Part III — Technical Architecture

Chapter 6 — Technical Services

Introduction

This chapter provides a discussion of the Medicaid IT Architecture (MITA) Technical Services. A MITA Technical Service provides the guidance and specifics to an IT staff (e.g., States or vendors) on how to implement a MITA technical capability.

A service-oriented architecture (SOA) using MITA Business and Technical Services solves the problems of creating a custom framework and vendor lock-in. It enables a State Medicaid organization to use multiple vendors to supply and support the MITA Framework. Technical services required by a Medicaid enterprise using MITA will have a much larger support base and, as such, will be debugged to a greater degree than single-use applications. By using the MITA Framework, it will be practical to purchase prebuilt services in the open market, or, in the case of State-developed systems, share service implementations. Prebuilt Technical Services can be used As-Is or enhanced using standard object-oriented techniques to vastly leverage development. Organizations can also purchase a wide variety of tools to help use and build applications in the MITA Framework, including design and implementation tools, data analysis tools, languages, libraries, and utilities. The use of standard services will also reduce the amount of training needed. Development organizations will be better able to find employees and consultants who already understand how the system operates.

This chapter answers the following questions:

- What is a MITA Technical Service?
- What are the parts of a MITA Technical Service?
- How is a MITA Technical Service developed?
- What is the MITA Technical Services flow?
- How do States use MITA Technical Services?
- How to MITA Technical Services benefit the Medicaid enterprise?
- How do States participate in developing MITA Technical Services?

Purpose

The MITA Framework has two categories of services: Business Services and Technical Services. Technical services are derived from the Business Service requirements (as described in Part I Chapter 5); technical principles, goals, and objectives (as described in Part III Chapter 2); and the MITA Technical Capability Matrix (TCM) (as described in Part III Chapter 5). Technical services provide underlying technical functionality (e.g., forms management, security, etc.) and are discussed in this chapter.

A MITA Technical Service defines a standard interface and functionality for a technical process that will align the common factors of a State's implementation with the MITA enterprise definition. The MITA Technical Service, as does a Business Service, allows two things:

1. **Plug-and-Play.** With plug-and-play, an individual service can be replaced with a new implementation without affecting the rest of the enterprise. For example, an enterprise can replace a service that is currently a wrapped COBOL application with a COTS product or J2EE C++ program without changing any of the external interfaces.
2. **Interoperability**. With interoperability, a system can change an external user of a service (e.g., delete, add, or modify external services or clients) without changing the service itself. For example, a new service could be an application or a client added to the enterprise that takes as input the output from an existing service.

Scope

A MITA Technical Service is an independent block of code with a well-defined standard interface that implements the logic of a specific technical capability.

Independence is an important characteristic of a service. An independent service can be replaced easily by a different service, provided the new service meets the needs of the user. Services are also location independent, because, in today's IT environment, a service does not have to be collocated with the users of that service.

Details of exactly how the service is performed must be documented so that other computers can read and interpret them. The documentation includes the functions that are included in the service (e.g., what is the expected output, what error checking will occur to ensure accuracy of the output, etc.) and describes how to obtain the service and how other computers request the service. Because computers cannot "complain" if the service is not satisfactory, documentation must include precise information about possible unsatisfactory conditions (i.e., errors) and how each should be handled.

Definition methods for MITA Technical Services:

- Interfaces are defined in Web Service Definition Language (WSDL).
- Messages are defined in XML Schema.
- Business Logic, which is currently freeform text, will become business rules in the future.

Service Management (i.e., orchestration) is defined in Web Services–Business Process Execution Language (WS–BPEL).

MITA Technical Services are implementation-neutral. They do not specify platform, binding protocols, programming models, operating systems, underlying infrastructure technologies, or other implementation details used to implement the service.

MITA Technical Services define what services are needed by a Medicaid enterprise to implement the required generic support functions. The goal of the MITA Framework is to specify services that enable interoperable Medicaid services. These services will be covered in future versions of the MITA Framework.

Individual services and messages are woven together with other Business and Technical Services using an orchestration process, which is defined in the Part III Chapter 7, Application Architecture.

What Is a MITA Technical Service?

A Technical Service is a piece of software that implements a generic IT capability. It has a defined interface for its invocation, performs a defined function that corresponds to the capability, and returns defined results. MITA Technical Services are divided into three technical areas:

- Interoperability services
- Data access services
- Security and privacy services

> This version of the Framework only discusses the technical areas and principles associated with that area. Specific technical capabilities and their associated technical services will be developed in a future version of the Framework. New technical areas may also be identified as part of this process.

The remainder of this section will discuss the technical areas and their associated principles. Technical areas are logical groupings of technical functions; the relationship between technical area and technical function is equivalent to the relationship between business area and business process.

Interoperability Services

Interoperability is one of the key MITA goals and requirements. Currently, many of the States are addressing this issue in one form or another, whether by using a translator for the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or by trying to connect internally or to other Federal agencies.

Given the importance of the interoperability of technical area and services to the overall Framework, the technical challenges related to interoperable systems are addressed in this chapter. **Table 6-1** includes questions and answers about the interoperability technical area.

Table 6-1. The Interoperability Technical Area

Question	Answer
Why is this technical area important to MITA?	The interoperability technical area describes the business capabilities and technical functionality necessary to achieve efficient system-to-system interactions within Medicaid programs and between Medicaid and other external initiatives for MITA.
Who should understand this technical area?	Designers and implementers should understand the concepts presented in the interoperability model to incorporate those concepts into system designs.
How will this model be used?	The interoperability technical area will provide guidance and recommendations that support the development and implementation of services and data that can be shared among the MITA community, while still allowing States to retain their autonomy. The States can follow the model to achieve cross-organizational information sharing through a common approach.
How will it be refined and updated?	The interoperability technical area will be reviewed along with the rest of the MITA Framework. Based of the findings of this review, changes may be made to the capabilities and services. Detailed interoperability guidelines and standards will be selected or defined.
How will it support ongoing business decision making?	New IT procurements should adopt these concepts of MITA interoperability.

