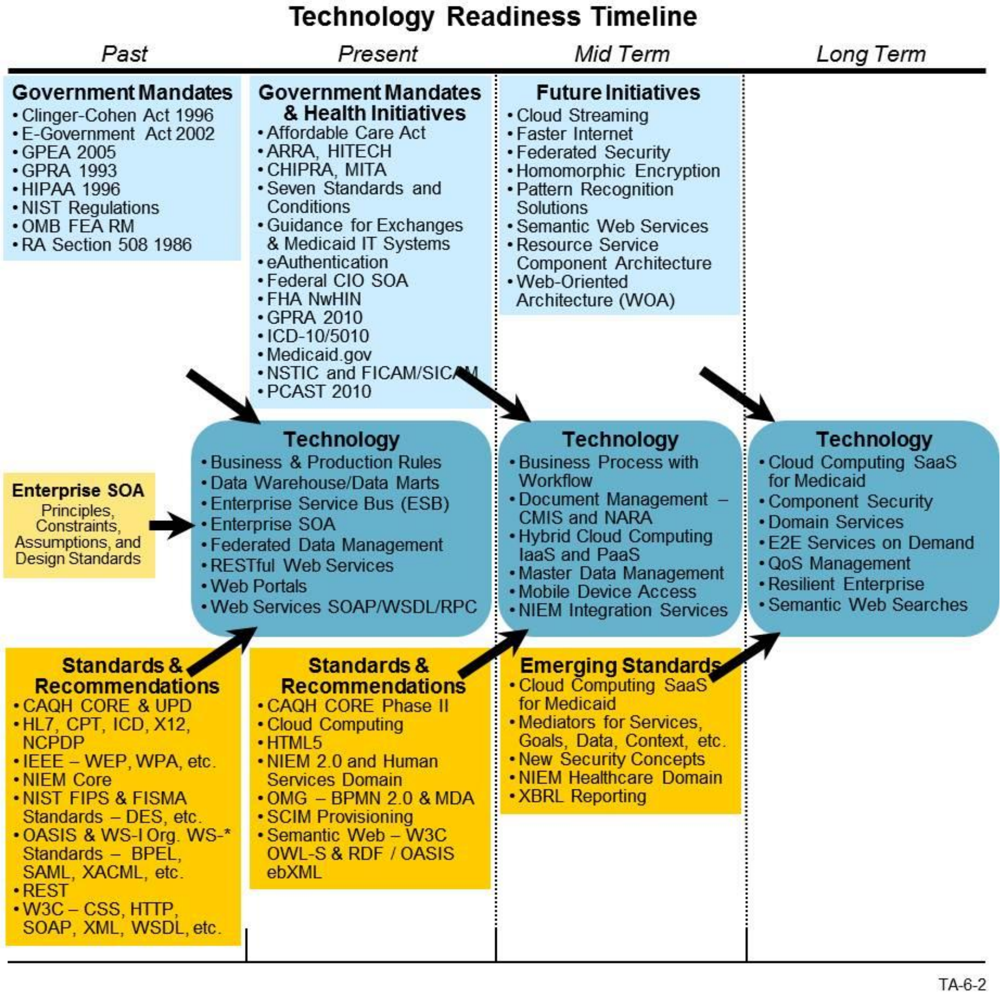
Technology Readiness Timeline
Past
Present
Mid Term
Long Term
Government Mandates
• Clinger-Cohen Act 1996
• E-Government Act 2002
• GPEA 2005
• GPRA 1993
• HIPAA 1996
• NIST Regulations
• OMB FEA RM
• RA Section 508 1986
Government Mandates & Health Initiatives
• Affordable Care Act
• ARRA, HITECH
• CHIPRA, MITA
• Seven Standards and Conditions
• Guidance for Exchanges & Medicaid IT Systems
• eAuthentication
• Federal CIO SOA
• FHA NwHIN
• GPRA 2010
• ICD-10/5010
• Medicaid.gov
• NSTIC and FICAM/SICAM
• PCAST 2010
Future Initiatives
• Cloud Streaming
• Faster Internet
• Federated Security
• Homomorphic Encryption
• Pattern Recognition Solutions
• Semantic Web Services
• Resource Service Component Architecture
• Web-Oriented Architecture (WOA)
Enterprise SOA
Principles, Constraints, Assumptions, and Design Standards
Technology
• Business & Production Rules
• Data Warehouse/Data Marts
• Enterprise Service Bus (ESB)
• Enterprise SOA
• Federated Data Management
• RESTful Web Services
• Web Portals
• Web Services SOAP/WSDL/RPC
Technology
• Business Process with Workflow
• Document Management – CMIS and NARA
• Hybrid Cloud Computing IaaS and PaaS
• Master Data Management
• Mobile Device Access
• NIEM Integration Services
Technology
• Cloud Computing SaaS for Medicaid
• Component Security
• Domain Services
• E2E Services on Demand
• QoS Management
• Resilient Enterprise
• Semantic Web Searches
Standards & Recommendations
• CAQH CORE & UPD
• HL7, CPT, ICD, X12, NCPDP
• IEEE – WEP, WPA, etc.
• NIEM Core
• NIST FIPS & FISMA Standards – DES, etc.
• OASIS & WS-I Org. WS-* Standards – BPEL, SAML, XACML, etc.
• REST
• W3C – CSS, HTTP, SOAP, XML, WSDL, etc.
Standards & Recommendations
• CAQH CORE Phase II
• Cloud Computing
• HTML5
• NIEM 2.0 and Human Services Domain
• OMG – BPMN 2.0 & MDA
• SCIM Provisioning
• Semantic Web – W3C OWL-S & RDF / OASIS ebXML
Emerging Standards
• Cloud Computing SaaS for Medicaid
• Mediators for Services, Goals, Data, Context, etc.
• New Security Concepts
• NIEM Healthcare Domain
• XBRL Reporting
TA-6-2

