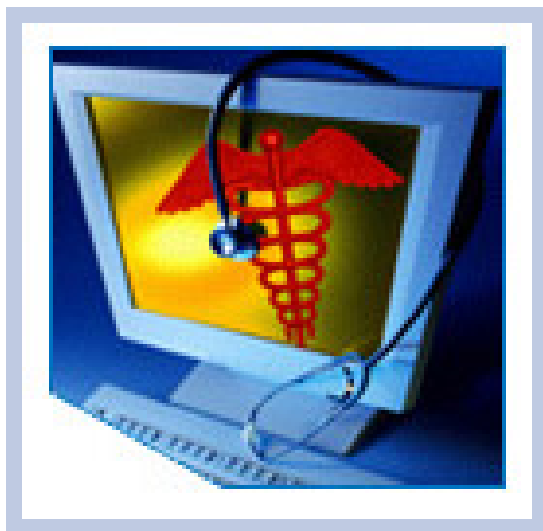


# HITSP Patient-Provider Secure Messaging Interoperability Specification

---

HITSP/IS12



*Submitted to:*

**Healthcare Information Technology Standards Panel**

*Submitted by:*

**Consumer Perspective Technical Committee  
(Formerly Consumer Empowerment Technical Committee)**



## DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
	Template V2.4	Project Team	July 31, 2008
0.0.1	Review Copy	Consumer Perspective Technical Committee	September 26, 2008
0.0.2	Review Copy	Consumer Perspective Technical Committee	December 10, 2008
1.0	Released for Implementation	Consumer Perspective Technical Committee	December 18, 2008



# TABLE OF CONTENTS

<b>1.0</b>	<b>INTRODUCTION .....</b>	<b>7</b>
1.1	Interoperability Specification Overview .....	7
1.2	Interoperability Specification Document Map .....	7
1.2.1	List of Constructs .....	8
1.3	Copyright Permissions .....	10
1.4	Reference Documents .....	10
1.4.1	Glossary Term Clarifications .....	11
<b>2.0</b>	<b>REQUIREMENTS .....</b>	<b>13</b>
2.1	Use Case Synopsis .....	13
2.2	Use Case Requirements .....	15
2.2.1	Mapping of Use Case Actions to Information Exchange Requirements .....	15
2.2.2	Data and Information Exchange Requirements .....	16
2.2.3	Identification of Business Actors Mapped to Requirements .....	17
2.2.4	High-Level Diagrams .....	19
<b>3.0</b>	<b>DESIGN .....</b>	<b>24</b>
3.1	Scope of Design .....	24
3.1.1	Assumptions .....	27
3.1.2	Constraints .....	28
3.1.3	Pre-conditions .....	28
3.1.4	Post-conditions .....	29
3.1.5	Process Triggers .....	29
3.2	Detailed Design .....	30
3.2.1	Technical Actor Role Descriptions .....	30
3.2.2	Construct Requirements .....	32
3.2.3	Mapping of Business Actors to Technical Actors and Constructs with Optionality ....	35
3.2.4	Construct Dependencies .....	38
3.2.5	Additional Constraints on Required Constructs .....	38
<b>4.0</b>	<b>STANDARDS SELECTION .....</b>	<b>39</b>
4.1	Standards .....	40
4.1.1	Regulatory Guidance .....	40
4.1.2	Selected Standards .....	41
4.1.3	Informative Reference Standards .....	43
4.2	Gaps Where There Are No Standards .....	44
4.3	Standard Overlaps .....	45



<b>5.0</b>	<b>CONFORMANCE.....</b>	<b>46</b>
5.1	Conformance Criteria .....	46
5.2	Conformance Scoping, Subsetting and Options .....	46
5.3	Test Methods .....	47
<b>6.0</b>	<b>APPENDIX .....</b>	<b>48</b>
6.1	Description of Standards .....	48
6.2	Use Case to Information Exchange and Data Requirements .....	51
6.3	Use Case Sequence Diagrams .....	56
6.4	Mapping of Constructs to Information Exchange and Data Requirements.....	63
<b>7.0</b>	<b>DOCUMENT UPDATES .....</b>	<b>65</b>
7.1	December 10, 2008 .....	65
7.1.1	Updates from Public Comment .....	65



## FIGURES AND TABLES

Figure 1.2-1 Interoperability Specification Document Map .....	8
Figure 2.2.4-1 Legend for Component Diagrams .....	20
Figure 2.2.4-2 Implementation Variants .....	21
Figure 2.2.4-3 Patient-Provider Secure Messaging Component Data Flow Diagram .....	23
Figure 3.2.2-1 Detailed Sequence Diagram for Scenario 1 .....	34
Figure 3.2.2-2 Detailed Sequence Diagram for Scenario 2 .....	35
Figure 6.3-1 Scenario 1: Patient-Initiated Communication High Level Sequence Diagram .....	57
Figure 6.3-2 Scenario 1: Secure Communication Using Two Secure Messaging Systems High Level Sequence Diagram .....	58
Figure 6.3-3 Scenario 1: Secure Communication Using a Third-Party Secure Messaging System High Level Sequence Diagram .....	59
Figure 6.3-4 Scenario 2: Clinician Initiated Communication High Level Sequence Diagram .....	60
Figure 6.3-5 Scenario 2: Secure Communication Using Two Secure Messaging Systems High Level Sequence Diagram .....	61
Figure 6.3-6 Scenario 2: Secure Communication Using a Third-Party Secure Messaging System High Level Sequence Diagram .....	62
Table 1.2.1-1 List of Constructs .....	8
Table 1.4-1 Reference Documents .....	10
Table 1.4.1-1 Glossary Term Clarifications .....	12
Table 2.2.2-1 Data Element and Information Requirements (DR) .....	16
Table 2.2.2-2 Information Exchange Requirements (IER) .....	17
Table 2.2.3-1 Business Actors .....	18
Table 3.1-1 Scoping Clarifications .....	24
Table 3.1.1-1 Assumptions .....	27
Table 3.1.2-1 Constraints .....	28
Table 3.1.3-1 Pre-conditions .....	28
Table 3.1.4-1 Post-conditions .....	29
Table 3.1.5-1 Process Triggers .....	30
Table 3.2.1-1 Technical Actor Role Descriptions .....	30
Table 3.2.2-2 Unstructured Document Metadata Requirements .....	33
Table 3.2.3-1 Business-Technical Actor Mapping to Transaction and/or Content .....	36
Table 3.2.3-2 Implementation Conditions/Constraints .....	38
Table 3.2.4-1 Construct Dependencies .....	38
Table 3.2.5-1 Additional Constraints on Required Constructs .....	38
Table 4.1.1-1 Regulatory Guidance .....	40
Table 4.1.2-1 Selected Standards Linked to HITSP Constructs .....	41
Table 4.1.3-1 Informative Reference Standards .....	43
Table 4.2-1 Use Case Requirements and Associated Standards Gaps .....	45



Table 4.3-1 Use Case Requirements and Associated Standards Overlaps.....	45
Table 6.1-1 Description of Standards .....	48
Table 6.2-1 Mapping of Use Case Actions to Information Exchange Requirements .....	51
Table 6.4-1 Mapping of Requirements to HITSP Constructs.....	63

RELEASED FOR IMPLEMENTATION



## 1.0 INTRODUCTION

As an introduction to the Healthcare Information Technology Standards Panel (HITSP) Patient-Provider Secure Messaging Interoperability Specification, this section provides a high level overview of the information sharing scenario enabled by following this specification, provides a document map of the construct relationships for the Interoperability Specification, acknowledges the copyright protections that pertain, and provides a list of key reference documents and background material.

### 1.1 INTEROPERABILITY SPECIFICATION OVERVIEW

This section provides a high level definition of this Interoperability Specification and background information about the underlying Use Case that it is based upon.

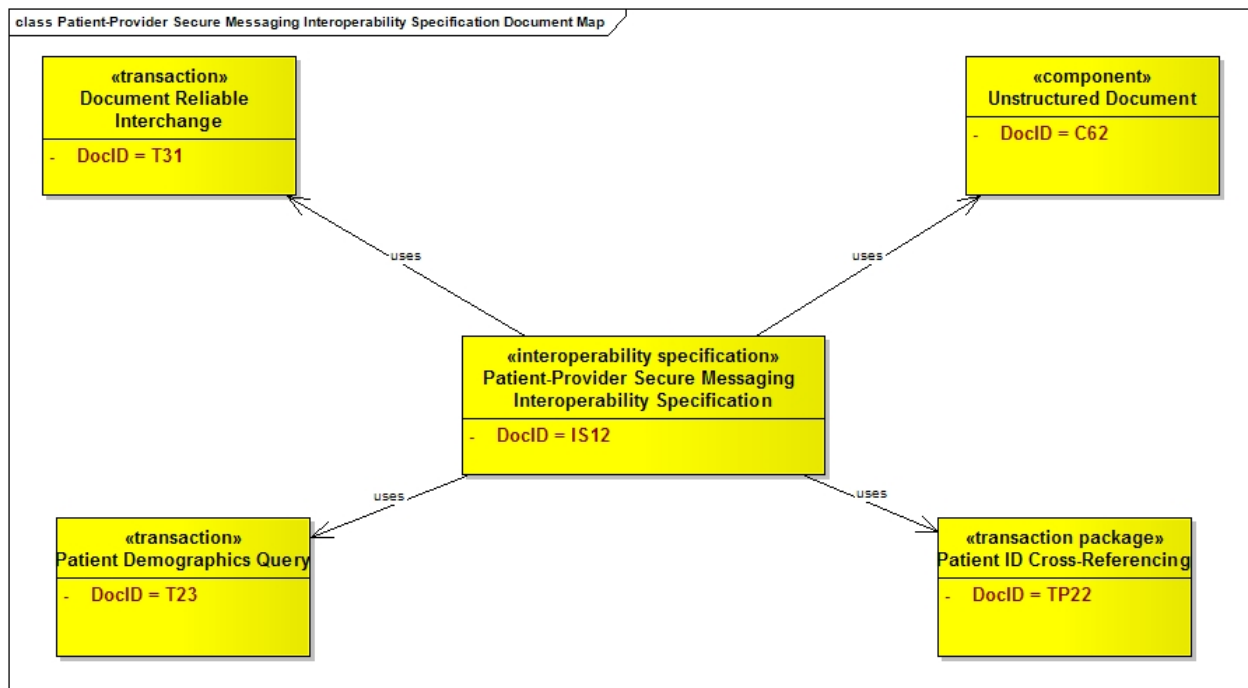
This HITSP Patient-Provider Secure Messaging Interoperability Specification describes the information flows, issues, and system capabilities that are required for patients to interact with their healthcare clinicians remotely using common computer technologies readily available in homes and other settings.

### 1.2 INTEROPERABILITY SPECIFICATION DOCUMENT MAP

Each HITSP Interoperability Specification (IS) is comprised of a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications to satisfy the requirements imposed by a given Use Case. The IS groups specific actions and actors to describe the relevant context(s) for the use of HITSP constructs that further identify and constrain standards where necessary. In addition to ISs, there are three other types of HITSP constructs called Transaction Packages (TP), Transactions (T), and Components (C). The document map in Figure 1.2-1 depicts how this IS integrates and constrains HITSP constructs to support the information exchange, within the defined context of the Use Case. Implementers should read the documents that describe the constructs depicted in the diagram for their details and specific uses. Note that the baseline Security and Privacy constructs are not shown in the diagram, however, they are described in Table 1.2.1-1.



**Figure 1.2-1 Interoperability Specification Document Map**



### 1.2.1 LIST OF CONSTRUCTS

The following table lists and describes the HITSP constructs that are used by the Interoperability Specification. All references to HITSP specifications are to the current, and Panel approved 'Released for Implementation' versions of the specifications retrieved from [www.hitsp.org](http://www.hitsp.org).

Where HITSP has adopted HL7 V3.0 CDA/CCD for conveying information between Electronic Health Record (EHR) and Personal Health Record (PHR) applications and in other healthcare scenarios, it has consolidated common constraints applied against the Content Modules in HITSP/C83 CDA Content Modules. Likewise, HITSP/C80 Clinical Document and Message Terminology maintains commonly applied terminology constraints. Readers should refer to HITSP/TN901 Technical Note for Clinical Documents to better understand how HITSP/C83 and HITSP/C80 are used by other constructs that are based upon HL7 V3.0 CDA/CCD (e.g., HITSP/C32 Summary Documents Using HL7 Continuity of Care Document (CCD), HITSP/C48 Encounter Document Using IHE Medical Summary (XDS-MS) and HITSP/C84 Consult and History & Physical Note).

**Table 1.2.1-1 List of Constructs**

Construct	Description
HITSP/C19 - Entity Identity Assertion	The Entity Identity Assertion Component provides the mechanisms to ensure that an entity is the person or application that claims the identity provided. An example of this Component is the validation and assertion of a consumer logging on to a Personal Health Record (PHR) system





Construct	Description
HITSP/C62 - Unstructured Document	The Unstructured Document Component is provided for the capture and storage of patient identifiable, unstructured document content, such as text, PDF, and images rendered in PDF. It is based on the Cross-Enterprise Sharing of Scanned Documents (XDS-SD) profile from the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF)
HITSP/T15 - Collect and Communicate Security Audit Trail	The Collect and Communicate Security Audit Trail Transaction is a means to provide assurance that security policies are being followed or enforced and that risks are being mitigated. This document describes the mechanisms to define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed
HITSP/T16 - Consistent Time	The Consistent Time Transaction provides a mechanism to ensure that all of the entities that are communicating within the network have synchronized system clocks
HITSP/T17 - Secured Communication Channel	The Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of transmissions, and the mutual trust between communicating parties. Its objectives include providing: mutual node authentication to assure each node of the others' identity; transmission integrity to guard against improper information modification or destruction while in transit; and transmission confidentiality to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes
HITSP/T23 - Patient Demographics Query	The Patient Demographics Query Transaction is intended to provide a 'list patients and their demographics' query/'patient(s) and their demographics identified' response message pair (QBP^K22, RSP^K22) for use wherever such needs exist. This Transaction document extracts the Health Level Seven (HL7) version 2.5 Query and Response data mapping. The underlying basis for this extraction can be found in the Integrating the Healthcare Enterprise IT Infrastructure Technical Framework, Patient Demographics Query integration profile
HITSP/T31 - Document Reliable Interchange	The Document Reliable Interchange Transaction provides a standards-based mechanism for conveying a set of medical documents in a point-to-point network-based communication. This Transaction uses the IHE Cross-Enterprise Document Reliable Interchange (XDR) Integration Profile, a companion to the IHE Cross-Enterprise Document Sharing (XDS) Integration Profile. Cross-Enterprise Document Reliable Interchange (XDR) uses the XDS defined metadata formats in a simpler environment in which the communicating parties have agreed to a point-to-point interchange rather than communicating via document sharing
HITSP/TP20 - Access Control	The Access Control Transaction Package provides the mechanism for security authorizations which control the enforcement of security policies including: role-based access control; entity based access control; context based access control; and the execution of consent directives. An example of this is a functional role that has the permission to perform an act (e.g., consumer updating a Personal Health Record (PHR). In an emergency, this construct must support the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents
HITSP/TP22 - Patient ID Cross-Referencing	The Patient ID Cross-Referencing Transaction Package is used for identifying and cross-referencing different attributes for the same patient. It contains a query for cross-reference and patient identity feed transactions. These transactions are used to identify patients from a list of potentials, and/or to communicate patient demographic data



Construct	Description
HITSP/TP30 - Manage Consent Directives	The Manage Consent Directives Transaction Package describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use or disclose individually identifiable health information (IIHI), and also supports the delegation of the patient's right to consent. The transactions described in this construct are intended to be carried out by HITSP/TP13 - Manage Sharing of Documents

### 1.3 COPYRIGHT PERMISSIONS

#### COPYRIGHT NOTICE

© 2008 ANSI. This material may be copied without permission from ANSI only if and to the extent that the text is not altered in any fashion and ANSI's copyright is clearly noted.