It should also be noted that business interoperability challenges should be addressed as well. Some of those challenges include the following:

- Lack of incentives to cooperate may make it necessary to sell organizations on the benefits of interoperability.
- Lack of funds for cross-organization activities may require changes to budget allocation methods.
- Lack of infrastructure to support interoperability and reconciliation may slow implementation.
- Legacy systems with disparate definitions and stovepiped systems may not conform to new interoperability standards.

Although the MITA hub architecture, interoperability, and access channels services are generic capabilities based on standards-based contracts that can be applied to meet the technical challenges, it is the focus on creating a service-oriented government approach to interoperability that will best overcome the business challenges. The service-oriented approaches are represented in **Figure 6-1** and **Figure 6-2**.

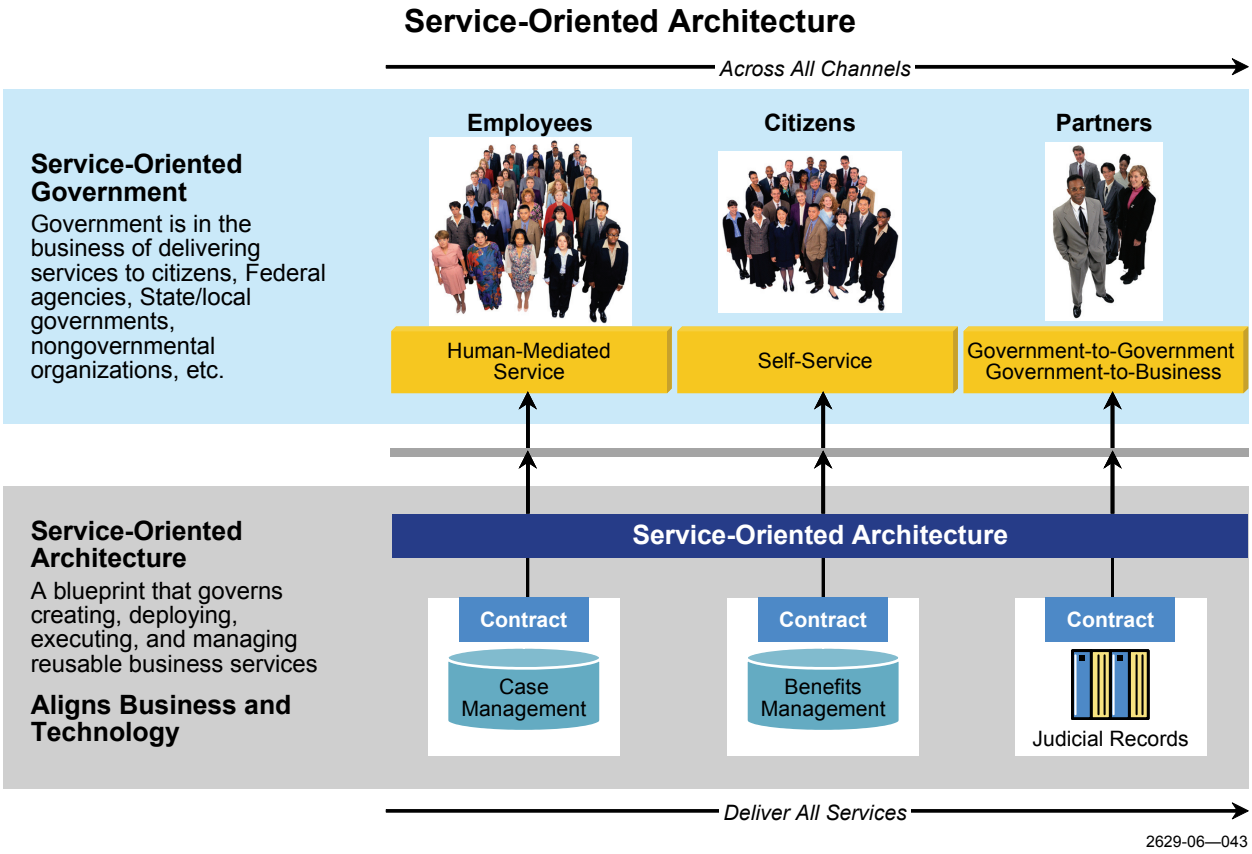

Figure 6-1. Service-Oriented Architecture Approach

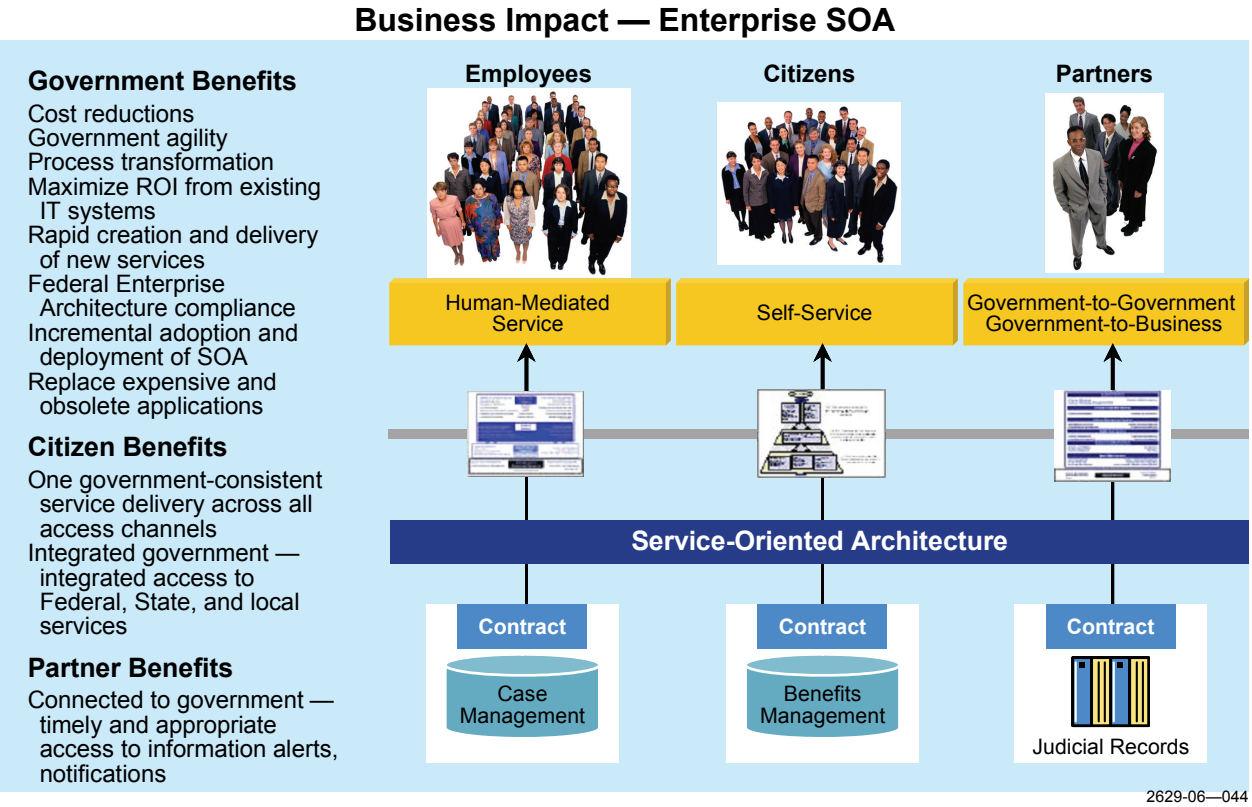

Figure 6-2. Service-Oriented Government and Architecture

The key concepts for interoperability services are listed below:

- Use services and messaging standards for real-time communication between business areas and across organizations.
- Establish a clear process and consistent mechanism for system-to-system communication through the definition of communication requirements and the recommendation of technologies for automated responses (e.g., Web services, XML protocols, etc.).
- Define a common MITA interface that can hide complexity and shield the States and partners from technical details.
- Define a common set of functions and features that can be separated from the applications and implemented using service utilities.
- Define a logical interoperability architecture (i.e., a service overlay) based on hub technology and the communication protocols that can be adapted based on channel definitions and the use of virtual communication access mechanisms.
- Support alternative access to the same information and services — such as the Web (i.e., human interface), Internet (i.e., machine to machine), etc. — and enable the data,