Figure 6-2. Technology Readiness and the MITA Maturity Model

Note: Government mandates, industry standards, and recommendations that are in place continue to influence the Medicaid Enterprise and are subject to modifications going forward. Unless indicated otherwise assume that mandates, standards, and recommendations listed in the past continue in the present and may potentially carry over into the future.

A principal purpose of technology management is to understand the maturity of a state's current technology and the business value of new and emerging technologies to improve benefits. Technology drivers (e.g., government mandates and initiatives) follow overall guiding principles and assumptions and identify mature technologies or emerging and new technologies.

Key Elements of the Technology Readiness and Maturity

The SRM and related analyses identify key drivers, including government mandates (e.g., federal health initiatives, Regional Health Information Organizations (RHIOs), NwHIN, and other government initiatives). The purpose of the SRM is to identify technologies that are ready and emerging. Emerging technologies and processes that have significant impact are those involved with creating and enabling the definition of a SOA and the creation of distributed components. The MITA Framework selects technologies with open standards and basis interoperability and data management features on open standards. It leverages similar initiatives within other government agencies. Fundamental technologies to watch in the near future include maturing S&P, model-driven architecture and implementation technologies that allow the full implementation of the system model, configuration management, and dynamic configuration control of distributed services.

Technology Standards Reference Guide

This section provides the technology standards used by the MITA TA. The organization of the Technology Standards Reference Guide (TSRG) reflects the need for periodic updates. The MITA Framework organizes architecture, analysis, and design standards around technical areas with an additional section devoted to standards about architecture. Additionally, there are both medical information and Medicaid-specific groups of standards. As the Health Care Industry identifies relevant standards, the MITA team adds or updates them in the TSRG.

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.

A TSRG is a collection of standards applicable to the administration and operation of a State Medicaid Enterprise. Previously, the MITA Framework presented a series of tables as part of the TSRG; however, the MITA team modified the style to include a minimal number of fields and an internet resource for the SMA to evaluate. Each standard consists of the following attributes:

- **Standard Name –** The official title of the specification.
- **Objective** - A brief description of the standard.
- **Source –** The internet address for the standards organization or related website.

There are four (4) categories of standards:

- **Architecture, Analysis and Design Standards** – Generally accepted industry standards and specifications for the planning, analysis, and design of a State Medicaid Enterprise's architecture.

- **Service Interoperability** – Generally accepted industry standards and specifications for web service standards across platforms, operating systems, and programming languages.
- **Security and Privacy** – Generally accepted industry standards and specifications for securing information.
- **Business Enabling Technologies** - Generally accepted standards and specifications for process management involving definition, improvement, and innovation of business processes.