### 1.4 REFERENCE DOCUMENTS

This section provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.

A list of key reference documents and background material is provided in the table below. These documents can be retrieved from [www.hitsp.org](http://www.hitsp.org).

**Table 1.4-1 Reference Documents**

Reference Document	Document Description
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Conventions List	Describes the conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
HITSP Harmonization Framework	Describes the current framework within which the Interoperability Specifications are built
HITSP Interoperability Specification Overview	Provides background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. The document also provides a description of the HITSP process for healthcare standards harmonization and explains how to use the Interoperability Specifications and other related documents to inform your health IT system development or refinement
Patient-Provider Secure Messaging – Use Case: March 21, 2008	AHIC Use Case that is the basis of this HITSP Interoperability Specification



Reference Document	Document Description
TN900 - Security and Privacy Technical Note	<p>Developed as a reference document to provide the overall context for use of the HITSP Security and Privacy constructs. It includes the following:</p> <ul style="list-style-type: none"> <li>• The scope, reference policy background, and Security and Privacy principles used in the development of the constructs</li> <li>• A detailed description and schematics of the conceptual relationship between the Security and Privacy constructs</li> <li>• A mapping of existing standards and constructs to be used in meeting the stated requirements of the AHIC Use Cases</li> <li>• A list of identified gaps and the recommended approaches to resolving those gaps</li> <li>• A roadmap for how the Security and Privacy constructs will evolve and eventually align with other HITSP Interoperability Specifications</li> <li>• A conceptual framework for Security and Privacy management, including reference information on privacy policies, risk assessment, and risk management</li> <li>• A description of the application of the Security and Privacy constructs to the HITSP Interoperability Specifications for the three initial AHIC Use Cases – Biosurveillance, Electronic Health Records - Laboratory Results Reporting, and Consumer Empowerment</li> </ul> <p>HITSP will periodically update this Technical Note as required by the introduction of new contexts for use.</p>
TN901 - Technical Note for Clinical Documents	<p>Developed as a reference document to provide the overall context for use of the HITSP Care Management and Health Records constructs. It includes the following:</p> <ul style="list-style-type: none"> <li>• The scope, background, and principles for use in the development of the CMHR constructs</li> <li>• A detailed description and schematics of the relationship between CMHR constructs</li> <li>• A conceptual framework for the construction of clinical documents</li> <li>• An overview of Clinical Document concepts</li> <li>• An overview of Vocabulary concepts</li> </ul>

#### 1.4.1 GLOSSARY TERM CLARIFICATIONS

The following table lists HITSP Glossary Terms used by this Interoperability Specification where the meaning or intent of the term differs between the glossary and common practice. The intent of this section is not to re-define the HITSP Glossary Terms, but to point out subtle or significant differences between HITSP terms and those terms in general use within the industry segment described by this Interoperability Specification. Public comment is requested on these terms and definitions.



**Table 1.4.1-1 Glossary Term Clarifications**

Term	HITSP Glossary Definition and Clarification
Clinician	<p>HITSP Glossary V1.2 does not include the term "clinician." A proposed definition is: "Refers to a person licensed, certified, or otherwise authorized or permitted by law to administer healthcare in the ordinary course of business or practice of a profession. This includes primary care physicians, other physicians, nurse-practitioners, physician assistants, etc. The definition of a clinician is not limited by the working environment: the clinician does not have to work within a hospital or other traditional healthcare organization or facility, a clinician may provide healthcare services within any business environment and still be considered a clinician. NOTE: HL7 uses "practitioner". The term "clinician" does not include non-person entities such as healthcare facilities, clinics, hospitals, etc."</p> <p>In common use, "clinician" is often used interchangeably with "provider" or "healthcare provider." However, the HITSP use of "healthcare provider" includes non-person entities. The use of "clinician" in this Interoperability Specification is purposeful to refer to people and to exclude non-person entities.</p>
Clinician Support Staff	<p>HITSP Glossary V1.2 does not include the term "Clinician Support Staff." A proposed definition is: "Refers to a person or group of people that assist Clinicians with business and clinical workflow who are not themselves permitted to administer healthcare."</p>
Healthcare Provider	<p>HITSP Glossary V1.2: "Refers to a person authorized or permitted by law to administer healthcare. The term "provider" may also refer to healthcare facilities, clinics, hospitals, etc."</p> <p>In common use, "healthcare provider" is often used interchangeably with "clinician." However, the HITSP use of "healthcare provider" is inclusive of individuals, facilities and organizations. The use of "healthcare provider" in this Interoperability Specification is purposeful to include these non-person entities.</p>
Provider	<p>HITSP Glossary V1.2 does not include the term "provider" but does define "healthcare provider."</p> <p>This Interoperability Specification uses the terms "provider" and "healthcare provider" interchangeably. The preferred term is "healthcare provider."</p>



## 2.0 REQUIREMENTS

This section provides a high level description of the Patient-Provider Secure Messaging Use Case, as well as the specific information exchange and data requirements that are extracted from the Use Case. It includes the following information:

- Mapping from the Use Case actions and events, to the derived information exchange and data requirements – this table lists the requirements grouped by actor for each event and related action
- Data requirements – this table further describes the data requirements for each specified information exchange requirement
- Information exchange requirements – this table further describes the information exchange requirements for each applicable Use Case action
- Business Actors – this table defines the business actors that are included for the Interoperability Specification, and maps them to the applicable scenario, information exchange, and data requirements
- High Level Diagrams – these diagrams are used to describe the interaction between the business actors, and the data involved in each scenario that is documented

### 2.1 USE CASE SYNOPSIS

This section provides a synopsis of the Patient-Provider Secure Messaging Use Case, including any applicable scenarios that are part of the Use Case.

This Use Case addresses processes and information needs associated with patient-provider secure messaging. It discusses scenarios in which patients interact with their healthcare clinicians remotely using common computer technologies readily available in homes and other settings.

The broad term "patient-provider secure messaging" includes both secure messages sent from patients to providers as well as secure messages sent from providers to patients. The terms "provider", "healthcare provider" and "clinician" are sometimes used interchangeably. In this Interoperability Specification, "clinician" refers to an individual while "healthcare provider" and "provider" include individuals, facilities, organizations and other non-person entities (see Section 1.4.1 Glossary Term Clarifications).

In addition to patients and clinicians, communications could also include caregivers, family members, and patient advocates to further promote and coordinate patient care. Patients could also benefit from message based prompts and reminders, initiated by clinicians and their staff to remind patients and their advocates, of recommended events and activities that are important to maintaining and improving health. Personal health information related to these prompts and reminders would need to be provided using messages that are communicated in a secure sending and receiving environment, also known as a secured communication channel. In specific terms:



- Giving patients the ability to compose and send a secure communication to a clinician will, at times, give them access to their clinicians in a more timely and efficient manner than an office visit or a phone call
- Similarly, clinicians will benefit from having the ability to respond to or initiate secure communications to facilitate the care process and promote better patient health. This communication will be done in a manner which provides appropriate information to the patient and meets existing needs for clinical documentation
- Giving clinicians the ability to securely communicate reminders to patients and their family members will promote preventive healthcare. These reminders could include items such as annual check-ups, cancer screenings (e.g., mammograms and colonoscopies), and immunizations

When describing secure messaging, the content of messages includes information specific to a particular patient-clinician transaction. These transactions and their information content may also be made available to patients through the use of secure Internet web page access (e.g., “patient portals”). Moreover, secure messages may include message content as well as an implied process (e.g., pharmacy refill request). Therefore, these patient portal transactions accomplish secure information exchange and are within the scope of this Use Case.

Similarly, messages can include structured and unstructured content, or a combination of the two. Certain content such as adult patient age is amenable to a structure that would restrict input to a whole number of years. Other content (e.g., patient’s chief complaint) might be better served through unstructured text. Likewise, structuring methods (e.g., the use of drop-down boxes or other familiar web-based presentation techniques) may be relevant for this discussion. Similarly, “secure forms” are other tools that can provide structured support for this information exchange and would be within the scope of this Use Case. This Use Case does not attempt to prescribe the use of structured or unstructured content for any particular type of message transaction.

One of the goals of the American Health Information Community (AHIC) is establishing a pathway, based on common data standards, to facilitate the use of interoperable, clinically useful secure messaging information as a complement to, or as part of, Electronic Health Records (EHRs) to support care, clinical decision-making, promote wellness and consumer empowerment. This Use Case was developed to support the many stakeholders who are active in the development and implementation of Personal Health Records (PHRs), EHRs, and health information exchange capabilities including those engaged in activities related to standards, interoperability, harmonization, architecture, policy development, and certification.



### Scenario 1 - Patient-to-Clinician Communication:

This scenario is focused on the patient's ability to use computerized technologies that are readily available, such as secure web access, to communicate with clinicians using unstructured and structured messaging capabilities.

### Scenario 2 - Clinician-to-Patient Communication:

This scenario includes the ability of clinicians to initiate communications to the patient and respond to their communications. This scenario also includes the ability of a clinician to send relevant clinical reminders to patients regarding medical screening examinations, regular diagnostic tests, or wellness activities.

## **2.2 USE CASE REQUIREMENTS**

This section describes the Use Case requirements and outlines all the given scenarios at a high level.

The Patient-Provider Secure Messaging Use Case is simply the exchange of a message between two individuals. Whether Patient-to-Provider or Provider-to-Patient, the goal is to exchange predominately unstructured information between two people, not two systems. Incorporation of the information into systems (PHR, EHR or other) is secondary to the user's comprehension of that information. In addition, the nature of the Patient-Provider relationship requires the assumption that the message contains Protected Health Information (PHI). And PHI must be secure and protected from unauthorized access at all times. Thus the essential requirements for this Use Case are user to user message content integrity and the security of that same content.

The Use Case encompasses two scenarios: In the first scenario, the Patient creates a message intended for a designated Provider, the message is delivered to that Provider or Clinician Support Staff. After consideration and review, the Provider, or clinician support staff on behalf of the provider, creates a response back to the Patient. The Patient is notified of the new message, which they subsequently access. The second scenario is for the most part the converse of the first: The Provider, Clinician Support Staff, or an automated process triggers the creation of a message to the Patient. The Patient receives a notification, accesses the message and creates a response which is sent back to the Provider (or staff).

### 2.2.1 MAPPING OF USE CASE ACTIONS TO INFORMATION EXCHANGE REQUIREMENTS

Section 6.2 contains the perspectives, scenarios, and events from the Use Case. This section maps these events and actions to extracted Information Exchange Requirements (IER), and Data Requirements (DR) that are described in Section 2.2.2. An Information Exchange Requirements (IER) describes a requirement for information exchange between HITSP Business Actors. Data Requirements (DR) define requirements for part, or all, of the data exchanged by one or more IERs. The DR's are defined as a set of information attributes with specific details for each attribute. IER's and DR's form the basis for the construct requirements of the Interoperability Specification that are described in Section 3.





## 2.2.2 DATA AND INFORMATION EXCHANGE REQUIREMENTS

This section contains an extraction of data and information requirements (Table 2.2.2-1) and information exchange requirements (Table 2.2.2-2).

Table 2.2.2-1 provides the data requirement numbers, requirement descriptions, and a listing of the actual data elements and information that meet the data requirements. These requirements are referenced from the Data Requirements column of the Use Case Mapping Table 6.2-1 provided in Section 6.2.

**Table 2.2.2-1 Data Element and Information Requirements (DR)**

Data Requirement Number (DR)	Description
DR17	<p><b>Decision Support Data:</b> A potentially broad range of information which may be employed to evaluate a given clinical situation to suggest a course of action, or to set up criteria to trigger one or more actions when a clinical event meets those criteria</p> <p>In general, the data may include, but is not limited to:</p> <ul style="list-style-type: none"> <li>• Medication reconciliation</li> <li>• Clinical protocols</li> <li>• Administrative protocols (e.g: Insurance)</li> <li>• Diagnosis</li> <li>• Laboratory results</li> </ul>
DR27	<p><b>Message Routing and Content/Envelope/Metadata of the Secure Message, including (but not limited to):</b></p> <ul style="list-style-type: none"> <li>• Message ID</li> <li>• From (ID/name)</li> <li>• To (ID/name)</li> <li>• Subject (in the secure message, this may contain sensitive information)</li> <li>• Timestamps(s)</li> <li>• Keywords (billing, appointment, medication, allergy, to clinician, lab result – list may vary based upon provider setting) – aka "Payload type"</li> <li>• Message Priority</li> <li>• Payload ID(s)</li> <li>• Body (structured/unstructured) – may include payload by reference</li> <li>• Notes: <ul style="list-style-type: none"> <li>▪ Consider metadata requirements from SMTP, X.400, CORE Phase II, and similar</li> <li>▪ The specific metadata attributes are somewhat flexible depending on what the available constructs/standards have available</li> </ul> </li> <li>• Receipt/Delivery Request flag</li> </ul>
DR28	<p><b>Secure Message Integrity; data is provided, including (but not limited to):</b></p> <ul style="list-style-type: none"> <li>• Message integrity information (hash, etc.)</li> </ul>
DR29	<p><b>Read/Delivery Confirmation; data is provided, including (but not limited to):</b></p> <ul style="list-style-type: none"> <li>• Read/Delivery Date/Time</li> <li>• Read Receipt Confirmation</li> <li>• Delivery Receipt Confirmation</li> </ul>

Table 2.2.2-2 below contains an extraction of the Information Exchange Requirements from the Use Case. These requirements are referenced from the Information Exchange Requirements column of the Use Case Mapping Table 6.2-1 provided in Section 6.2.