process, or services to be hidden behind interoperability channels that can adapt to changing needs using configuration files.

- Use a business-oriented service interoperability process that focuses on business needs based on three principles:
  - Defined common semantics (i.e., the meaning of something)
  - Defined common syntax (i.e., the structure of the message)
  - Defined common mechanism (i.e., the means of exchanging information)
- Define a set of common service elements that will be adaptable through variants and extensions, with the goal being to define commonality and design for change, while also providing a limited set of change management within the service layer through adaptable "wrappers."
- Define service interoperability solutions that rely on common definitions for channels and utilities that are specific to business areas but designed with common underlying architecture and common utility components.
- Define and create virtual access mechanisms that can be used by the hubs or by individual State systems for exchanging information.

MITA Interoperability Capabilities

MITA has taken a strategic business and technical approach to interoperability (see **Figure 6-3**). Interoperability is divided into the subfunctions, topics, and types of communication, while recognizing that common sets of conflicts occur and common solution patterns can be used.

Separate interoperability channels will be defined for each type of information flow, enabling the definition of utility services that can be shared across the Medicaid enterprise.

Interoperability channels will be refined and detailed collaboratively through the MITA workgroup process.

The key concepts of the interoperability technical area are as follows:

- Interoperability is addressed with a set of common elements and approaches that are designed to fit with other areas and be adapted to meeting dynamic needs.
- Each business area is made up of a selection of business processes that includes a set of connectors. The connectors are defined by the type of connection (e.g., asynchronous communication, publish and subscribe, and request and respond) and the type of information or services exchanged. Topics, subjects, or access to a given type of information are grouped together on a common logical channel. Security and privacy access control may also result in separate channels.