Three (3) prominent standards groups provide a majority of the standards:

- **Object Management Group (OMG)** – A worldwide, open membership, not-for-profit consortium organized in 1989.
- **World Wide Web Consortium (W3C)** – An international community of member organizations and the public work together to develop web standards.
- **Organization for the Advancement of Structured Information Standards (OASIS)** – A not-for-profit consortium that develops and encourages the adoption of open standards.

Architecture, Analysis and Design Standards

Table 6-1 provides a listing of generally accepted standards and specifications for the planning, analysis, and design of the State Medicaid Enterprise architecture.

Note: A third party maintains the internet address for a resource, which may change over time.

Table 6-1. Architecture, Analysis and Design Standards

Architecture, Analysis and Design Standards		
Standard Name	***Objective***	***Source***
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	www.uml.org/#UMLProfiles

Architecture, Analysis and Design Standards		
Standard Name	***Objective***	***Source***
	- System on a Chip (SoC) - Systems Engineering (SysML) - Testing Profile	
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. (We do not restrict these functions to structural models, or to models defined in UML.)	www.omg.org/mof/
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.	www.omg.org/mof/
Business Process Definition Metamodel (BPDM)	This standard provides the ability to model business process with standard language and metadata.	www.omg.org/
UML Enterprise Distributed Object Computing (EDOC)	This standard simplifies development of component-based systems using a modeling framework in UML. There are seven specifications within EDOC: - Enterprise Collaboration Architecture (ECA) - Metamodel and UML Profile for Java(JB) - Flow Composition Model (FCM) - UML Profile for Patterns - UML Profile for ECA - UML Profile for Meta Object Facility - UML Profile for Relationships	www.omg.org/
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.	www.w3.org/TR/owl-features/
Web Service Definition 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	www.w3.org/TR/wsdl

Architecture, Analysis and Design Standards		
Standard Name	***Objective***	***Source***
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	www.oasis-open.org/
WS-Composite Application Models (WS-CAF)*	WS-CAF defines a generic and open framework for applications containing multiple services.	www.oasis-open.org/
Web Application and Compound Document*	This standard is under development and addresses client-side web applications. The standards will focus on: • Hosting environments • Declarative versus script web applications • User interface controls • Parsing data over the network	www.oasis-open.org/
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.	www.w3.org/TR/ws-arch
Web Services Modeling Ontology (WSMO)*	WSMO describes aspects of a Semantic Web with four main elements: • Ontology’s for terminology • Intention goals • Web service descriptions • Mediators	www.w3.org/
National Human Service Interoperability Architecture (NHSIA)*	For a number of years, the HHS Administration for Children and Families (ACF) has been working with others to create a conceptual Human Services Information Architecture (HSIA) to produce a technology framework and standards that would result in shared components and shared services	www.acf.hhs.gov

Architecture, Analysis and Design Standards		
Standard Name	***Objective***	***Source***
	among state human service program systems. The goal is to create an environment and infrastructure that would match state and federal data for ACF and the Johns Hopkins University to leverage past development of various federal and state programs, including MITA, National Information Exchange Model (NIEM), Global Reference Architecture (GRA), Service-Oriented Architecture (SOA), and cloud computing.	

***Note:** This item is not an official standard or standards organization.

Service Interoperability Standards

There are several standards groups involved in web service security and service interoperability including, but not limited to, the Institute of Electrical and Electronic Engineers (IEEE), the National Institute of Standards and Technology (NIST), OASIS, W3C, and the OASIS Web Services Interoperability Organization (WS-I). The following two (2) tables provide information pertaining to these standards groups. **Table 6-2** provides a listing of generally accepted Service Interoperability Standards that the SMA can use.

Note: A third party maintains the internet address for a resource, which may change over time.