**Table 2.2.2-2 Information Exchange Requirements (IER)**

Information Exchange Requirement Number (IER)	Description
IER01	<b>Provide authorization and consent</b> – Secure message system verifies authorization.
IER02	<b>Send data over secured communication channel</b> – A session oriented, synchronous, point-to-point communication channel establishing a secure path through which data can be transmitted
IER03	<b>Create audit log entry</b> – The secure message system will log that the message was sent, received or viewed. Provides assurance that security policies are being followed or enforced and that risks are being mitigated.
IER05	<b>Verify entity identity</b> – Secure message system authenticates user. Entities are asserted to assure that the entity is the person or application that claims the identity.
IER07	<b>Verify message integrity</b> – The secure message system verifies the integrity of the message
IER08	<b>Generate a delivery-receipt</b> – If requested, and if a two-system architecture is being used, the secure message system will transmit a notification that the message has been received (delivery receipt)
IER09	<b>Generate a read-receipt</b> – If requested, the secure message system will transmit a notification that the message has been accessed (read receipt)
IER10	<b>Identify patient</b> – Support for identifying, cross referencing, and query of patients NOTE: Identification of Patient (Registry Patient Id/Id Domain OID) – Leverage Entity Identity Assertion HITSP/C19 (Authenticate Consumers-Partial Gap)
IER30	<b>Compose message</b> – The secure messaging system will compose a complete message in the defined format from the required and optional information provided by the user. The output must conform. The means to create that output is not within the scope for this Use Case.
IER31	<b>Provide message routing/description information</b> – The secure messaging system will, at a minimum, prompt the User to provide necessary message routing and descriptive information (meta-data). The system will validate these elements (e.g., "address" is of the correct form, "category" is an accepted value)
IER32	<b>Request message</b> – The consumer/patient would request that the secure message be transported to their secure message system.
IER33	<b>Send/receive message</b> – In two-system architecture (both the clinician and the consumer have secure message systems). The message object is transferred via secure connection to the secure message system associated with the designated receiver. In a one-system architecture, "sending" is an internal process such as saving the message object to the receiver's "inbox", and not considered an interoperability issue, therefore <u>out of scope</u>
IER34	<b>Retrieve message 'envelope' data</b> – The systems may permit the consumer/patient to retrieve just the "envelope" information in order to assess whether the entire message is necessary
IER35	<b>Store Message into PHR</b> – For a secure message system integrated in a PHR, the message will be added to the health record for the PHR owner. For a secure message system not associated with a PHR, the PHR may have the capability to import a secure message and retain it in the health record of the PHR owner

### 2.2.3 IDENTIFICATION OF BUSINESS ACTORS MAPPED TO REQUIREMENTS

This section describes the Business Actors that impact information exchange requirements for each scenario. A Business Actor is an abstraction that is instantiated as an IT system application that a Stakeholder uses in the exchange of data needed to complete Use Case action(s); a Business Actor is not a Stakeholder. A HITSP Stakeholder is a person, organization or "personified system" that performs actions in a Use Case. Only Business Actors as an IT system are directly engaged and benefit from the



real world information exchange defined within a business Use Case action. Only Business Actors are associated with Technical Actors, which support the data exchanges of the Business Actors (see Section 3.2 for Technical Actors). The table below identifies the significant Use Case Business Actors, their descriptions, the Stakeholders they support, the Use Case scenarios, and the information exchange or data requirements for which they are used. Refer to the Use Case for a more detailed description of the listed stakeholders.

**Table 2.2.3-1 Business Actors**

Business Actor	Description	Supporting Stakeholders	Use Case Scenario	Information Exchange Requirement Numbers (IER)	Data Requirement Numbers (DR)
Personal Health Record (PHR) Systems	A healthcare record system used to create, review, annotate and maintain records by the patient or the caregiver for a patient. The PHR may include any aspect of the health condition, medications, medical problems, allergies, vaccination history, visit history or communications with healthcare providers	Patient	Patient-Provider Secure Messaging (1) Patient Initiated Communication (2) Clinician Initiated Communication	<a href="#">IER35</a> Store Message into PHR <a href="#">IER10</a> Identify Patient <a href="#">IER8</a> Generate a Delivery Receipt <a href="#">IER9</a> Generate a Read Receipt <a href="#">IER33</a> Send/Receive Message <a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER7</a> Request Message <a href="#">IER2</a> Send Data over Secured Communication Channel <a href="#">IER7</a> Verify Message Integrity <a href="#">IER3</a> Create Audit Log Entry <a href="#">IER30</a> Compose Message <a href="#">IER31</a> Provide Message Routing/Description Information <a href="#">IER34</a> Retrieve Message 'Envelope' Data	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation



Business Actor	Description	Supporting Stakeholders	Use Case Scenario	Information Exchange Requirement Numbers (IER)	Data Requirement Numbers (DR)
Electronic Health Record (EHR) System	The Electronic Health Record (EHR) System is a secure, real-time, point-of-care, patient-centric information source for clinicians	Clinician Provider Clinician Support Staff  Note: For this Use Case, individuals who support the workflow of clinicians may receive and evaluate communications from consumers or patients, and then engage the appropriate clinician in the response to the patient	Patient-Provider Secure Messaging (1) Patient Initiated Communication (2) Clinician Initiated Communication	<a href="#">IER35</a> Store Message into PHR <a href="#">IER10</a> Identify Patient <a href="#">IER8</a> Generate a Delivery Receipt <a href="#">IER9</a> Generate a Read Receipt <a href="#">IER33</a> Send/Receive Message <a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER7</a> Verify Message Integrity <a href="#">IER3</a> Create Audit Log Entry <a href="#">IER30</a> Compose Message <a href="#">IER31</a> Provide Message Routing/Description Information	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
Patient Identifier Service	An application that references a patient database for the purpose of identifying a particular patient based on one of many IDs or by matching patient demographics  NOTE: This is an element of the overall design, but not explicitly stated in the Use Case	N/A	Patient-Provider Secure Messaging (1) Patient Initiated Communication (2) Clinician Initiated Communication	N/A	N/A

#### 2.2.4 HIGH-LEVEL DIAGRAMS

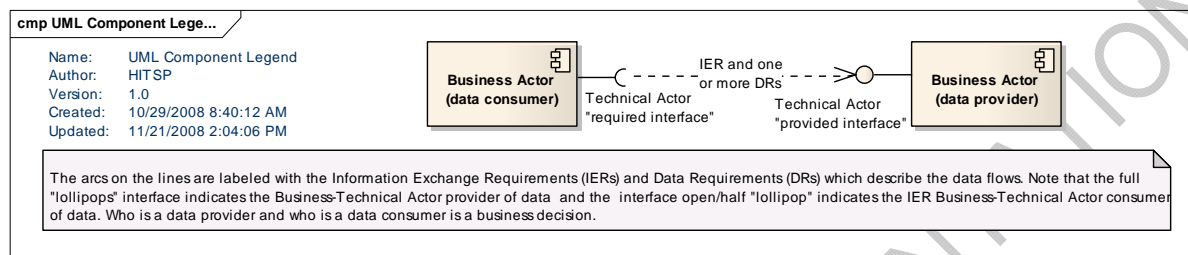
This section contains diagrams that describe the relationships and data interactions between the primary and alternative business actors and stakeholders for each Use Case scenario.

Section 6.3 provides High Level Sequence Diagrams to illustrate each Use Case scenario with a representation of a normal sequence of exchange between the primary actors.



The figures below are Component Data Flow diagrams that illustrate the data flow and information exchanges between the primary HITSP Business Actors. The information exchange and data requirement numbers from tables in Section 2.2.2 are annotated on the diagrams to show how the requirements relate to the primary actors. The in-scope requirements are supported by constructs which will be introduced in Section 3.0 of this Interoperability Specification. Figure 2.2.4-1 is a legend for reading the Component Data Flow diagrams.

**Figure 2.2.4-1 Legend for Component Diagrams**



### Implementation Variants on Business Actors and Their Relationships

During the review and analysis of the Use Case, it was recognized that several existing architectures are available to address the Use Case requirements. Three variants are shown in Figure 2.2.4 -1. Other variants may be possible; however these three demonstrate the range of possibilities.

The "As Implied in Use Case" is a literal interpretation of the Use Case. The Use Case describes the Clinician (and Support Staff) interacting with the Secure Message as a component of the EHR. The Use Case also describes the Patient as logging into the messaging system as part of the EHR. This model can be seen in current implementation of "tethered PHRs" where the Patient essentially interacts with their PHR and Secure Messaging as a component of the overall EHR.

In the secured variant "Third-Party Secure Message System," the Secure Messages are maintained in a system separate and distinct from both the PHR and EHR. In this variant, the three human actors (Patient, Provider, and Support Staff) log into the third system to create and retrieve secure messages. While it is a distinct system, accessing the Secure Messaging System may be integrated into the EHR or PHR user interface giving the appearance of a single system. In this variant, there are no interoperability requirements as there are no inter-system exchanges. Therefore, this is presented for information and not included further in this specification.

The third variant, "Two Secure Message Systems," has Secure Message capability built into both the PHR and EHR. In this variant, the Patient interacts with the PHR and its secure messaging capability, while the Clinician and Support staff interacts with the EHR and its secure messaging capability. The two messaging systems exchange messages securely between them.

In examining these variants, it is notable that almost all of the interactions depicted are user interface interactions. Only the "Two Secure Message Systems" variant requires system-to-system information exchange. In this sense, only the "Two Secure Message Systems" variant has an interoperability



requirement. With this in mind, further analysis of the Use Case requirements definition and standards selection focus solely on the "Two Secure Message Systems" scenario, with the other variants requirements (primarily vocabulary) included in this variant.

A final point on the implementation variants is that secure email is not included. While standards exist for secure email, it is not implemented in many email clients and is generally considered to be burdensome to implement. As such, secure email is not included in the variants and is not included in the design portion of this document.

**Figure 2.2.4-2 Implementation Variants**

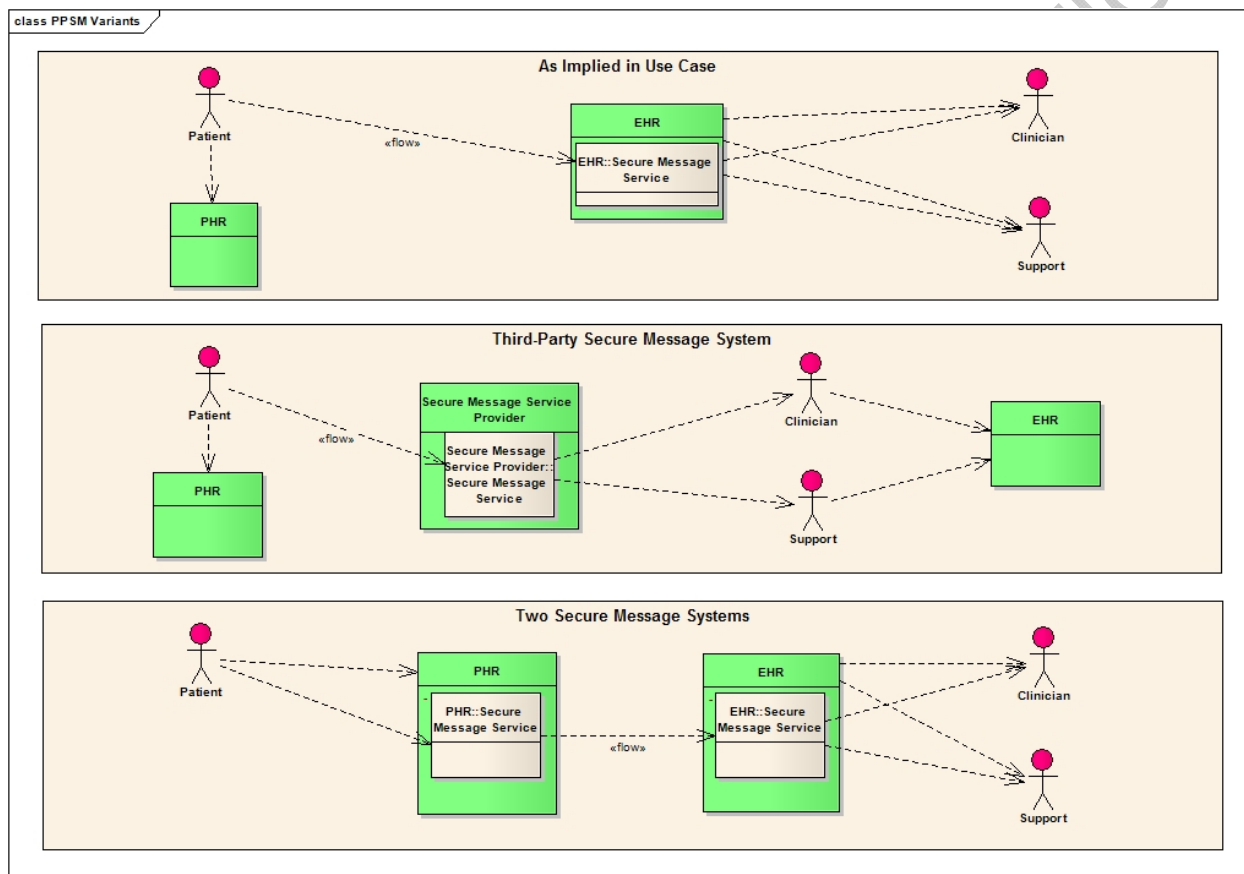


Figure 2.2.4-3 is a Component Data Flow diagram that illustrates the data flow and information exchanges between the primary actors. The information exchange and data requirement numbers from tables in Section 2.2.2 are annotated on the diagrams to show how the requirements relate to the primary actors. The in-scope requirements are supported by constructs which will be introduced in Section 3.0 of this Interoperability Specification.