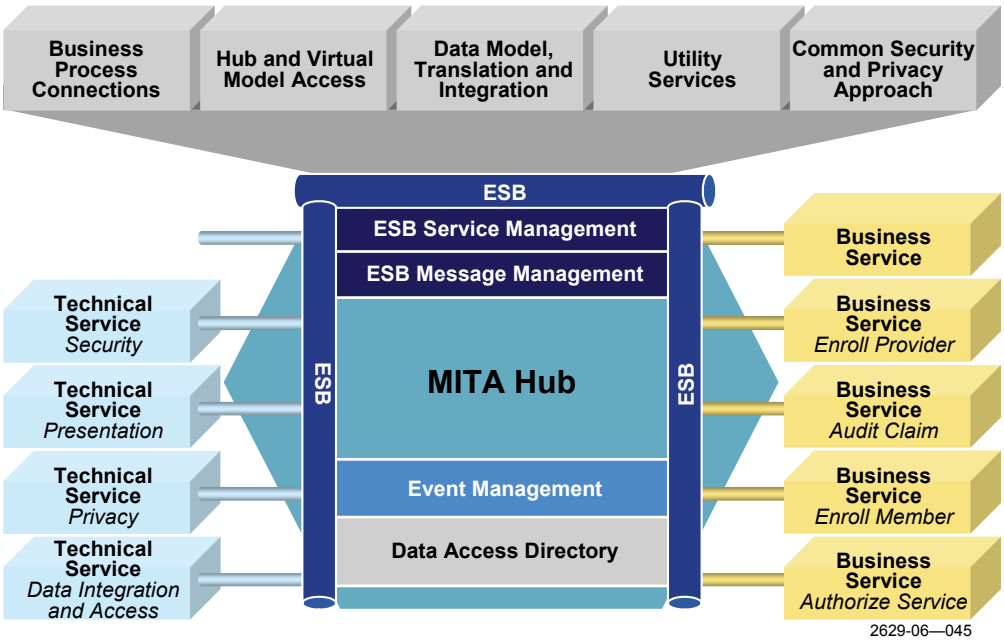

Figure 6-3. Conceptual Interoperability Capability

- Access channels will provide the Medicaid staff with access to interfaces with organizations through multiple means (e.g., mobile, wireless, PDA, kiosks, etc.) that provide batch interaction with a series of messages. Private–public partnership access may include an organization that can receive access because of a contractual arrangement. The types of features and functions accessed must be clearly defined.
- Access channels also provide rights to certain information or the ability to share information through access to specific interoperability channels. These exchanges can be planned for, and a set of collaborative tools provided. The access channels to interoperability channels will include defined connectors, and the connectors will define alternate access approaches. These access paths will be adaptable based on policy, failure, or recovery conditions.
- Hub architecture is the most mature means of transmitting and receiving services and information over an interoperability channel. It also offers additional security and privacy control points and the ability to locate utility services on the hubs. Once the request is at the hub, the interoperability services may need to access information and services through virtual access.
- The interoperability channel may define data translation capabilities that mask any incompatibilities. A set of services will be used to create an interoperability channel. An interoperability table will be used to define all these elements and for the adaptation.
- Security and privacy services will be defined with alternative levels of protection, depending on the services and topics communicated over that channel.

- Interoperability conflicts will be identified through interoperability assessments. These are grouped into business-centric pieces that are based on common business interests or purposes and defined by the interoperability channels.
- Functionality is provided by individual services, not built into each application.

Future versions of the Framework will identify the specific interoperability services required to implement these interoperability capabilities.

Data Access Services

The data access technical area contains the Technical Services required to implement the data access methods specified by the MITA Data Management Strategy (Part II Chapter 2).

Table 6-2 includes questions and answers about the data access technical area.

Table 6-2. The Data Access Technical Area

Question	Answer
Why is this technical area important to MITA?	The data access technical area describes the data access capabilities and functionality necessary to achieve efficient service-to-data interactions within Medicaid programs and between Medicaid and other external initiatives for MITA.
Who should understand this technical area?	Designers and implementers should understand the presented concepts in order to incorporate those concepts into system designs.
How will this model be used?	This model provides guidance and recommendations that support the development and implementation of data access services that can be shared among the MITA community, while enabling States to retain their autonomy. The States can use the services to achieve cross-organizational information sharing through a common approach.
How will it be refined and updated?	The technical area will be reviewed along with the rest of the MITA Framework. Based of the findings of this review, changes may be made to the capabilities and services. Detailed interoperability guidelines and standards will be selected or defined.
How will it support ongoing business decision making?	New IT procurements should adopt these MITA data access concepts.

Some key data-access capabilities are listed below:

- It provides access methods to data based on content, user, and role.
- Network transparency — Only a few people (e.g., service analysts and service architects) will define which services are local and which are remote. Network aspects are hidden so that local or remote data objects are fully interchangeable. This will allow for failover, and it will enable all services to use a common alerting and failure notification approach that can be routed to one or more facilities.

- Persistence transparency — The services components must be connected to a set of data and documents, as well as have the ability to recognize the existence of different replicas of the same document, data, information through the use of metadata. Data access and data sharing utility services with models, metadata, linked translation, and mapping capabilities will be used to address this issue and define the master and replica copies and recovery strategies.
- Protocol transparency — It will enable protocols transport and data to reside anywhere on a network within the scope of security and privacy access as defined for the user or system elements.
- Point-of-view transparency — Users should be able to access around their point of view, their context of operations, and the way they want to solve problems.
- Location transparency — Locations of data can change, and the services need to provide globally unique handles that hide the exact physical location of the data and allow the restructuring of operations without breaking the virtually linked components that represent the related context.
- Replication transparency — Users of a service will not know the difference between the original data and the copies or replicas. The original recognizes the replicas and can set up a dirty flag if the data or service has changed. Different replication strategies can exist (e.g., close synchronization, loose synchronization, or even unsynchronization) for certain types of notices. For most types of data and information, it is okay or even desirable to always get the newest available version; for others, the timeframe may dictate using selected services or data.
- It receives messages based on defined interoperability channels; handles all the message buffering, transport protocols, and necessary message translation; includes any routing; and supports the adaptability needs or any manual functions that may need to be done (e.g., special queries).
- It supports data stores that are either data mart types or more relational data models.
- It supports virtual data access capability.
- It provides capabilities for collection, filtering, and delivery of blocks of information to the business area.

Future versions of the Framework will identify the specific data access services required to implement these interoperability principles.

Security and Privacy Service

Security and privacy issues have many common elements that must be addressed by each agency, especially concerning the privacy of personal health data. While there is extensive guidance in this area, little clear guidance exists for moving forward and addressing security and privacy as an integral, woven element of all the business process and technical aspects. The security and privacy Solution Set guide and associated informational templates and models are designed to address this issue. This documentation is open to evolving security and privacy

needs and aids in the creation of a decision framework that balances risk and value. The security and privacy Solution Sets go beyond HIPAA Security and Privacy Rules to provide a comprehensive and open approach that can address new threats.