Table 6-2. Service Interoperability Standards

Service Interoperability Standards		
Standard Name	***Objective***	***Source***
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: • 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	www.w3.org

Service Interoperability Standards		
Standard Name	***Objective***	***Source***
	(XPath)	
Simple Object Access Protocol (SOAP) **SOAP with attachments- Message Transmission Optimization Mechanism (MTOM)**	This is a protocol for the exchange of information. It does not define application semantics, but a simple mechanism for expressing application semantics. SOAP with attachments allows a message to contain attachments and provides rules for Uniform Resource Identifier (URI) references	www.w3.org
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.	www.oasis-open.org
Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol – Secure (HTTPS)	These standards are networking protocol for distributed, collaborative, hypermedia information systems. The Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) develop and coordinate these standards. HTTP is a request-response protocol for client-server models – web browsers. HTTPS combines HTTP with Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol to provide encrypted communications and secure identification.	www.ietf.org www.w3.org
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.	www.w3.org
Electronic Business XML (ebXML) Registry	This standard provides interoperable registries and repositories with an interface that enables submission, query, and retrieval.	www.oasis-open.org
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,	www.w3.org

Service Interoperability Standards		
Standard Name	***Objective***	***Source***
	and capabilities.	
WS-Agreement	Standards are at varying levels of maturity. Some standards are ready for use today, some are emerging, and others are in a stagereferred to as “incubating.” The term incubating describes a standard that is developing convergence and may require 3 to 5 years before finalization and adoption.	Grid Resource Allocation Agreement Protocol (GRAAP) WG forge.gridforum.org/sf/projects/graap-wg
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	www.w3.org
WS-Reliability	WS-Reliability is a SOAP-based protocol for exchanging SOAP messages with guaranteed delivery, no duplicates, and guaranteed message ordering. WS-Reliability are 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 transport and applies to WS services.	www.w3.org
Defense Advanced Research Projects Agency (DARPA) Agent Markup Language (DAML-S)	DAML-S is a semantic markup language; however, Web Ontology Language (OWL-S) supersedes it.	www.w3.org/Submission/OWL-S/
Structured Query Language (SQL)	A database computer declarative language designed for managing data in relational database management systems.	www.ansi.org
XML Schema	Other developers who are building their own special-purpose application use these sets of standard application elements.	www.w3.org

Service Interoperability Standards		
Standard Name	***Objective***	***Source***
	Standard XML Applications consist of the following: • XSL • XSLT • XSL-FO • XML Schema	
Service Level Arrangement 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.	ieeexplore.ieee.org
Web Service Distribution Management (WSDM)	WSDM is a web service standard for managing and monitoring the status of other services. It contains two specifications: • 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.	www.oasis-open.org
WS-Reliable Messaging (WSRM)	A protocol that allows reliably delivery of SOAP messages to distributed applications.	www.oasis-open.org
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 addressing in order to improve the effectiveness and efficiency of the infrastructure used.	www.itil-officialsite.com
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.	www.dmtf.org
Common Information	CIM is an object-oriented model that describes the conceptual framework for describing	www.dmtf.org

Service Interoperability Standards		
Standard Name	***Objective***	***Source***
Model (CIM)	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.	

Security and Privacy Standards

Figure 6-3 is a taxonomy of security standards and their relationship to front-end technology.