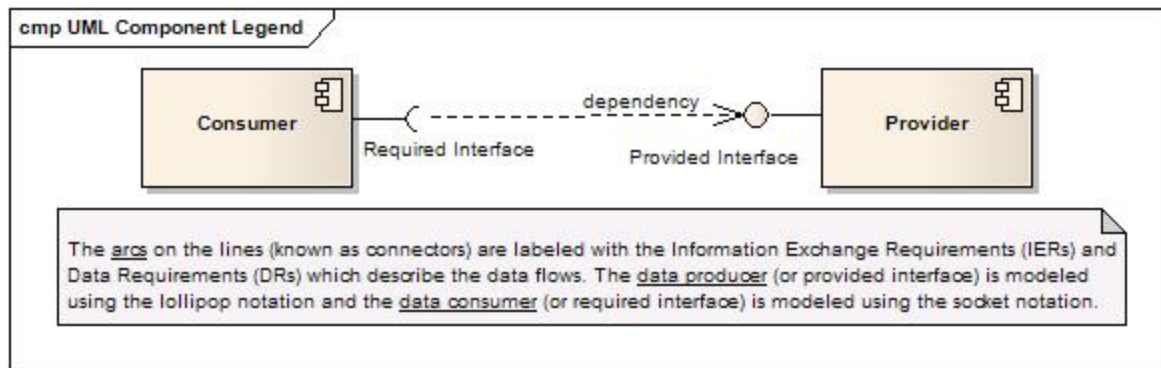
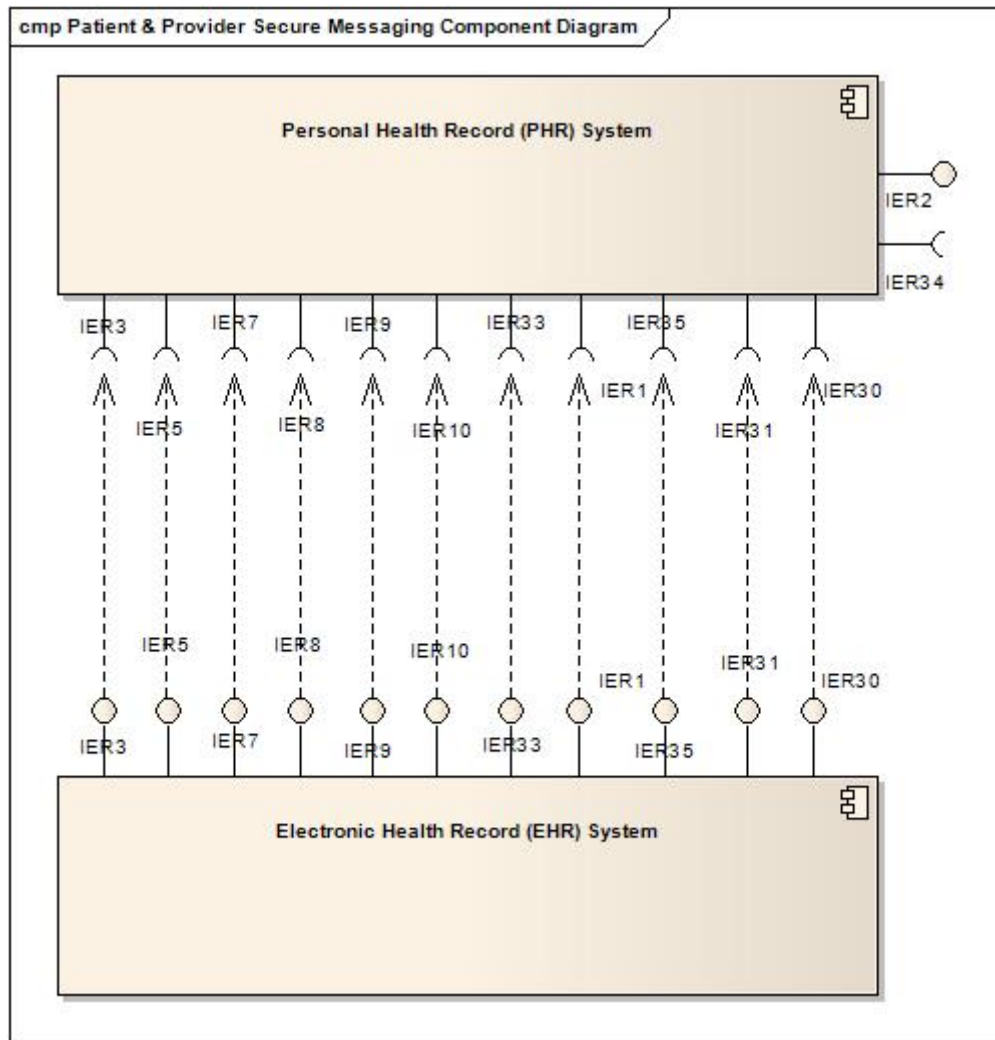


Figure 2.2.4-3 Patient-Provider Secure Messaging Component Data Flow Diagram





## 3.0 DESIGN

The design for the Interoperability Specification is the result of the requirements analysis and iterative standards selection process. This section describes the design based on the specified Business Actors and their Information Exchange and Data Requirements. It provides a detailed mapping of the specified requirements to HITSP constructs and their Technical Actors, groupings of specific Technical Actors which support Business Actors are specified to further describe the relevant interactions from existing or new HITSP constructs required for interoperability.

### 3.1 SCOPE OF DESIGN

This section describes the scope of the design as it relates to the requirements for this Use Case that were identified in Section 2.2 above. The scope identifies the assumptions that provide the boundaries for the specification and the constraints that limit the use of the specification. In addition, any pre-conditions, post-conditions and triggers that underlie the interactions between the various actors, data and transactions are provided.

Primary scoping criteria included system-to-system information exchange and end-to-end semantic interoperability. That is, requirements definition and standards application are focused on data interoperability between systems and information interoperability between end users. User interfaces, cognitive processes, internal data management, user set-up and training and workflow issues are noted, but not included in the requirements analysis. This solution supports existing best practice, and does not prohibit the use of secure email. In addition, Read Receipt is considered a system functionality issue (functional requirement of the PHR or EHR application system) and not an interoperability issue. The following table specifies those Event/Actions deemed out of scope based on these criteria.

**Table 3.1-1 Scoping Clarifications**

Scope Item	Event	Scoping Action	Recommended Resolution
1	All	Secure email is not being considered	HITSP's solution does not prohibit the use of secure email but did try to support existing best practice
2	All	Read Receipt is considered a functional requirement of the PHR or EHR system	Read Receipt is considered a system functionality issue (functional requirement of the PHR or EHR application system) and not an interoperability issue
3	All	Message Retraction	The ability to retract or recall a message is not within the scope of this Use Case
4	All	Secure messaging provides the wrapper and transport, without consideration of the content of the message itself	Aside from metadata for the message content, specification of the content contained in a Patient-Provider Secure Message is not within the scope of this Use Case
5	All	Exclude live interactions	Live interactions such as video links, instant messaging, or other similar technologies are not included in the scope of this Use Case





Scope Item	Event	Scoping Action	Recommended Resolution
6	7.1.4 Receive response 7.1.5 Update PHR 7.2.1 Receive and evaluate patient communication 7.2.2 Request clinician input 8.1.3 Receive and consider communication 8.1.4 Update PHR	Read Receipt Delivery Receipt	Delivery Receipts are not inherent in HITSP/T31 - Document Reliable Interchange, so they would have to be a system functional response, as would Read Receipts. Both would be handled, if supported by the system, as document exchanges with the "receipt" as the payload.
7	7.1.1 Establish secure messaging ability	7.1.1.3 Conduct training and other remaining set-up as needed	Specifics of training or system operation are not part of interoperability
8	7.2.1 Receive and evaluate patient communication	7.2.1.2 Evaluate patient communication	Cognitive processes are not interoperability issues
9	7.2.2 Request clinician input	7.2.2.2 Forward patient communication to clinician(s)	Internal operation or workflow is not an interoperability concern (assumes that the support and clinician are on the same system)
10	7.2.3 Formulate response	7.2.3.1 Determine appropriate clinical response	Cognitive processes are not interoperability issues
11	7.2.3 Formulate response	7.2.3.2 Compose communication response	Cognitive processes/user input are not interoperability issues  The secure messaging system will, at a minimum, prompt the consumer to provide necessary message routing and descriptive information (meta-data). The system will validate these elements (e.g., "address" is of the correct form, "category" is an accepted value)  The secure messaging system will compose a complete message (from the required and optional information provided by the consumer) in the defined format. (The output must conform, the means to create that output is not within the scope of this Use Case)
12	7.2.5 Complete information and documentation of communication event	7.2.5.1 Complete medical information related to this communication exchange	Updates to patient clinical records are not interoperability issues
13		7.2.5.2 Complete documentation of communication	Workflow processes are not interoperability issues
14	7.3.1 Evaluate clinical situation	7.3.1.1 Evaluate patient communication and clinical situation	Cognitive processes are not interoperability issues
15	7.3.2 Formulate Response	7.3.2.1 Determine appropriate clinical response	Cognitive processes are not interoperability issues



Scope Item	Event	Scoping Action	Recommended Resolution
16	7.3.4 Complete information and documentation of communication event	7.3.4.1 Complete medical information related to this communication exchange	Updates to patient clinical records are not interoperability issues
17		7.3.4.2 Complete documentation of communication	Workflow processes are not interoperability issues
18	8.1.1 Establish secure messaging ability	8.1.1.3 Conduct training and other remaining set-up as needed	Specifics of training or system operation are not part of interoperability
19	8.1.3 Receive and consider communication	8.1.3.2 Consider communication	Cognitive processes are not interoperability issues
20	8.2.1 Configure decision support for clinical reminders	8.2.1.1 Receive decision support information on clinical reminders	Receiving information from Decision Support Systems (DSS) vendor is considered out of scope, pending further work in the HITSP Technical Committee Quality Work Group
21		8.2.1.2 Incorporate decision support for clinical reminders	Internal processes for provider systems are not an interoperability issue
22	8.2.2 Trigger need for clinical reminder	8.2.2.1 Activate a clinical reminder message based on patient data	Internal trigger processes are not an interoperability issue
23	8.2.3 Communicate clinical reminder	8.2.3.1 Compose a clinical reminder	Cognitive processes are not interoperability issues The secure messaging system will, at a minimum, prompt the consumer to provide necessary message routing and descriptive information (meta-data). The system will validate these elements (e.g., "address" is of the correct form, "category" is an accepted value) The secure messaging system will compose a complete message (from the required and optional information provided by the consumer) in the defined format. (The output must conform, the means to create that output is not within the scope of this Use Case)
24	8.2.4 Complete information and documentation of communication event	8.2.4.1 Complete medical information related to this communication exchange	Updates to patient clinical records are not interoperability issues
25		8.2.4.2 Complete documentation of communication	Workflow processes are not interoperability issues
26	8.3.1 Configure decision support for clinical reminders	8.3.1.1 Receive decision support information on clinical reminders	Receiving information from DSS vendor is considered out of scope, pending further work in the HITSP Technical Committee Quality Work Groups
27		8.3.1.2 Implement decision support for clinical reminders	Internal processes for provider systems are not interoperability issues



Scope Item	Event	Scoping Action	Recommended Resolution
28	8.3.3 Complete information and documentation of communication event	8.3.3.1 Complete medical information related to this communication exchange	Updates to patient clinical records are not interoperability issues
29		8.3.3.2 Complete documentation of communication	Workflow processes are not interoperability issues

### 3.1.1 ASSUMPTIONS

This section provides an overview of the assumptions, including the circumstances, actors, policies and/or technologies that need to be in place for the design to be completed as specified. Assumptions are different from constraints which are specifically used to narrow the definition, or indicate limitations of the specified interactions.

**Table 3.1.1-1 Assumptions**

Assumption	Use Case Scenario
Providers already have secure messaging capability set up. It is not part of this specification	All
Secure messages (the composite object that includes both the "enveloping" information and any "payload" data – which may include other objects) may be persistent objects, and have an existence beyond the immediate interaction between sender and receiver The secure message (the composite object) may be persisted in the originating system The functionalities available for document management may also be applied to persistent objects	All
Notifications (the non-secure notification that a secure message is available) are transient messages in that they are not intended to persist	All
This Use Case employ's networking capabilities available to the consumer, e.g., DSL and dial-up access to Internet/World-Wide Web	All
The nature of the notification message is out of scope (e.g. an email, a phone call, a text message)	All
"Messages" between the clinician and support staff are internal operations to the EHR and not obligated to employ the Secure Messaging System. The messages would be secure as part of the EHR, but these are internal messages which are not intended to transit outside of the EHR	All
The patient and the provider are known to each other as senders and recipients of messages in this Use Case. That is, the specific addresses for each are established prior to engaging in messaging. For example, when the patient and provider first meet, various information elements are exchanged, which would also include messaging addresses (may be related to other information such as PHR identification)	All
This Use Case assumes the developing presence of electronic systems such as Electronic Health Records (EHRs), Personal Health Records (PHRs), and other local or Web-based solutions supporting consumers and clinicians, while recognizing the issues and obstacles associated with these assumptions. This approach helps promote the development of longer-term efforts	All



Assumption	Use Case Scenario
A Patient Identifier Service may be available and accessed by any of the Business Actors, in the case of an application that references a patient database for the purpose of identifying a particular patient based on one of many IDs or by matching patient demographics. This is considered an element of overall design, but is not explicitly stated in the Use Case	All
Non-electronic /non-web based notifications (e.g., phone call, SMS) are <u>not</u> excluded by this Use Case	All

### 3.1.2 CONSTRAINTS

This section describes the constraints that limit the context in which the Interoperability Specification may be used. A constraint describes a rule that limits the use of the actors, actions or data within the given context, or to which the interactions must conform to be used within the described context. It is a description of the limits and scope of the interactions and can describe actions or events that are not part of the initial definition for the context.

**Table 3.1.2-1 Constraints**

Constraint	Use Case Scenario
Appropriate computer, communication and network technologies (broadband, dial-up, WiFi) must be available to the patient. These resources may be "owned" by the patient, or acquired through other sources (e.g., work, libraries, cyber cafes/public wifi, family and friends)	All
Notifications (the non-secure notification that a secure message is available) SHALL NOT contain any PHI or information which may imply PHI or other sensitive information	All
Notifications SHALL contain sufficient information such that the recipient can access or retrieve the secured message	All

### 3.1.3 PRE-CONDITIONS

This section describes the necessary conditions that must be in place prior to the start of each scenario. The pre-conditions are used to convey any conditions that must be true at the outset of a scenario. It describes the context that must be established before the scenario is executed. They are not however the triggers that initiate a Use Case. Where one or more pre-conditions are not met, the behavior of the Use Case should be considered uncertain.

**Table 3.1.3-1 Pre-conditions**

Pre-condition	Use Case Scenario
All pre-conditions from the lower level constructs are incorporated	All
When needed, the patient is uniquely registered with the Patient Identity Cross-Referencing service	All
Patient Identities (name, demographics etc.) are known and are consistent with policies	All



Pre-condition	Use Case Scenario
Support for Provider to Health Plan transactions (HITSP/T40 - Patient Health Plan Eligibility Verification, HITSP/T68 - Patient Health Plan Authorization Request and Response, and HITSP/T85 Administrative Transport to Health Plan). These constructs are necessary to enable third-party reimbursement for the Provider-Patient interaction when the communication is a service covered by a Health Plan. In general, the Patient-Provider Secure Message is not dependent upon eligibility verification and authorization, and is therefore not included formally in this specification. In practice, the HITSP/T40, HITSP/T68 and HITSP/T85 transactions may occur outside of (or within) the workflows as described in this specification. In addition, HITSP/T40, HITSP/T68 and HITSP/T85 may be present at multiple points within the workflow, as may be dictated by Health Plan policies and requirements	All
To mitigate fraud, any unsecured electronic (web-based) notification should not contain a link directly to the secure message site	All
Appropriate virus protection software shall be installed on any computer/hardware that is participating in HITSP Patient Provider Secure Messaging Interoperability Specification	All
Support the technical measures to ensure Security and Privacy of consumer/patient health information	All
Authentication service to authenticate requestors and/or data submissions from various locations	All
Security and Privacy policies, procedures and practices are commonly implemented to support acceptable levels of consumer/patient security and privacy	All
Legal and governance issues regarding data access authorizations, data ownership, and data use are in effect	All
Support the following HITSP Security and Privacy constructs: HITSP/C19 - Entity Identity Assertion HITSP/T16 - Consistent Time HITSP/T17 - Secured Communication Channel HITSP/T15 - Collect and Communicate Security Audit Trail HITSP/TP30 - Manage Consent Directives – Capture/Request consent directive HITSP/TP20 - Access Control	All

### 3.1.4 POST-CONDITIONS

This section provides an overview of the conditions or results that must occur at the end of each scenario in order for the scenario to be deemed successfully completed. This includes any required outputs from the scenario, or specific actor states.