A key role of this Solution Set is to bring the security and privacy issues to the attention of each of the leaders of the Medicaid support system, going beyond the traditional boundaries of the Medicaid Management Information System (MMIS) and reaching out to other agencies (e.g., those that are partners in human service benefits delivery and State IT delivery), the provider community, and the beneficiaries/members/citizens themselves. It is important to create a protected and trusted environment that is not costly to maintain and to show where security and privacy solutions are integrated within the enterprise and aligned with the cross-enterprise via a set of controlled and managed interfaces that follow a set of policies.

The area of security and privacy is changing rapidly, with new standards and products being introduced almost monthly to address the constant stream of new threats and viruses. Security and privacy can no longer be addressed by only the specialist; it must also be understood from a business point of view. The development of Solution Sets was based on the marrying of common threat and attack models into a set of common security and privacy scenarios that can be related to a user's business with a business impact and risk gathering activity.

In response to ever-evolving threats and the growing complexity of technologies responding to these threats, the Security and Privacy Goals and Policy Model along with a set of business impact security and privacy use cases were developed. They were developed from common sets of security and privacy goals and policies derived from the HIPAA Security and Privacy Rules (relying on the National Institute of Standards and Technology [NIST] HIPAA guidance and the gathering of HIPAA lessons learned) and more general goals and policies gathered from experience and government documents. These elements will be described with the detail to be provided within the MITA Design Center Repository.

An initial set of key solution principles and concepts provided the foundation for many of the steps taken. These are explained below and will be elaborated in the future based on feedback from early adopter States and planned workshops.

Key security and privacy principles include the following:

- Goals and objectives are defined with both informal and formal policies. The formal policies are based on industry-standard security and privacy languages and can be accessed and shared with security service elements within packages and within a unified but distributed and federated security and privacy framework.
- The federated and policy-based environment is service oriented. The architectural approach is based on the fact that end users and their many entry points into the State systems need a unified and conceptually centralized "view" of the policies to be enforced, while these policies need to be delivered in a distributed and changing world. Common direction and adaptable implementation is often called *federated policy management*, which enables users to specify preferences and policies at a high level and

then uses automated tools to map those preferences and policies into appropriate rule sets (i.e., mechanism), rules on policy-driven enforcement, and control mechanisms.

- Security and privacy must be integrated at many points throughout the enterprise and through the "communities" or cross-enterprise domains that are defined with channels with selected endpoints. Many of the security concepts (e.g., security context, decentralized label models, and usage control) have been taken to a higher level of abstraction and integrated into the reference models at all levels so that security and privacy integration points and aspects are considered throughout, with common sets of security and privacy meta models and data elements that are exchanged in a consistent service interface manner.
- Security and privacy solutions will rely on service and privacy utility services and patterns of use that can be "declaratively changed" and monitored within the design center. In addition, exceptions can be tracked and actions managed within a security and privacy control center. These include common ways to share vulnerabilities, receive alerts, and collaborate around common cross-enterprise troubleshooting activities.
- Bounding, partitioning, and abstracting of the services and communications interfaces are incorporated so that roles, responsibilities, and coordinated actions can be managed.
  - *Zone*. The enterprise and application have been divided into presentation, demilitarized zone (DMZ), business, data access, and shared exchange zones.
  - *Boundary Crossing Point*. The zones will have clearly defined boundary crossing points with firewalls based on business agreements among the participating parties. These include government employees who act on behalf of the citizens and establish privacy rights policies that can be read and understood by end users (i.e., requiring no more than an eighth-grade education and delivered in a just-in-time manner).
  - *Federation*. The system can provide a combination of global policies and individual implementation and control within the security and privacy area. Both the Liberty Project and the Web Services Interoperability Organization (WS-I) have defined *federation*, and the MITA approach is primarily based on the WS-Federation standard.
  - *Value Management*. Continuity of service delivery, loss of information of value, and loss of real dollars. An overall balanced approach between risk and value and performance reference model and approach to gather and measure the phased approach to meeting the objectives.
  - *Identity Management.* The system maintains a mechanism for authorization and authentication to be used for access to data and services.
  - *Channels*. Channels provide topic-based service and data resource abstraction that can be used by a community of organizations and individuals to define, manage, and audit policies and claims on proper and improper usage.

- *Service and Data Endpoint*. This involves a set of service elements that can be defined along a channel. The endpoints will be defined using WSDL 2.0 with any necessary extensions for healthcare.
- *Decentralized Label Management*. This provides a self-describing and managed resource with an associated set of protections whether the data is at rest or in motion. It will enable owners and authorized users to taking data resources with them, including the history of who has read and updated the data and the frequency of changes.
- *Common Security and Privacy Metadata and Metadata Exchange*. Consistency requires that a common format be used for all security and privacy mechanisms. When establishing the services and data that will be exchanged, the policies and practices can be reviewed by others in the community or along the channels of communication. The individual security and privacy standards will have defined metadata elements, and the initial definition of common standards profiles for the MITA community has started. A common set of security and privacy metadata will be defined, and the WS-Metadata Exchange standard will be used for managing consistency.

Goals

Although security and privacy solutions are influenced by the HIPAA laws, they must go beyond these laws. They must also provide a set of security and privacy implementations that can be adapted and extended, while at the same time providing a consistent base for the Medicaid community and aligning with the security and privacy aspects of other initiatives (e.g., the Federal Health Architecture [FHA] and the National Health Information Initiative [NHII]). In the future, security and privacy solutions will also address common issues arising from other industries and lessons learned from HIPAA experience.