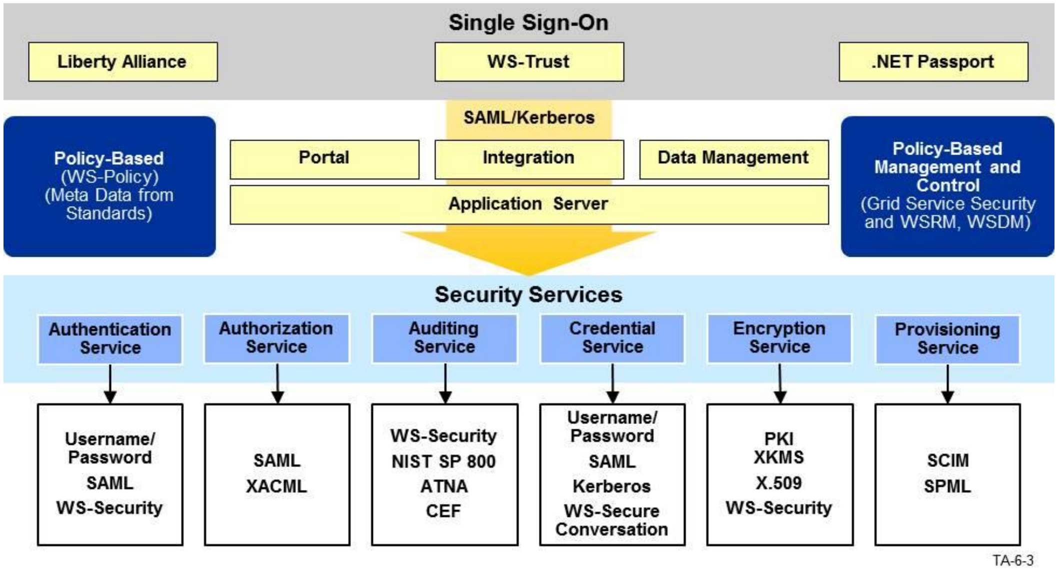

Figure 6-3. Technology and Standards Put into Context

As indicated in the Technology Readiness and the MITA Maturity Model (**Figure 6-2**), a current government initiative is to implement identity, credentialing, and access management architectures for both state and federal government entities. The White House recently published the *National Strategy for Trusted Identities in Cyberspace, Creating Options for Enhanced Online Security and Privacy (NSTIC)* in recognition of the rising cyber security risks due to increased online transactions. The broad vision of the strategy is for individuals and organizations to utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. The Department of Health and Human Services (HHS) is also developing credentialing guidelines, and the Health Information Technology for Economic and Clinical Health (HITECH) Act is driving them to promote the adoption and meaningful use of health information technology.

The NASCIO State Digital Identity Working Group is taking the lead to produce a State Identity, Credential, and Access Management (SICAM) Roadmap and Implementation Guideline, a document that follows the path that the Federal Identity, Credential, and Access Management (FICAM) established for the federal sector. The SICAM approach will leverage concepts of a federated trust model that allows for access of existing and new resources, rapidly and securely across boundaries. The MITA team envisions that all state agency Identity, Credential, and Access Management (ICAM) programs within Government will align with a central SICAM framework and the central infrastructure that will integrate resources and identity mechanisms across agencies boundaries.

The Draft SICAM documentation indicates that the initiative will adopt a series of harmonized standards developed by voluntary consensus standards organizations for exchange of identity information among all such entities and networks. The SICAM principles state there will be an emphasis on a service-oriented, layered architecture to provide a common messaging, security and privacy foundation to support the SICAM identity information exchange services. The foundation will also rely on web services exchange capabilities with a Public Key Infrastructure (PKI) and Security Assertion Markup Language (SAML) version 2.0 for identity federation. These security and privacy standards, and others, are in the following table. **Table 6-3** provides a simple listing of generally accepted Security and Privacy Standards that the State Medicaid Enterprise can use.

Note: A third party maintains the internet address for a resource, which may change over time.

Table 6-3. Security and Privacy Standards

Security and Privacy Standards		
Standard Name	***Objective***	***Source***
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.	http://www.cio.gov/documents/fea-security-privacy-profile-v3 09-30-2010.pdf
National Institute of Standards and Technology (NIST) Initiatives	NIST has a variety of initiatives to address IT standards. Some of these initiatives include: • Computer Security • Cloud Computing • Biometrics • Data and Informatics	www.nist.gov/information-technology-portal.cfm

Security and Privacy Standards		
Standard Name	***Objective***	***Source***
	• Health IT • Information Delivery	
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.	www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html
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.	www.oasis-open.org/wss
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.	www.projectliberty.org kantarainitiative.org
Security Assertion Markup Language (SAML)	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 in order 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	Organization for the Advancement of Structured Information Standards (OASIS) Security Services Technical Committee www.oasis-open.org/committees/security/

	Security and Privacy Standards	
Standard Name	***Objective***	***Source***
	Consumers, Authorization Decision Authorities, and Affiliate Members.	
Enterprise Privacy Authorization Language (EPAL) – W3C	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).	www.oasis-open.org
WS-Trust Model	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.	www.oasis-open.org
eAuthentication and use of *services Object Management Group (OMG) initiative*	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) has established an eAuthentication setup. OASIS tested and proved the E-Gov eAuthentication initiative using WS-* standards.	www.cio.gov/eauthentication www.idmanagement.gov
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.	www.ietf.org
Health Security	ISO/International Electrotechnical Commission (IEC) 17799:2000 "Information Technology Code of Practice For Information Security	www.iso.org/iso/catalogue_detail?csnumber=33441