**Table 3.1.4-1 Post-conditions**

Post-condition	Use Case Scenario
No applicable post-conditions	

### 3.1.5 PROCESS TRIGGERS

This section describes the triggers, including actors and/or processes, which are necessary to start any scenarios, actions or events. It can be an automatic or manual process or result that in turn starts off



another scenario, action or event. A trigger is not the same as a pre-condition that describes a context that needs to be in place at the start of the event.

**Table 3.1.5-1 Process Triggers**

Process Trigger	Use Case Scenario
Patient desires to communicate to a Healthcare Provider	(1) Patient Initiated Communication
Clinician, or clinician support staff, needs to communicate to a patient	(2) Clinician Initiated Communication
Clinical Decision Support System matches criteria on a patient that indicates communication between the clinician and patient is needed	(2) Clinician Initiated Communication

## 3.2 DETAILED DESIGN

This section provides a detailed description of the technical design, along with an analysis of the main interactions and decisions between all actors, actions and data in support of the specific requirements for each scenario of the Use Case. In addition, this section provides the data element details and an overview of the HITSP constructs used to meet the business and technical requirements for this Use Case. Any variances in the Security and Privacy implementation are also described here.

Note that with respect to Security and Privacy, local implementation policy as determined by risk assessment, including assessment of jurisdictional and regulatory requirements, will determine which assurance level of nonrepudiation of origin is needed. For instance, in document-based transmissions, a low level is offered by the basic use of HITSP/TP13 Manage Sharing of Documents construct. A medium level of assurance is offered by the use of the HITSP/TP13 construct option called "Document Integrity". A high level of assurance is offered by the use of the HITSP/C26 Nonrepudiation of Origin construct which requires the existence of a Public Key Infrastructure (PKI) (See TN900 for a discussion on the challenges with PKI's).

### 3.2.1 TECHNICAL ACTOR ROLE DESCRIPTIONS

This section identifies the Technical Actors used within the Interoperability Specification. Note that a Technical Actor represents an internal software component or IT system, which supports a specific aspect of a real world business information interchange (e.g., set of message exchanges). Technical Actors implement system data exchange transactions, which support real world Business Actor information interchanges (see Section 2.2.3 for Business Actor definitions). The table below identifies the Technical Actors and provides a description of the Technical Actor roles involved in the Interoperability Specification.

**Table 3.2.1-1 Technical Actor Role Descriptions**

Technical Actor(s)	Actor Role	Construct
Access Control Service (ACS)	The enterprise security service that supports and implements user-side and/or service side access control capabilities. This service would be utilized by the Service User, and/or Service Provider	HITSP/T20



Technical Actor(s)	Actor Role	Construct
Audit Record Repository	Provides a repository for audit events	HITSP/T15
Audit Record Source	Creates and communicates an Audit Record to the Audit Record Repository on behalf of another actor that performs an action requiring logging	HITSP/T15
Consent Directive Requestor	Accesses Consent Directives located through a Consent Registry from Consent Repositories	HITSP/T30
Consent Originator	Captures consent directives and may publish the consent directive as a document. It is responsible for sending Manage Consent Directive Requests to a Consent Repository. It also supplies Metadata to the Consent Repository for subsequent registration of the Consent within a Consent Registry	HITSP/T30
Consent Registry	Responsible for providing location information and sender notification regarding consent directives. The Consent Registry receives a Manage Consent Directive Metadata Request	HITSP/T30
Consent Repository	Responsible for both the persistent storage of consent directives as well as for their registration with the appropriate Consent Registry. It assigns Metadata such as confidentiality codes to the consent directive for subsequent retrieval by an authorized consumer, e.g., for association with published personal healthcare information or for evaluation at a policy decision point	HITSP/T30
Content Consumer	A Content Consumer is responsible for viewing, import, or other processing of content created by a Content Creator	HITSP/C62
Content Creator	The Content Creator is responsible for the creation of content and transmission to a Content Consumer	HITSP/C62
Document Recipient	Receives a set of documents sent by another actor. Typically this document set will be made available to the intended recipient who will choose to either view it or integrate it into a health record	HITSP/T31
Document Source	Producer and publisher of documents. It is responsible for sending documents to a Document Repository Actor. It also supplies metadata to the Document Repository Actor for subsequent registration of the documents with the Document Registry Actor. Also used for point-to-point document exchanges	HITSP/T31
Identity Provider	Receives the credentials and identifier from the Entity (principal). It may perform authentication at that point or may require additional authentication from another source (the Service Provider)	HITSP/C19
Node	The originating or terminating point of information or signal flow in a telecommunications network. This actor is equivalent to the Secure Node in the IHE-ITI-TF ATNA Transaction	HITSP/T17
Patient Demographics Consumer	Queries the Patient Demographics Supplier for a list of patient demographic information, if any, and receives a list of corresponding patient demographic information from the Patient Demographics Supplier	HITSP/T23
Patient Demographics Supplier	Receives the query for a list of corresponding patient demographics from the Patient Demographics Consumer, sends a list of corresponding patient demographic information to the Patient Demographics Consumer, maintains one or more Patient Information Sources of patient demographics data	HITSP/T23
Patient Identifier Cross-Reference Consumer	Queries the Patient Identifier Cross-Reference Manager for a list of corresponding patient identifiers, if any and receives a list of corresponding patient identifiers from the Patient Identifier Cross-Reference Manager	HITSP/TP22





Technical Actor(s)	Actor Role	Construct
Patient Identifier Cross-Reference Manager	Receives the query for a list of corresponding patient identifiers from the Patient Identifier Cross-Reference Consumer. Sends a list of corresponding patient identifiers to the Patient Identifier Cross-Reference Consumer. Receives patient demographic information from the Patient Identity Source	HITSP/TP22
Patient Identity Source	Sends patient demographic information when requested, assigns a unique identifier to each instance of a patient, and maintains a collection of identity traits	HITSP/TP22
Service Provider	Represents the system providing a service to all entities that need an assertion or authentication. The service (or assertion) provider is the trusted third party issuer of the trustable identity assertion	HITSP/C19 HITSP/TP20
Service User	The entity represents any individual entity (such as a clinician or an EHR/PHR system) that needs to make a service request of a Service Provider. The Entity may also be known as a principal and/or entity, which represents an end user, an application, a machine, or any other type of entity that may act as a requester in a transaction. A principal is typically represented in a transaction with a digital identity and the principal may have multiple valid digital identities to use with different transactions	HITSP/C19 HITSP/TP20
Time Client	Establishes time synchronization with one or more Time Servers using the NTP protocol and either the Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) algorithms. Maintains the local computer system clock synchronization with Coordinated Universal Time (UTC) based on synchronization with the Time Servers	HITSP/T16
Time Server	Provides Network Time Protocol (NTP) time services to Time Clients. It is either directly synchronized to a Coordinated Universal Time (UTC) master clock (e.g. satellite time signal) or is synchronized by being grouped with a Time Client to other Time Server(s)	HITSP/T16

### 3.2.2 CONSTRUCT REQUIREMENTS

This section incorporates the comprehensive business and technical requirements and a detailed specification of the transactions and information content specified to complete the information exchange actions identified in each Use Case scenario.

Table 6.4-1 (see Section 6.0) provides a mapping of the HITSP constructs that will be used in the design of the Interoperability Specification, and the data and information exchange requirements that are being satisfied by the construct. The requirements are limited to those that are deemed within scope for this Interoperability Specification, which are described in Section 3.1. Further details about the required technical actors, transactions, and content are also provided in the sections below.

The Unified Modeling Language (UML) sequence diagrams used in this section incorporate the detailed data requirements for the selected standards (defined in Section 2.2.2), with the Technical Actors, and their specific and detailed Transactions and content (encapsulated in the HITSP constructs listed above). The detailed actor Transactions described in these diagrams show all common or independent technical actors, data, and the specific transactions from the HITSP constructs that are used for the Interoperability Specification.





Transactions that make use of existing HITSP constructs are shown explicitly, indicating opportunities for reuse.

The detailed applications of the main HITSP constructs required by this specification are shown in the steps below. Note that the Technical Actor 'Document Source' represents the Business Actor of Secure Messaging System when sending a message. When receiving a message, the Document Consumer or Document Recipient Technical Actors represents the Secure Messaging System Business Actor.

1. The Patient's Secure Messaging System (Document Source) creates the message as a HITSP/C62 Unstructured Document, with metadata containing all of the special data requirements shown below:

**Table 3.2.2-2 Unstructured Document Metadata Requirements**

Data Element	Value
Message ID/Payload ID	XSDSDocumentEntry.uniqueID
From (ID/name?)	XSDSDocumentEntry.Author
To (ID/Name?)	IntendedRecipient <sup>1</sup>
Subject (in the secure message, this may contain sensitive information)	XSDSDocumentEntry.Title
Timestamp(s)	XSDSDocumentEntry.CreationTime
Keywords	XSDSDocumentEntry.ClassCode
Message Priority	XSDSDocumentEntry.EventCodeList
Confidentiality Code <sup>2</sup>	XSDSDocumentEntry.ConfidentialityCode
--indicates that this is a C62 Unstructured Document (simple text message) --	XSDSDocumentEntry.FormatCode

2. For Point-to-Point Document communications environments
  - a. The PHR Secure Messaging System (Document Source) communicates this document using HITSP/T31 Document Reliable Interchange point-to-point document sharing directly to the Provider's Secure Messaging System (Document Recipient) with appropriate security, and consent checking. Note that any other documents of interest may also be included in the same submission.
  - b. The location of the Provider's Document Recipient is based on pre-configuration of the relationship between Provider/Patient.
  - c. The reception by the Provider's Document Recipient would then trigger the functional routing and alerting of the Provider. The Provider's Secure Messaging System is responsible for providing a way for the Provider to view and/or respond to a message.

<sup>1</sup> The IntendedRecipient metadata attributes is associated with the SubmissionSet entry, whereas all of the other metadata attributes are associated with the XSDSDocument entry

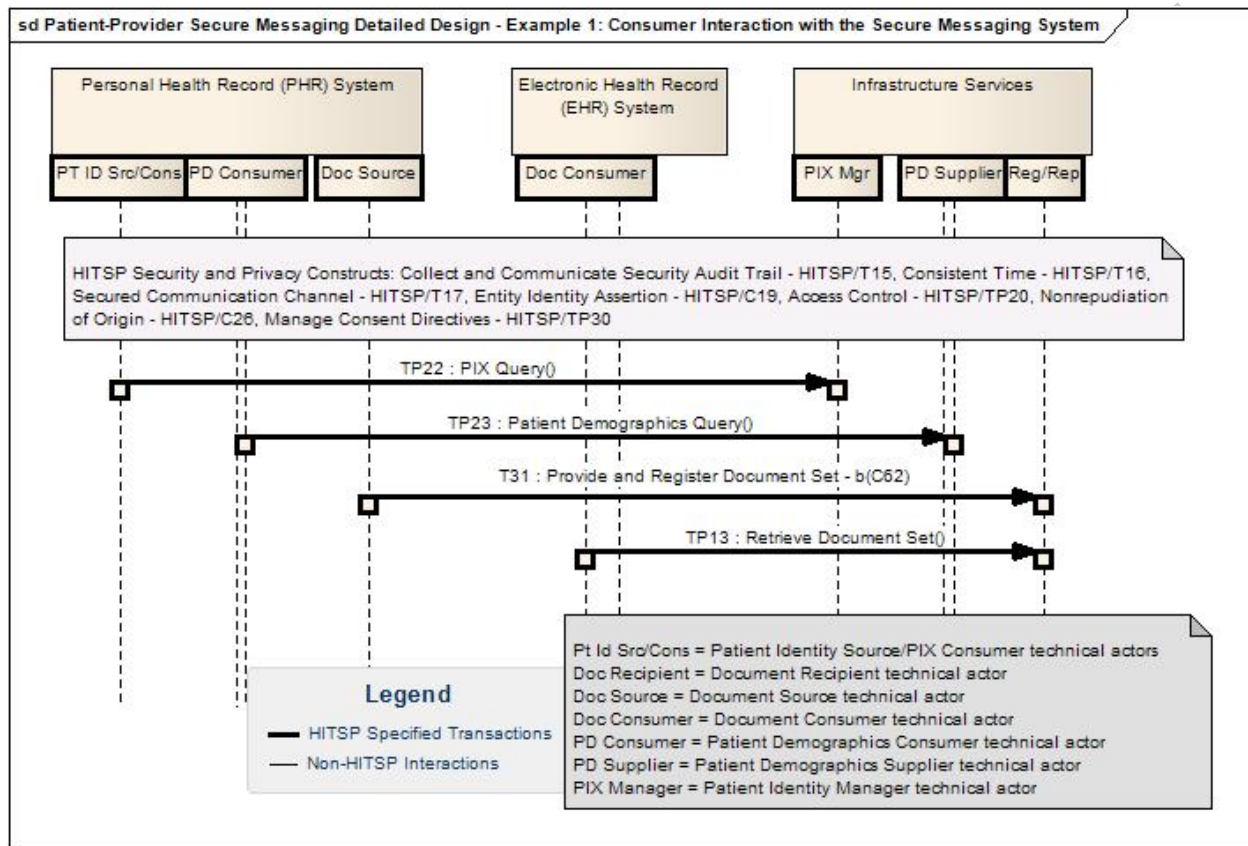
<sup>2</sup> Inclusion of support for a "For Clinician Eyes Only" indication on messages containing very sensitive patient information is addressed using the Confidentiality Code.