The initial set of goals has been defined as follows:

- A consistent approach to security and privacy across the Medicaid enterprise, including services and solutions, the human elements, and cross-organizational understanding (i.e., from management to administrative personnel)
- The ability to react as a community to detect, deter, and respond to common issues that effect Medicaid and the healthcare industry (i.e., continuity of operations) through the use of common terminology, common threats, and shared concerns
- Provide security and privacy mechanisms needed for sharing information
- Provide privacy mechanisms related to healthcare and personal information
- The introduction of security analysis as part of business analysis (i.e., security and privacy integration points are introduced into business activity models and technical models)
- The ability to adapt and extend the security and privacy aspects as new threats and forms of attack are identified

These goals parallel the development of business impact security and privacy use cases and Solution Sets definitions. This risk/value framework has been refined into a common goal hierarchy.

Cross-Cutting Security and Privacy Concerns

Security and privacy issues are often thought of as isolated from the rest of the organization, characterized by protecting against boundary threats and ensuring that personnel can be trusted. However, the greater threats have appeared, including those from insiders and a combination of insiders and outsiders. Some organizations have attempted to bolt on security and privacy aspects, but this approach has been extremely difficult as the HIPAA experience has shown.

The target vision is for security and privacy to be woven into all aspects of the business process, so that it is understood by all organization members with different levels of understanding depending on individual needs. This vision should be implemented with each new business initiative and change in technology. While security and privacy is a complex issue, it must be understandable by the management, business leaders, partners, and customers of the services delivered; citizens receiving services and supplying personal information must trust the ability of the organization to secure and protect their information; and the organization leaders must be able to protect the valued assets and keep the continuity of services intact.

The area of security and privacy leverages the work of government, industry, and federally funded academic research on security, privacy, and continuity of operations; and it has a strong link to delivered and emerging products and solutions, extensive industry investment in new products, and the involvement in standards organizations. Previous efforts have tried to create a separate security and privacy architecture and set of products, but MITA treats this issue as a cross-cutting design aspect that includes a limited group of common centralized elements and many distributed mechanisms and controls.

The security and privacy services are designed to meet a set of key principles. These principles can be applied regardless of implementation technology or application scenario. The security principles are summarized in **Table 6-3**.

Future versions of the Framework will identify the specific security and privacy services required to implement these interoperability principles.

Table 6-3. MITA Security Principles

Principle	Concepts
Compartmentalize	This involves reducing the surface area of attack. Firewalls, least privileged accounts, and least privileged code are examples of compartmentalizing. Ask yourself how you will contain a problem. If an attacker takes over your application, what resources can be accessed? Can network resources be accessed? How are you restricting potential damage?
Use least privilege	This involves running processes using accounts with minimal privileges and access rights, which significantly reduces the capabilities of an attacker who manages to compromise security and run code.
Apply defense in depth	This uses multiple gatekeepers to keep attackers at bay. Defense in depth means that systems do not rely on a single layer of security or become vulnerable if one of its layers is bypassed or compromised. Can your system survive the situation where one of the firewalls between different zones is not operational?
Do not trust user input	User input is the attacker's primary weapon when targeting an application. This principle assumes that all input is malicious until proven otherwise. It applies a defense-in-depth strategy to input validation and takes particular precautions to ensure that input is validated whenever a trust boundary in an application is crossed.
Check at the gate	This authenticates and authorizes callers early, usually at the first gate.
Fail securely	This principle ensures that sensitive data is not left accessible if a system component or application fails. It returns friendly error messages to end users that do not expose internal system details that may help an attacker exploit vulnerabilities in an application.
Secure the weakest link	This involves identifying any vulnerabilities at the network layer that an attacker can exploit.
Create secure defaults	Ways to create secure defaults include setting up the default account with least privilege, disabling the default account by default and then explicitly enabling it when required, using a password in plaintext in configuration, and ensuring that sensitive information does not leak back to the client when an error occurs.
Reduce your attack surface	This involves reducing the surface area of attack by disabling or removing unused services, protocols, and functionality. Does your server need all those services and ports? Does your application need all these features?

All implementation details are private to a service. The message-oriented interfaces and operations that a Technical Service exposes provide ample insulation from the implementation choices made by a particular service developer. This characteristic is critical to service autonomy, and it allows flexibility of implementation details. It also allows the substitution of one service implementation for another. As long as both services respond to the same set of messages and operations with comparable results, the requestor is unaware that a different implementation of a service has been used.

In order to accommodate these implementation details (e.g., performance, platform, infrastructure, and software model), each MITA service may have one or more State logical description of the service, and for each of these one or more implementations may be instantiated. Specific implementation details are specified for each unique implementation by a State- or vendor-developed logical service definition. This relationship is shown in **Figure 6-4**.

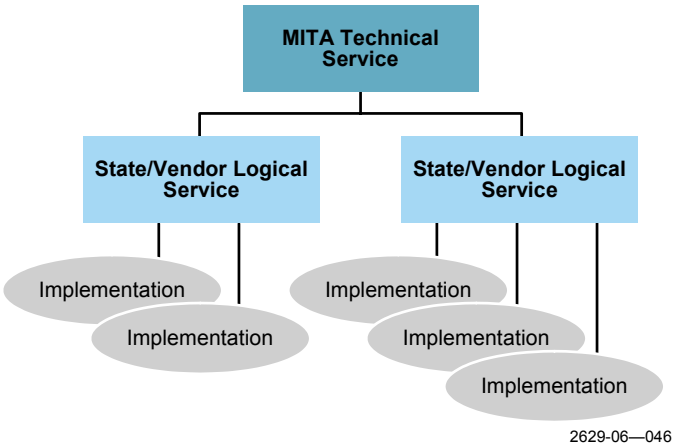

Figure 6-4. Technical Service Implementations

What Are the Parts of a MITA Technical Service?