Security and Privacy Standards		
Standard Name	***Objective***	***Source***
	Management”. Standards and Certification Criteria for Electronic Health Records (EHR). Metadata Standards To Support Nationwide Electronic Health Information Exchange.	healthit.hhs.gov/portal/server.pt?open=512&objID=1195&parentname=CommunityPage&parentid=97&mode=2&in_hi_userid=11673&cached=true www.gpo.gov/fdsys/pkg/FR-2011-08-09/pdf/2011-20219.pdf
Unified Modeling Language (UML)sec and Security Engineering Profiles	Efforts to create new security stereotypes to integrate them with the UML 2.0 activity diagrams along with other formal Message Sequence Chart extensions.	www.omg.org
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.	download.oracle.com/docs/cd/B10501_01/network.920/a96578/intro.htm
Consumer Health Informatics (CHI) Initiatives	CHI is a Kaiser Foundation Model 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: • Electronic Health Records Systems (EHR-S) • NwHIN	www.hhs.gov/healthit/healthnetwork/background/

***Note:** This item is not an official standard or standards organization.

Business Enabling Technologies

Table 6-4 provides a listing of generally accepted standards and specifications for process management involving definition, improvement, and innovation of business processes that drive the Medicaid Enterprise.

Note: A third party maintains the internet address for a resource, which may change over time.

Table 6-4. Business Enabling Technologies

Business Enabling Technologies		
Standard Name	***Objective***	***Source***
Business Process Model and Notation (BPMN) previously known as Business Process Modeling Notation **Business Motivation Model (BMM)**	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).	www.omg.org/technology/documents/br_pm_spec_catalog.htm
Extensible Markup Language (XML) Forms (XForms)	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.	www.w3.org/TR/2009/PR-xforms11-20090818/
Rule Markup Language (RuleML) Initiative	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, tool, and application development.	ruleml.org
Workflow Management Coalition (WfMC)	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.	www.wfmc.org
Customer Relationship Management (CRM) Extended Relationship Management (xRM)*	xRM is the principle and practice of applying CRM and is a standardized interchangeable relationship for services.	

***Note:** This item is not an official standard or standards organization.

Data and Information Standards

Table 6-5 provides a listing of generally accepted data and information standards and specifications for validation of content and structure.

Table 6-5. Data and Information Standards

Data and Information Standards		
Standard Name	***Objective***	***Source***
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 (XML) schemas that drive business processes globally.	www.x12.org
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.	www.astm.org/Standards/E2369.htm
Current Procedure Terminology (CPT)	The American Medical Association (AMA) is the source for official Current Procedural Terminology (CPT)—the most widely accepted medical nomenclature used to report medical procedures and services under public and private health insurance programs.	www.ama-assn.org
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.	www.ada.org/
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.	medical.nema.org
Health Level 7 (HL7)	Health Level Seven International (HL7) is the global authority on standards for interoperability of health information	www.hl7.org

Data and Information Standards		
Standard Name	***Objective***	***Source***
	technology with members in over 55 countries.	
International Classification of Diseases (ICD)	The International Statistical Classification of Diseases and Related Health Problems (most commonly known by the abbreviation ICD) is a medical classification that provides codes to classify diseases and a wide variety of signs, symptoms, abnormal findings, complaints, social circumstances, and external causes of injury or disease.	www.who.int
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.	www.regenstrief.org
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 health care providers and pharmacies.	www.ncpdp.org/indstry_outreach.aspx
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.	www.niem.gov/
Public Health Information Network (PHIN)	This agency provides various standards and measure definitions including Syndromic Surveillance messaging, EHR Meaningful Use, and Immunization Messaging.	www.cdc.gov/phin/
Systematized Nomenclature of Medicine – Clinical Terms (SNOMED CT)	This is the most comprehensive set of multilingual clinical health care terminology. Its aim is to improve patient care through the development of standardized clinical terminology regardless of language.	www.ihtsdo.org/snomed-ct/
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.	www.nlm.nih.gov/research/umls/quickstart.html

***Note:** This item is not an official standard or standards organization.

Using Technology Standards

The SMA should leverage the proven technology standards solutions identified in the Technology Standards Reference Guide by adopting and adapting them for their environment. The TA selects technologies and standards that meet the MITA Framework requirements, identifies the functional components that apply to the Medicaid Enterprise, as well as any gaps in the standards, and tailors them as necessary into robust solution sets. States should ensure alignment with, and incorporation of, industry standards.