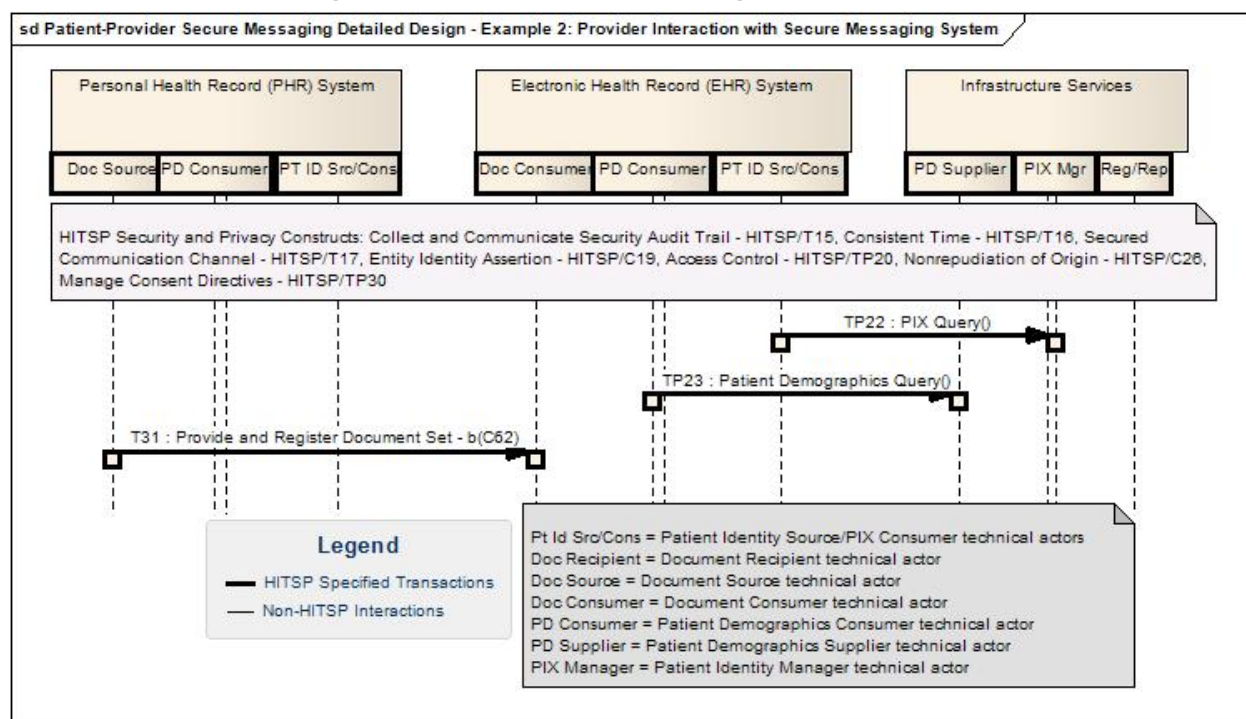
- d. The communication from the Provider to the Patient utilizes the same flow as above.

These main primary HITSP constructs, along with additional constructs provided in Table 3.2.3-1 are further illustrated in the UML diagram below.

**Figure 3.2.2-1 Detailed Sequence Diagram for Scenario 1**



**Figure 3.2.2-2 Detailed Sequence Diagram for Scenario 2**



### 3.2.3 MAPPING OF BUSINESS ACTORS TO TECHNICAL ACTORS AND CONSTRUCTS WITH OPTIONALITY

The table below maps the individual business actors to the technical actors defined in the Interoperability Specification and depicted in the above detailed UML sequence diagram. Table 3.2.3-1 below specifies the requirements associated with each business actor in the Interoperability Specification. For each implemented business actor, the table specifies the following:

1. All Required or Conditionally Required technical actors listed for the business actor shall be supported as specified in the associated construct
2. Optional technical actors listed for the business actor may be supported as specified in the associated construct
3. All Required or Conditionally Required transactions and content subsets listed for each implemented technical actor assigned to the business actor shall be supported as specified in the associated construct
4. Optional transactions and content subsets listed for each implemented technical actor assigned to the business actor may be supported as specified in the associated construct

This table also includes the corresponding technical actors associated with the relevant Security and Privacy constructs that are used for this Interoperability Specification. Section 1.2 provides a summary description of all the referenced HITSP constructs. Note that this table only shows the business and technical actors that are implemented by the specification. Business actors that are out of scope, or gaps



are not included in this section, however, they are discussed in Section 3.1 if they are out of scope, or in Section 4.2 if they are found to be gaps where there are no standards.

**Table 3.2.3-1 Business-Technical Actor Mapping to Transaction and/or Content**

Business Actor	Technical Actor(s)	Actor Optionality	Construct	Transaction/Content	T/C Optionality <sup>3</sup>
Electronic Health Record (EHR) System	Document Recipient	R	HITSP/T31	Provide & Register Document Set-b (online mode)	R
			HITSP/C19	Convey Assertion	O
	Document Source	R	HITSP/T31	Provide & Register Document Set-b (online mode)	R
			HITSP/C19	Convey Assertion	O
	Patient Identifier Cross Reference Consumer	C <sup>[105]</sup>	HITSP/TP22	PIX Query	R
	Patient Demographics Consumer	C <sup>[105], [106]</sup>	HITSP/T23	Patient Demographics Query	R
	Audit Record Source	C <sup>[104]</sup>	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Content Consumer	R	HITSP/TP30	Consent Document	R
			HITSP/C62	Unstructured Document	R
	Time Client	C <sup>[104]</sup>	HITSP/T16	Maintain Time	R
	Node	C <sup>[104]</sup>	HITSP/T17	Secured Communication Channel	R
	Consent Directive Requester	C <sup>[104]</sup>	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	Service User	R	HITSP/TP20	Access Control Request	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Access Control Service (ACS)	R	HITSP/TP20	Access Control Request	O
	Service Provider (SP)	R	HITSP/TP20	Access Control Request	O
Personal Health Record (PHR) Systems	Document Source	R	HITSP/T31	Provide & Register Document Set-b (online mode)	R
			HITSP/C19	Convey Assertion	O
	Document Recipient	R	HITSP/T31	Provide & Register Document Set-b (online mode)	R
			HITSP/C19	Convey Assertion	O
	Patient Identity Source	C <sup>[105]</sup>	HITSP/TP22	Patient Identity Feed	R
	Patient Identifier Cross-Reference Consumer	C <sup>[105]</sup>	HITSP/TP22	PIX Query	R
				PIX Update Notification	O

<sup>3</sup> Optionality = "R" for Required, "O" for Optional, or "C" for Conditional



Business Actor	Technical Actor(s)	Actor Optionality	Construct	Transaction/Content	T/C Optionality <sup>3</sup>
	Patient Demographics Consumer	C <sup>(105)</sup>	HITSP/T23	Patient Demographic Query	R
	Content Creator	R	HITSP/TP30	Consent Document	O
		R	HITSP/C62	Unstructured Document	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Consent Originator	O	HITSP/TP30	Provide and Register Document Set	R
	Consent Directive Requester	R	HITSP/TP30	Registry Stored Query	R
				Retrieve Document Set-b	R
	Service User	R	HITSP/TP20	Access Control Request	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Access Control Service (ACS)	R	HITSP/TP20	Access Control Request	O
	Service Provider (SP)	R	HITSP/TP20	Access Control Request	O
Patient Identifier Service	Patient Identifier Cross - Reference Manager (PIX Manager)	R	HITSP/TP22	PIX Query	R
				Patient Identity feed	R
				PIX Update Notification	R
	Patient Demographics Supplier	R	HITSP/T23	Patient Demographics Query	R
	Consent Repository	O	HITSP/TP30	Register Document Set	R
				Provide and Register Document Set	R
				Retrieve Document	R
	Consent Registry	O	HITSP/TP30	Registry Stored Query	R
				Register Document Set	R
	Consent Originator	O	HITSP/TP30	Provide and Register Document Set	R
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O

### Implementation Conditions/Constraints

The following table describes the implementation conditions or constraints placed on the technical actors, transactions, or content. The constraint codes listed below correspond to the codes placed in the Actor and Transaction/Content optionality column in Table 3.2.3-1 above. For example, the Patient



Demographics Consumer Technical Actor has an optionality code of C<sup>[105]</sup> <sup>[106]</sup> which represents a conditionally required actor with the constraint codes of 105 and 106 described in the table below.

**Table 3.2.3-2 Implementation Conditions/Constraints**

Constraint Code	Constraint Description
104	Shall be grouped with Document Consumer when implemented
105	Shall support Patient Identity Source plus PIX Consumer and/or Patient Demographics Consumer
106	Shall only be implemented when supporting a Document Consumer Technical Actor

### 3.2.4 CONSTRUCT DEPENDENCIES

The following table shows a list of constructs with their existing dependencies. Dependencies usually exist when there are some additional pre-requisites for a specific construct. To support a dependent construct, a technical actor must implement all the required actions in the pre-requisite construct, or be grouped together with another construct as specified in the table below.

**Table 3.2.4-1 Construct Dependencies**

Construct	Depends On (Name of construct that it depends on)	Dependency Type (Pre-condition, Post-condition, General)	Purpose (Reason for this dependency)
No applicable construct dependencies			

### 3.2.5 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

This section describes the constraints that further limit the constructs that are used by this Interoperability Specification.

**Table 3.2.5-1 Additional Constraints on Required Constructs**

Data Element	Construct	Constraint	Constraint Type (Pre-condition, Post-condition, General)	Purpose (Reason for this constraint)
No applicable additional constraints				





## 4.0 STANDARDS SELECTION

This section presents the standards required to support each major Use Case event. Standards selection is based on the following process:

- **Evaluation:** The Technical Committee evaluates the standards using the Tier 2 Readiness Criteria.
- **Selection:** Based on the Tier 2 evaluations, named standards are selected and listed in the table of selected standards below. It is important to understand that the standards selected here are within the context of the specific Use Case requirements and do not necessarily reflect selection in other contexts
- **Gap and Overlap Analysis and Recommendations:** The Technical Committee also identifies and analyzes gaps and overlaps within the standards industry as they relate to the specific Use Case. The Technical Committee provides a description of the gaps, including missing or incomplete standards, a description of all overlaps, or competition among standards for the relevant Use Cases, and recommendations for resolving these gaps and overlaps

It is HITSP's policy to incorporate only standards that have been approved according to the formal policy of the standards organization, as defined by HITSP, which publishes the standard. HITSP interprets approval to include Draft Standards for Trial Use. The objective is to incorporate only standards that are managed within a formal life cycle process as defined by the standards organization. In some cases, where we believe a standard that is not yet approved may best meet the requirements of an Interoperability Specification, HITSP may provide a roadmap of its future intent conditional on future actions by either or both the standards organization and the HITSP Technical Committee. Thus there are four classes of HITSP-committed standards.

- **Approved for Use** – standards included for unconditional use within a HITSP construct
- **Interim** – standards included for use now within a HITSP construct but for a defined time period or conditional on future actions, e.g., "Intended for Use" standard is available
- **Provisional** - standards that are not yet but are expected to be approved by the standards organization at the time the Interoperability Specification is released by HITSP. A "Provisional" standard becomes an "Approved for Use" standard only if:
  - It is approved by the Standards Organization by the time that the Interoperability Specification is released by HITSP and
  - It is substantially the same as it was when it was provisionally used and
  - It requires no further action by the Technical Committee
- **Intended for Use** – proposed standards that are roadmapped for future use pending actions by the Technical Committee and/or the standards organization. Therefore a standard is defined as "Intended for Use" if it will not be approved by the standard organization at the time that the HITSP construct is released, but is sufficiently defined to enable detailed evaluation of how well it will meet technical and information exchange requirements.



HITSP may continue to use “Provisional” or “Interim” standards as they existed when incorporated into the HITSP construct if the expected conditions are not satisfied until such time as HITSP can replace it with a more suitable standard. In this circumstance, the standards organization would have no responsibility to maintain or correct this artifact. If a standard “Intended for Use” is not developed and approved in terms of time frame or content as expected by the Technical Committee at the time of its initial selection, it may be replaced. All standards used by HITSP must meet the HITSP selection criteria. The use of “Interim” and “Intended for Use” standards will be weighed against the alternative of simply declaring a gap for HITSP and the standards organizations to resolve.

## 4.1 STANDARDS

It is important to understand that the standards selected here are within the context of the specific Use Case requirements and do not necessarily reflect selection in other contexts. In addition, adherence to the selected standards alone is not sufficient to ensure interoperability. In order to ensure interoperability for the Use Case, and to claim conformance to the specification, an implementation must satisfy all the requirements and mandatory statements listed in the HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards. A conformant system must also be constrained as specified in Table 3.1.2-1, and implement all of the required technical actors from Table 3.2.3-1, within the scope and implementation subset that is selected.

The standards used by this Interoperability Specification fall into the following categories:

- Regulatory guidance is a legal or other authoritative declaration that HITSP must abide by in standards selection (see Section 4.1.1)
- Selected standards are necessary for interoperability. These are standards that are used to meet information exchange requirements of associated constructs. For example, they are used to realize direct information exchange, to provide the transport mechanism, to specify the content, or to address security (see Section 4.1.2)
- Informative reference standards provide additional background information or guidance, and are not required for interoperability. These standards are not required to implement the Interoperability Specification (see Section 4.1.3)

### 4.1.1 REGULATORY GUIDANCE

The following table provides a list of legal or other authoritative guidelines that HITSP must abide by, or has agreed to use as guidance in the selection of standards. Note that only the referenced sections of the regulations are relevant to this Interoperability Specification.

**Table 4.1.1-1 Regulatory Guidance**

Regulation	Description
For Regulatory and Guidance Standards relating to the Security and Privacy of Health Information, please see HITSP/TN900 Security and Privacy Technical Note	The HITSP/TN900 document is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs. It also includes a set of overarching principles and concepts, derived from an analysis of major federal and common state laws and regulations





#### 4.1.2 SELECTED STANDARDS

The following table provides a list of standards that are used to meet information exchange requirements of the Interoperability Specification, and the HITSP constructs that use each standard. A detailed description of each standard is also provided in Section 6.0 Appendix.

Note that the standards selected for this Interoperability Specification are approved for use as defined in Section 4.0 above.