This section defines the individual parts of a MITA Technical Service. In the MITA Framework, a Technical Service has the same metadata as a Business Service. Both must have the following associated data:

- **Service Name.** The name of the service that is invoked by the Technical Service Definition Package (TSDP) is a MITA-defined set of metadata describing the service. The service contract describes the expected behavior of the interface (e.g., whether the interface a real-time or online interface), as well as the security and privacy constraints on the service (i.e., required strong encryption). The following are examples of interface behavior patterns:
  - A *one-way* interface only receives or outputs data (e.g., report generator).
  - A *two-way* interface receives and sends data. Two-way traffic has two other attributes: (1) *initiator* defines who initiates the interface, either the service (e.g., request for information) or the outside client (e.g., inquiry), and (2) *processing characteristic* defines the relationship between the input and the output:
    - Point-of-sale (POS) transaction. A real-time transaction (e.g., a pharmacy POS) that features very constrained response time and high reliability

  - Online transaction. An inquiry on a member or provider that features more relaxed response time while still allowing for conversation-type human interaction
  - Batch. Typical batch processing constraints
  - Asynchronous**.** No constraints on processing times but response and coordinating data are required

- **Purpose**. The purpose is developed from the technical area's principles and Technical Capability Matrix.
- **Business Logic**. Business logic describes what goes on "under the hood" of the Technical Service. It documents the underlying logic, functionality, and capability provided by the service. Initially, the business logic will be freeform text or template driven, but it will eventually become business rules.
- **Constraints.** Any constraints of the service are listed.
- **Formal interface definition.** This defines the services triggers and results. It also documents the interfaces and operations used by the service. The interface is defined by using WSDL. Initially, MITA will provide an informal textual description (i.e., template) of the services interface. As the MITA services are developed, WSDL interface descriptions will be developed.

WSDL is a document written in XML and is an XML document. The document describes a Web service. It specifies the location of the service and the operations (or methods) the service exposes.

- **Use Case.** This will initially only document the main success path and critical failure conditions of the service. Initially, it will be in freeform text, but it will be in UML once the population of the Business Services begins.
- **Solution Set.** This area maps the Solution Sets developed to implement this service.
- **Structure Diagram.** This graphically depicts the business logic performed by the service and interconnects the Solution Sets.
- **Performance Measures.** Performance measures are defined, so that all stakeholders can measure the same things in the same way.
- **Test Scenarios and Test Cases.** Test scenarios and test cases that could be used to validate compliance to the service contract are documented.
- **Map to MITA data models.** This mapping provides a trace of data used by the service (e.g., data in motion and shared business data only) to the MITA conceptual and logical data model. This is an enhancement of the mapping done for the Business Service. Data in motion is defined by XML Schemas.

How Is a MITA Technical Service Developed?

The process for developing a MITA Technical Service is the same as that used for developing a Business Service. An overview of the process is presented in Part III Chapter 4.

The first step in developing a Technical Service is to decide what technical area capability is being implemented. Once this is done, the MITA repository[1] must be accessed to determine if the service already exists. If the service already exists, the implementer must then look at the associated metadata to determine whether the service will need to be adapted or extended. If the service does not have to be extended, the implementer should then examine the associated Solution Sets to determine whether an implementation meets the specific technology requirements. (Solution sets are described in Part III Chapter 9.) If a Solution Set exists, the implementer should use the existing definition. If a Solution Set does not exist, the implementer should define a new Solution Set and submit it back to the MITA governance board for review. (**NOTE:** This board does not currently exist.)

If the Technical Service does not exist in the MITA repository, then the Technical Service and TSDP must be created. Most of the information is derived from the Business Service requirements, technical area principles, and technical TCM.

The process for creating a TSDP is similar to that of creating a BSDP (see Part III Chapter 4). The differences between to two processes are described below:

- **Service Name Development.** This name will be used to register the Technical Service in the MITA service registry. The technical naming convention is to be determined.
- **Service Contract Development.** This process involves the following elements.
  - The *purpose* is a short one- to two-sentence description of what the service does, and it is derived from the Business Service requirements, technical area principles, and TCM.
  - The *formal interface definition* is developed using the required Triggers, Results, and MITA data model. It also documents the interfaces and operations used by the service. Initially, MITA will provide an informal textual description (i.e., template) of the services interface. As MITA matures, WSDL interface descriptions will be developed.

[1] The MITA repository does not currently exist but will be developed in the future.

WSDL describes a Web service in two fundamental stages: one abstract and one concrete. Within each stage, the description uses a number of constructs to promote reusability of the description and separate independent design concerns.

At an abstract level, WSDL describes a Web service in terms of the messages it sends and receives. Messages are described independent of a specific wire format using a type system, typically XML Schema.

An *operation* associates a message exchange pattern with one or more messages. A *message exchange pattern* identifies the sequence and cardinality of messages sent and/or received as well as those who the messages are logically sent to and/or received from. An *interface* groups together operations without any commitment to transport or wire format.

At a concrete level, a *binding* specifies transport and wire format details for one or more interfaces. An *endpoint* associates a network address with a binding. And finally, a *service* groups together endpoints that implement a common interface.

Technical Service Solution Sets

Since MITA Technical Services are implementation-neutral, the MITA Framework requires a method for documenting theses implementation details. This is required so that individual States and vendors do not have to keep recreating the solution for the service. Solution sets are the logical implementation of a MITA service. (Chapter 9 discusses Solution Sets in more detail.) The Solution Sets are pattern-specific and can be platform- and technology-dependent:

- A Solution Set is an implementation of a MITA Technical Service.
- Solution set mapping is shown in **Figure 6-5**.
- A MITA repository will be available to store Solution Set information.
- States can use MITA Solution Sets to determine whether there is already an implementation of a MITA service that is applicable to their specific implementation.

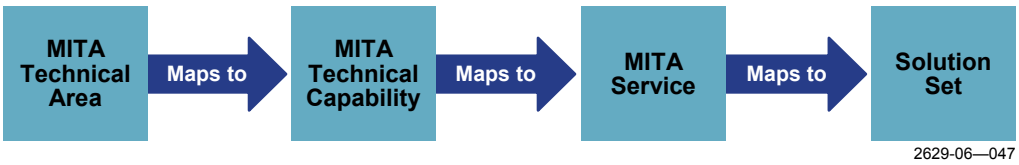

Figure 6-5. Conceptual Relationship Between Technical Solution Sets and Technical Areas

A MITA Technical Service Solution Set consists of an implementation-specific TSDP and an associated implementation. The implementation-specific TSDP is derived from the MITA TSDP and adds the implementation-specific details to the MITA TSDP attributes (e.g., protocol and binding information and endpoint). The implementation-specific TSDP provides the specifications for the Technical Service being implemented by the State. In some cases, the WSDL in the implementation-specific TSDP may be used by a code generator to actually

generate some of the required code. The implementer of the Technical Service (i.e., the State or vendor) is responsible for producing the implementation-specific TSDP for this solution if one does not already exist in the MITA repository. When completed, the Solution Sets are submitted back to the MITA repository.

What Is the MITA Technical Services Flow?

The Technical Service's objective is to provide an independent version of a technical capability that can be woven together with other services to form composite business processes. This independence is provided by services guided by the following architectural concepts:

- Loosely coupled services
- **No** predefined predecessor or successor services to an individual service
- Services configured through the use of a service contract and an orchestration language
- Changes to the flow of services made through changes to this orchestration, **not** to the service itself
- Mandatory interface compatibility between the services

As stated earlier, access to an individual service is defined by the service contract using WSDL. The process to define a flow linking several services together is called orchestration, which is done using BPEL.

> BPEL is used to describe the behavior of a Business or Technical Service based on interactions between the service and other services. The interaction with each service occurs through the service interfaces, and the structure of the relationship at the interface level is encapsulated in the service interface link. The BPEL defines how multiple service interactions are coordinated to achieve a business goal, as well as the State and the logic necessary for this coordination. Finally, BPEL also introduces systematic mechanisms for dealing with exceptions and processing faults.

Orchestration defines successor and predecessor services to a service. Since this orchestration is based on definite implementation specifics, MITA will not develop the BPEL orchestration for a service. States will be responsible for developing BPEL orchestration and submitting them to the MITA repository as part of a Technical Services Solution Set. Once in the repository, the BPEL orchestration will be available for reuse by other States.

How Do States Use MITA Technical Services?

A MITA Technical Service should be used as a reference document that identifies:

- The technical interfaces that must be exposed to other processes
- The standard interface definition
- A description of the underlying business logic

It should also be used as a requirements document specifying the details for Business Services. The document in this role can be used as a source for a State's Advance Planning Documents (APDs) and RFPs.

How Do MITA Technical Services Benefit the Medicaid Enterprise?

The use of MITA Technical Services will provide the following benefits:

- **Reuse.** A service can be shared by multiple organizations and systems. Each time a service is used by an additional system, value is gained from the original investment in that service. An example would be security access and controls, which is a service needed by every application. By writing this service once and reusing it for all applications, development time and complexity are reduced.
- **Cost.** A service that is written once and maintained in one place reduces overall development and maintenance costs. An example would be security access and controls because costs increase when each application writes its own security access and control modules.
- **Consistency.** When a service is shared across multiple applications, results will always be the same. Using the security access and control example, users would benefit from using the same password to access multiple systems. Another example would be performance measurement services. By always measuring performance in the same way, it is possible to perform valid comparisons between organizations or within a single organization over a period of time.
- **Flexibility.** Widespread use of services makes it possible for systems to be more responsive to change. Changes can be implemented by improving the functionality of a single service, using a different service to accomplish a task, or incorporating new services.
- **Broader Market place.** MITA Technical Services are defined as general Technical Services and are not specifically tailored to the Medicaid environment. This allows technical solutions from non-Medicaid environments to be used in the MITA Medicaid enterprise.

In addition, MITA Technical Services support State alignment with the MITA enterprise architectures. MITA Technical Services are defined in terms of common solutions that enable

State-specific implementations, making it possible to develop services that are adaptable and extensible. The MITA Technical Service approach combined with the accommodation for State-specific implementations means that the MITA services will help meet State business needs.

How Do States Participate in Developing MITA Technical Services?

States participate in developing the MITA Technical Services by:

- Participating in working groups defining the common Technical Services requirements
- Participating in working groups defining the standard interface for each Technical Service
- Defining implementation-specific portions of a Technical Service's WSDL
- Defining orchestration specifics in BPEL
- Participating in defining standards for the MITA infrastructure
- Submitting details into the repository as MITA Solution Sets

As mentioned earlier, States may need to adapt or extend a MITA Technical Service to meet their individual requirements. The MITA Framework provides several ways for States to personalize a MITA Technical Service. These personalization methods are listed below:

- **Change message structure.** This is done by changing the schema used in the Business Service's WSDL. For example, a schema change could be used if the standard schema shows certain entities as being optional and a State wants those entities to be mandatory in its implementation.
- **Change data being used.** This involves changing a dataset name (e.g., instead of mapping to "State-A-MVA," map to "State-B-MVA") or substituting a different dataset with the same name.
- **Replace capability.** This involves replacing the service with a State's unique service, but preserving input and output.
- **Reorchestrate services.** This involves adding new services to the flow. Reorchestration can be used to recombine existing services or to add new services.
- **Change business rules.** This involves replacing the set of business rules used by a service with a new set of business rules.

Conclusion

MITA Technical Services help to ensure that implementations are interoperable and plug-and-play capable. With participation by States, partners, and other stakeholders, MITA Technical Services will be refined and become more specific over time. State Medicaid enterprises will evolve to optimize adaptability, flexibility, interoperability, and data sharing. This evolution will enable major improvements in policy, decision making, and day-to-day operations.