**Table 4.1.2-1 Selected Standards Linked to HITSP Constructs**

Standard	HITSP Construct	Remarks/ Minor Gaps
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	HITSP/TP20 - Access Control	
Health Level Seven (HL7) Version 2.3.1 Chapter 2 – Control, Chapter 3 – Patient Administration	HITSP/TP22 - Patient ID Cross-Referencing	
Health Level Seven (HL7) Version 2.5, Chapter 2 – Control, Chapter 3 – Patient Administration, Chapter 5 - Query	HITSP/TP22 - Patient ID Cross-Referencing HITSP/T23 - Patient Demographics Query	
Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise User Assertion (XUA) Integration Profile	HITSP/C19 - Entity Identity Assertion	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) – Revision 5.0 or later, Cross Enterprise Sharing of Scanned Documents (XDS-SD) Integration Profile	HITSP/C62 - Unstructured Document	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile	HITSP/T15 - Collect and Communicate Security Audit Trail	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	HITSP/T17 - Secured Communication Channel	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Consistent Time (CT) Integration Profile	HITSP/T16 - Consistent Time	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 or later, Patient Demographics Query (PDQ) Integration Profile	HITSP/T23 - Patient Demographics Query	



Standard	HITSP Construct	Remarks/ Minor Gaps
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2008 - 2009, Pediatric Demographics, Draft for Trial Implementation (August 22, 2008)	HITSP/T23 - Patient Demographics Query HITSP/TP22 - Patient ID Cross-Referencing	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) 2007-2008 Trial Implementation Supplement Cross-enterprise Document Reliable Interchange (XDR) Release 3	HITSP/T31 - Document Reliable Interchange	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Patient Identifier Cross-Referencing (PIX) Integration Profile	HITSP/TP22 - Patient ID Cross-Referencing	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a) Integration Profile	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 - 2008 Cross-Enterprise Document Sharing-B (XDS.b) Integration Profile	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) Integration Profile - Trial Implementation	HITSP/TP30 - Manage Consent Directives	
International Organization for Standardization (ISO) PDF/A ISO 19005-1b. Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF (PDF/A)	HITSP/C62 - Unstructured Document	
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	HITSP/T16 - Consistent Time	
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996	HITSP/T16 - Consistent Time	
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) Core V2.0 OASIS Standard; ITU-T X.1141	HITSP/TP20 - Access Control	



Standard	HITSP Construct	Remarks/ Minor Gaps
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	HITSP/TP20 - Access Control	
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	HITSP/TP20 - Access Control	

#### 4.1.3 INFORMATIVE REFERENCE STANDARDS

The following table lists standards that provide additional background information or guidance; however, they are not required for the implementation of the Interoperability Specification.

**Table 4.1.3-1 Informative Reference Standards**

Standard	Description
American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS), #359-2004	This standard describes RBAC features that have achieved acceptance in the commercial marketplace. It includes a reference model and functional specifications for the RBAC features defined in the reference model. It is intended for (1) software engineers and product development managers who design products incorporating access control features; and (2) managers and procurement officials who seek to acquire computer security products with features that provide access control capabilities in accordance with commonly known and understood terminology and functional. For more information visit <a href="http://www.ansi.org">www.ansi.org</a> .
ASTM International Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems: # E2147-01	E2147-01 "is for the development and implementation of security audit/disclosure logs for health information. It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of health information to external users for use in manual and computer systems. The process of information disclosure and auditing should conform, where relevant, with the Privacy Act of 1974 (1)." For more information visit <a href="http://www.astm.org">www.astm.org</a> .
Health Level Seven (HL7) Consent related vocabulary including Confidentiality Codes	HL7 concept domains, including ConfidentialityCodes, ActInformationCategoryCode, ActInformationAccessType, ActInformationAccessContextCode, AuthorizedParticipationFunctionCode, ActPolicyType, ActConsentType, and ActMaskableCode For more information visit <a href="http://www.hl7.org">www.hl7.org</a> .
Health Level Seven (HL7) Version 3.0 Clinical Document Architecture (CDA) Release 2.0	The HL7 Clinical Document Architecture is an XML-based document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA is one instantiation of HL7's Version 3.0 Reference Information Model (RIM) into a specific message format. Of particular focus for HITSP Interoperability Specifications are message formats for Laboratory Results and Continuity of Care (CCD) documents. Release 2 of the HL7 Clinical Document Architecture (CDA) is an extension to the original CDA document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA R2 includes a prose document in HTML, XML schemas, data dictionary, and sample CDA documents. CDA R2 further builds upon other HL7 standards beyond just the Version 3.0 Reference Information Model (RIM) and incorporates Version 3.0 Data Structures, Vocabulary, and the XML Implementation Technology Specifications for Data Types and Structures. For more information visit <a href="http://www.hl7.org">www.hl7.org</a> .



Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> .
International Organization for Standardization (ISO) Health Informatics -- Information technology -- Open Systems Interconnection -- Systems Management: Security alarm reporting function, Technical Specification #10164-- Part 7: Security Alarm Reporting Function, 1992	Establishes user requirements for the service definition needed to support the security alarm reporting function, defines the service provided by the security alarm reporting function, specifies the protocol that is necessary in order to provide the service, defines the relationship between the service and management notifications, defines relationships with other systems management functions, specifies conformance requirements. The security alarm reporting function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information for the purpose of systems management. For more information visit <a href="http://www.iso.org">www.iso.org</a> .
Internet Engineering Task Force (IETF) Tags for the Identification of Languages, "Request for Comment" (RFC) #3066, January, 2001	Describes a language tag for use in cases where it is desired to indicate the language used in an information object, how to register values for use in this language tag, and a construct for matching such language tags. For more information visit <a href="http://www.ietf.org">www.ietf.org</a> .
Internet Engineering Task Force (IETF) The application/pdf Media Type (RFC 3778)	PDF, the 'Portable Document Format', is a general document representation language that has been in use for document exchange on the Internet since 1993. This document provides an overview of the PDF format, explains the mechanisms for digital signatures and encryption within PDF files, and updates the media type registration of 'application/pdf'. For more information visit <a href="http://www.ietf.org">www.ietf.org</a> .
Organization for the Advancement of Structured Information Standards (OASIS) Web Services Security SOAP Message Security Version 1.0	Describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies. This specification also provides a general-purpose mechanism for associating security tokens with message content. No specific type of security token is required, the specification is designed to be extensible (i.e.. support multiple security token formats. Additionally, this specification describes how to encode binary security tokens, a framework for XML-based tokens, and how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the tokens that are included with a message. For more information visit <a href="http://www.oasis-open.org">www.oasis-open.org</a> .
Organization for the Advancement of Structured Information Standards (OASIS) Simple Object Access Protocol (SOAP) Version 1.1	SOAP is a protocol specification for invoking methods on servers, services, components and objects. SOAP codifies the existing practice of using XML and HTTP as a method invocation mechanism. The SOAP specification mandates a small number of HTTP headers that facilitate firewall/proxy filtering plus an XML vocabulary that is used for representing method parameters, return values, and exceptions." {DevelopMentor} SOAP consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. For more information visit <a href="http://www.oasis-open.org">www.oasis-open.org</a> .

## 4.2 GAPS WHERE THERE ARE NO STANDARDS

This section describes gaps in standards. Gaps occur in the following two cases, where HITSP has:

- Identified requirements derived from the context that have no standards that meet all tiers of HITSP criteria to merit selection for that context
- Identified a single standard that encompasses and singly fulfills a set of tightly-coupled standards from the given context, yet is lacking in fulfilling one or more of the tightly-coupled requirements



The gap is only relative to the specific Use Case requirement. Recommended resolutions were developed through a series of steps including the Technical Committee's initial recommendations, cross Technical Committee validation of the gap, provisional recommendations and peer review by the Technical Committee.

The table below identifies the Use Case requirements and known associated gaps, along with the recommended resolutions.

**Table 4.2-1 Use Case Requirements and Associated Standards Gaps**

Requirement Number	Summary Description	Identified Gaps	Recommended Resolution
<a href="#">IER33</a> Send/Receive Message	Receive unsecured notification of secure message	This Use Case would be simplified if the Secure Messaging Systems could subscribe for notifications of new message documents	There is a need for a HITSP construct to allow for the subscription requirement. IHE is working on a white paper on the topic. Solution is the same as that being implemented by the NHIN
<a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity	Secure messaging system authenticates user and verifies authorization	Partial gap for HITSP/C19 - Entity Identity Assertion	A work item exists in the HITSP Security, Privacy & Infrastructure Domain Technical Committee to address the authentication of individuals, and specifically consumers
<a href="#">IER9</a> Generate a Read Receipt <a href="#">IER8</a> Generate a Delivery Receipt <a href="#">DR29</a> Read/Delivery Confirmation	If requested, system will transmit a notification that the message has been accessed (Read Receipt)	Read Receipt is not supported at this time by HITSP/T31 - Document Reliable Interchange. In addition, this may be a system functionality issue (functional requirement of the PHR or EHR application system) and not an interoperability issue	A work item exists in the HITSP Security, Privacy & Infrastructure Domain Technical Committee to consider adding "Read Receipt" interactions to HITSP/T31

#### 4.3 STANDARD OVERLAPS

This section describes the instances where there are overlaps among standards for the Use Case requirements. The overlap is only relative to the specific Use Case requirement. Overlaps refer to instances wherein some of the requirements are met by multiple standards. Recommended resolutions were developed through a series of steps including the Technical Committee's initial recommendations, cross Technical Committee validation of the overlap, provisional recommendations and peer review by the Technical Committee's.

The table below presents the identified overlaps and the respective resolution plans.

**Table 4.3-1 Use Case Requirements and Associated Standards Overlaps**

Requirement Number	Summary Description	Standard Overlap	Recommended Resolution
No applicable overlaps			



## 5.0 CONFORMANCE

This section describes the conformance criteria, which are objective statements of requirements that can be used to determine if a specific behavior, function, interface, or code set has been implemented correctly.

### 5.1 CONFORMANCE CRITERIA

In order to claim conformance to the specification, an implementation must satisfy all the requirements and mandatory statements listed in the HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards. A conformant system must be constrained as specified in Table 3.1.2-1, and implement all of the required actors from Table 3.2.3-1, within the scope, subset or implementation option that is selected from Section 5.2 below.

Claims of conformance to this specification must be made using the following language:  
This product conforms to the HITSP Patient-Provider Secure Messaging Interoperability Specification, available at [www.hitsp.org](http://www.hitsp.org).

### 5.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

A HITSP Interoperability Specification can be implemented for individual business actors defined in the Interoperability Specification. An implementation claiming conformance to a specific business actor from the Interoperability Specification shall support all of the requirements associated to that business actor as described in Table 3.2.3-1.

This means that **for each implemented business actor**:

1. All Required or Conditionally Required technical actors listed for the business actor shall be supported as specified in the associated construct
2. Optional technical actors listed for the business actor may be supported as specified in the associated construct
3. All Required or Conditionally Required transactions and content subsets listed for each implemented technical actor assigned to the business actor shall be supported as specified in the associated construct
4. Optional transactions and content subsets listed for each implemented technical actor assigned to the business actor may be supported as specified in the associated construct

Implementers of this Interoperability Specification who follow the principles listed above are being provided a level of implementation flexibility, while maintaining interoperability.



### 5.3 TEST METHODS

HITSP relies on the conformance test methods, test tools and other test-related material produced by, or under the auspices, of standards developers, profiling organizations and implementation guide producers as part of its collaborative implementation testing effort. Efforts to produce conformance test methods, tools, etc. may be internal to the organization, or provided by an external organization.

A Health Information Technology (HIT) Implementation Testing website has been developed in collaboration with HITSP, the National Institute of Standards and Technology (NIST), the Certification Commission for Healthcare Information Technology (CCHIT), and the Office of the National Coordinator (ONC) to advance conformance and interoperability testing capabilities. This website provides HIT implementers with the necessary resources to support and test their implementation of standards-based health systems. For more information, visit NIST at [www.nist.gov](http://www.nist.gov).





## 6.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

### 6.1 DESCRIPTION OF STANDARDS

The following table contains descriptions of the selected standards from section 4.1.2 above:

**Table 6.1-1 Description of Standards**

Standard	Description
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	The Healthcare Permission Catalog provides the necessary content for creating interoperable roles facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit <a href="http://www.hl7.org">www.hl7.org</a> .
Health Level Seven (HL7) Version 2.3.1 Chapter 2 – Control, Chapter 3 – Patient Administration	The HL7 Version 2.3.1 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets/code tables are contained in the standard. For more information visit <a href="http://www.hl7.org">www.hl7.org</a> .
Health Level Seven (HL7) Version 2.5, Chapter 2 – Control, Chapter 3 – Patient Administration, Chapter 5 - Query	The HL7 Version 2.5 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets/code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. For more information visit <a href="http://www.hl7.org">www.hl7.org</a> .
Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	The Data Consent RMIM captures the data and associations needed to (1) record or report a consumer's consent or dissent to authorize the access, collection, use, or disclosure of personally identifiable information; (2) convey a provider's request or intent to override a patient's recorded consent or dissent; (3) convey a type of consent directive associated with a privacy policy; or (4) to record or report a consumer's consent directive, which is to be applied to future access, collection, use or disclosure of personally identifiable information. For more information visit <a href="http://www.hl7.org">www.hl7.org</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise User Assertion (XUA) Integration Profile	The Cross-Enterprise User Assertion Profile (XUA) provides a means to communicate claims about the user identity of an authenticated principal (user, application, system...) in transactions that cross enterprise boundaries. To provide accountability in these cross enterprise transactions there is a need to identify the requesting user in a way that the receiver can make access decisions and proper audit entries. The XUA Profile supports enterprises that have chosen to have their own user directory with their own unique method of authenticating the entities, and others that may have chosen to use a third party to perform the authentication. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) – Revision 5.0 or later, Cross Enterprise Sharing of Scanned Documents (XDS-SD) Integration Profile	This profile defines how to store healthcare metadata in clinical documents, including patient identifiers, demographics, encounter, order or service information, represented within a structured HL7 CDA R2 header, with a PDF or plaintext formatted document containing clinical information. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> to retrieve Volume 1, and Volume 2 of the framework.





Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile	The Audit Trail and Node Authentication (ATNA) Integration Profile establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Consistent Time (CT) Integration Profile	The Consistent Time (CT) Integration Profile provides a means to ensure that the system clocks and time stamps of the many computers in a network are well synchronized. This profile specifies synchronization with a median error less than 1 second. This is sufficient for most purposes. The current version of the ITI-TF Final Text, specifies the IHE CT Integration Profile, and other transactions defined and implemented as of October 10, 2008. The latest version of the IHE Technical Framework is available at <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	The Audit Trail and Node Authentication (ATNA) Integration Profile establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This Integration Profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. The latest version of the IHE Technical Framework is available at <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 or later, Patient Demographics Query (PDQ) Integration Profile	Provides ways for multiple distributed applications to query a central patient information server for a list of patients, based on user-defined search criteria, and retrieve a patient's demographic (and, optionally, visit or visit-related) information directly into the application. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2008 - 2009, Pediatric Demographics, Draft for Trial Implementation (August 22, 2008)	The experience of immunization registries and other public health population databases has shown that matching and linking patient records from different sources for the same individual person in environments with large proportions of pediatric records requires additional demographic data. Pediatric Demographics makes use of the following six additional demographic fields to aid record matching in databases with many pediatric records. The latest version of the IHE Technical Framework is available at <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) 2007-2008 Trial Implementation Supplement Cross-enterprise Document Reliable Interchange (XDR) Release 3	This Supplement to the IHE IT Infrastructure Technical Framework provides a generic, standards based mechanism for conveying a set of medical documents in a point-to-point networked based communication. The current version of the XDR is specified in the XDR Trial Implementation Supplement to the ITI-TF, rev. 5.0, which is consistent with IHE XDS.b Supplement in term of document entry metadata. For more information visit <a href="http://www.ihe.net/technical_framework">www.ihe.net/technical_framework</a> .  NOTE: Off-line mode transaction expected to be updated once standards are available for Web Services Off-line.



Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a) Integration Profile	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. Section 10, Cross-Enterprise Document Sharing facilitates the registration, distribution and access across health enterprises of patient electronic health records. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The Registry Stored Query Transaction Trial Implementation Supplement specifies an IHE transaction that provides optimization and implementation simplification. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b) Integration Profile	The Cross-Enterprise Document Sharing-B Integration Profile (XDS.b) supplement provides a new implementation choice for the Cross-Enterprise Document Sharing (XDS) Integration Profile based on use of the Web Services and ebXML Reg/Rep standards that is consistent with current developments and best practices in the industry. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The trial implementation version of the XCA Supplement to the ITI-TF, rev. 4.0 Final Text, specifies the IHE transactions that support access between communities in a manner compatible with the XDS Integration profile. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) Integration Profile – Trial Implementation	The Basic Patient Privacy Consents (BPPC) Integration Profile provides a mechanism to record the patient privacy consent(s), a method to mark documents published to XDS with the patient privacy consent that was used to authorize the publication, and a method for XDS Consumers to use to enforce the privacy consent appropriate to the use. This profile complements XDS by describing a mechanism whereby an XDS Affinity Domain can develop and implement multiple privacy policies, and describes how that mechanism can be integrated with the access control mechanisms supported by the XDS Actors (e.g. systems). There are two key parts of the profile: 1) It provides a document content specification for capturing a patient acknowledgement of a privacy consent policy or policies. 2) It describes the method by which XD* Actors can enforce the privacy policies determined by the document confidentialityCode related to the patient privacy consents. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Patient Identifier Cross-Referencing (PIX) Integration Profile	The Patient Identifier Cross-referencing (PIX) Integration Profile is targeted at healthcare enterprises of a broad range of sizes (hospital, a clinic, a physician office, etc.). It supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains via the following interactions: 1) The transmission of patient identity information from an identity source to the Patient Identifier Cross-reference Manager. 2) The ability to access the list(s) of cross-referenced patient identifiers either via a query/ response or via update notification. By specifying the above transactions among specific actors, this integration profile does not define any specific enterprise policies or cross-referencing algorithms. By encapsulating these behaviors in a single actor, this integration profile provides the necessary interoperability while maintaining the flexibility to be used with any cross-referencing policy and algorithm as deemed adequate by the enterprise. For more information visit <a href="http://www.ihe.net">www.ihe.net</a> .



Standard	Description
International Organization for Standardization (ISO) PDF/A ISO 19005-1b. Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF (PDF/A)	Specifies how to use the Portable Document Format (PDF) 1.4 for long-term preservation of electronic documents. It is applicable to documents containing combinations of character, raster and vector data. For more information visit <a href="http://www.iso.org">www.iso.org</a> .
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	Describes the Network Time Protocol (NTP): the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet operating at rates from mundane to lightwave. For more information visit <a href="http://www.ietf.org">www.ietf.org</a> .
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996	Describes the Simple Network Time Protocol (SNTP) Version 4, which is an adaptation of the Network Time Protocol (NTP). SNTP can be used when the ultimate performance of the full NTP implementation is not needed or justified. When operating with current and previous NTP and SNTP versions, SNTP Version 4 involves no changes to the NTP specification or known implementations, but is rather a clarification of certain design features of NTP. For more information visit <a href="http://www.ietf.org">www.ietf.org</a> .
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) Core V2.0 OASIS Standard; ITU-T X.1141	SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. For more information visit <a href="http://www.oasis-open.org">www.oasis-open.org</a> .
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	Defines extensions that build on [WS-Security] to provide a framework for requesting and issuing security tokens, and to broker trust relationships. Defines Security Token Service (STS) model for security tokens including requesting, issuing, renewing, canceling and validating. For more information visit <a href="http://www.oasis-open.org">www.oasis-open.org</a> .
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	The Organization for the Advancement of Structured Information Standards (OASIS) standards group developed the eXtensible Access Control Markup Language (XACML) as a language to express and evaluate access decisions. The XACML technical specification includes a profile for RBAC using XACML that complies with the ANSI RBAC standard. The HL7 RBAC Permission Catalog provides a standard vocabulary that can be used for cross-enterprise access control. For more information visit <a href="http://www.oasis-open.org">www.oasis-open.org</a> .

## 6.2 USE CASE TO INFORMATION EXCHANGE AND DATA REQUIREMENTS

This section contains an extraction of business actors, required interactions and conditions/scenarios from the Use Case into a matrix/table.

**Table 6.2-1 Mapping of Use Case Actions to Information Exchange Requirements**

Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
Patient-Provider Secure Messaging: 7.1 Patient – 1 Patient-Initiated Communication			
7.1.1 Establish secure messaging ability	7.1.1.1 Establish required authorization and authentication	<a href="#">IER10</a> Identify Patient	



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
	7.1.1.2 Establish user identification code, password, and other security measures to enable access to secure messaging	Out of Scope: Policies and internal systems operation are considered internal functionality of the application	
	7.1.1.3 Conduct training and other remaining set-up as needed	Out of Scope: Specifics of training or system operation are not part of interoperability	
7.1.2 Compose and communicate secure communication	7.1.2.1 Compose message using tools established to support secure communication	<a href="#">IER2</a> Send Data over Secured Communication Channel <a href="#">IER31</a> Provide Message Routing/Description Information <a href="#">IER30</a> Compose Message Out of Scope: The user interface is not an interoperability issue	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity
	7.1.2.2 Send secure communication	<a href="#">IER33</a> Send/Receive Message <a href="#">IER3</a> Create Audit Log Entry Out of Scope: In a one-system architecture, "sending" is an internal process such as saving the message object to the receiver's "inbox", and not considered an interoperability issue, therefore out of scope	
7.1.3 Receive unsecured notification of secure message	7.1.3.1 Receive unsecured notification of secure message	Out of Scope: The nature and details of unsecured notification messages are not defined in the Use Case. (see Section 3.1.1 Assumptions and Section 3.1.2 Constraints)	
7.1.4 Receive response	7.1.4.1 Receive secure message from clinician	<a href="#">IER7</a> Verify Message Integrity In a two-system architecture <a href="#">IER32</a> Request Message <a href="#">IER34</a> Retrieve Message 'Envelope' Data <a href="#">IER9</a> Generate a Read Receipt	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
7.1.5 Update PHR	7.1.5.1 Update PHR or other patient tool with results of communication and response	<a href="#">IER3</a> Create Audit Log Entry <a href="#">IER9</a> Generate a Read Receipt <a href="#">IER8</a> Generate a Delivery Receipt <a href="#">IER35</a> Store Message into PHR	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
Patient-Provider Secure Messaging: 7.2 Clinician Support Staff – 1 Patient-Initiated Communication			
7.2.1 Receive and evaluate patient communication	7.2.1.1 Receive patient communication	<a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER10</a> Identify Patient <a href="#">IER8</a> Generate a Delivery Receipt <a href="#">IER9</a> Generate a Read Receipt <a href="#">IER7</a> Verify Message Integrity	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
	7.2.1.2 Evaluate patient communication	Out of Scope: Cognitive process, evaluation of message	
7.2.2 Request clinician input	7.2.2.1 Confirm receipt and evaluation of patient communication	<a href="#">IER8</a> Generate a Delivery Receipt <a href="#">IER9</a> Generate a Read Receipt Out of Scope: Cognitive process, evaluation of message	<a href="#">DR29</a> Read/Delivery Confirmation
	7.2.2.2 Forward patient communication to clinician(s)	Out of Scope: Internal operation (assumes that the support and clinician are on the same system)	
7.2.3 Formulate response	7.2.3.1 Determine appropriate clinical response	Out of Scope: Cognitive process: formalize response	
	7.2.3.2 Compose communication response	<a href="#">IER31</a> Provide Message Routing/Description Information <a href="#">IER30</a> Compose Message Out of Scope: Cognitive process: draft formalized response as communication message	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity
7.2.4 Communicate response	7.2.4.1 Transmit communication response	<a href="#">IER33</a> Send/Receive Message <a href="#">IER3</a> Create Audit Log Entry Out of Scope: In a one-system architecture, "sending" is an internal process such as saving the message object to the receiver's "inbox", and not considered an interoperability issue, therefore out of scope	
7.2.5 Complete information and documentation of communication event	7.2.5.1 Complete medical information related to this communication exchange	<a href="#">IER3</a> Create Audit Log Entry  Out of Scope: User process or Internal Process, updates to patient clinical record	
	7.2.5.2 Complete documentation of communication	Out of Scope: "Other workflow issues"	
Patient-Provider Secure Messaging: 7.3 Clinician – 1 Patient-Initiated Communication			
7.3.1 Evaluate clinical situation	7.3.1.1 Evaluate patient communication and clinical situation	Out of Scope: Cognitive process, access to clinical systems	
7.3.2 Formulate response	7.3.2.1 Determine appropriate clinical response	Out of Scope: Cognitive process: formalize response	
	7.3.2.2 Compose communication response	Out of Scope: Cognitive process/user input: draft formalized response as communication message <a href="#">IER31</a> Provide Message Routing/Description Information <a href="#">IER30</a> Compose Message	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
7.3.3 Communicate response	7.3.3.1 Transmit communication response	<a href="#">IER33</a> Send/Receive Message <a href="#">IER3</a> Create Audit Log Entry Out of Scope - In a one-system architecture, "sending" is an internal process such as saving the message object to the receiver's "inbox", and not considered an interoperability issue, therefore out of scope	
7.3.4 Complete information and documentation of communication event	7.3.4.1 Complete medical information related to this communication exchange	<a href="#">IER3</a> Create Audit Log Entry Out of Scope: Updates to patient clinical record, user or internal process	
	7.3.4.2 Complete documentation of communication	Out of Scope: "Other" workflow processes	
Patient-Provider Secure Messaging: 8.1 Patient – 2 Clinician-Initiated Communication			
8.1.1 Establish secure messaging ability	8.1.1.1 Establish required authorization and authentication	<a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity	
	8.1.1.2 Establish user identification code, password, and other security measures to enable access to secure message	Out of Scope: Policies and internal systems operation	
	8.1.1.3 Conduct training and other remaining set-up as needed	Out of Scope: Specifics of training or system operation are not part of interoperability	
8.1.2 Receive unsecured notification of secure message	8.1.2.1 Receive unsecured notification of secure message	<a href="#">IER33</a> Send/Receive Message <a href="#">IER3</a> Create Audit Log Entry Out of Scope: In a one-system architecture, "sending" is an internal process such as saving the message object to the receiver's "inbox", and not considered an interoperability issue, therefore out of scope <a href="#">IER10</a> Identify Patient Out of Scope: Non-electronic/non-web based notifications (e.g., phone call, SMS) are permitted within this Use Case, but are not directly within scope of this document	
8.1.3 Receive and consider communication	8.1.3.1 Receive secure message from clinician	<a href="#">IER7</a> Verify Message Integrity In a two-system architecture <ul style="list-style-type: none"> <li><a href="#">IER7</a> Request Message</li> <li><a href="#">IER34</a> Retrieve Message 'Envelope' Data</li> <li><a href="#">IER8</a> Generate a Delivery Receipt</li> </ul>	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
	8.1.3.2 Consider communication	Out of Scope: Patient cognitive process	





Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
8.1.4 Update PHR	8.1.4.1 Update PHR or other patient tool with results of communication and response	<a href="#">IER3</a> Create Audit Log Entry <a href="#">IER9</a> Generate a Read Receipt <a href="#">IER8</a> Generate a Delivery Receipt <a href="#">IER35</a> Store Message into PHR	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
Patient-Provider Secure Messaging: 8.2 Clinician Support Staff – 2 Clinician-Initiated Communication			
8.2.1 Configure decision support for clinical reminders	8.2.1.1 Receive decision support information on clinical reminders	Out of Scope: Receive information from DSS vendor (pending work in Quality Work Group)	<a href="#">DR17</a> Decision Support Data
	8.2.1.2 Incorporate decision support for clinical reminders	Out of Scope: Internal process for provider system	
8.2.2 Trigger need for clinical reminder	8.2.2.1 Activate a clinical reminder message based on patient data	Out of Scope: Internal trigger process	<a href="#">DR17</a> Decision Support Data
8.2.3 Communicate clinical reminder	8.2.3.1 Compose a clinical reminder	<a href="#">IER31</a> Provide Message Routing/Description Information <a href="#">IER30</a> Compose Message Out of Scope: Cognitive process/user input: draft formalized response as communication messaging	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity
	8.2.3.2 Transmit communication response	<a href="#">IER33</a> Send/Receive Message <a href="#">IER3</a> Create Audit Log Entry Out of Scope: In a one-system architecture, "sending" is an internal process such as saving the message object to the receiver's "inbox", and not considered an interoperability issue, therefore out of scope	
8.2.4 Complete information and documentation of communication event	8.2.4.1 Complete medical information related to this communication exchange	<a href="#">IER3</a> Create Audit Log Entry Out of Scope: Updates to patient clinical record (user process or internal integration)	
	8.2.4.2 Complete documentation of communication	Out of Scope: "other workflow issues"	
Patient-Provider Secure Messaging: 8.3 Clinician – 2 Clinician-Initiated Communication			
8.3.1 Configure decision support for clinical reminders	8.3.1.1 Receive decision support information on clinical reminders	Out of Scope: Receive information from DSS vendor (pending work in Quality Work Group)	
	8.3.1.2 Implement decision support for clinical reminders	Out of Scope: Internal process for provider system	
8.3.2 Initiate secure communication to the patient	8.3.2.1 Compose a secure communication	<a href="#">IER31</a> Provide Message Routing/Description Information <a href="#">IER30</a> Compose Message	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
	8.3.2.2 Transmit a secure communication	<a href="#">IER33</a> Send/Receive Message <a href="#">IER3</a> Create Audit Log Entry Out of Scope: In a one-system architecture, "sending" is an internal process such as saving the message object to the receiver's "inbox", and not considered an interoperability issue, therefore out of scope	
8.3.3 Complete information and documentation of communication event	8.3.3.1 Complete medical information related to this communication exchange	<a href="#">IER3</a> Create Audit Log Entry Out of Scope: Updates to patient clinical record (user process or internal integration)	
	8.3.3.2 Complete documentation of communication	Out of Scope: "Other workflow issues"	

### 6.3 USE CASE SEQUENCE DIAGRAMS

The Use Case sequence diagrams illustrate each Use Case scenario with a representation of a normal sequence of exchange between the primary actors. The event codes from the Use Case are annotated on the diagrams to show how the interactions relate to the Use Case. The interactions are supported by the various constructs which are introduced in Section 3.0 of this Interoperability Specification.

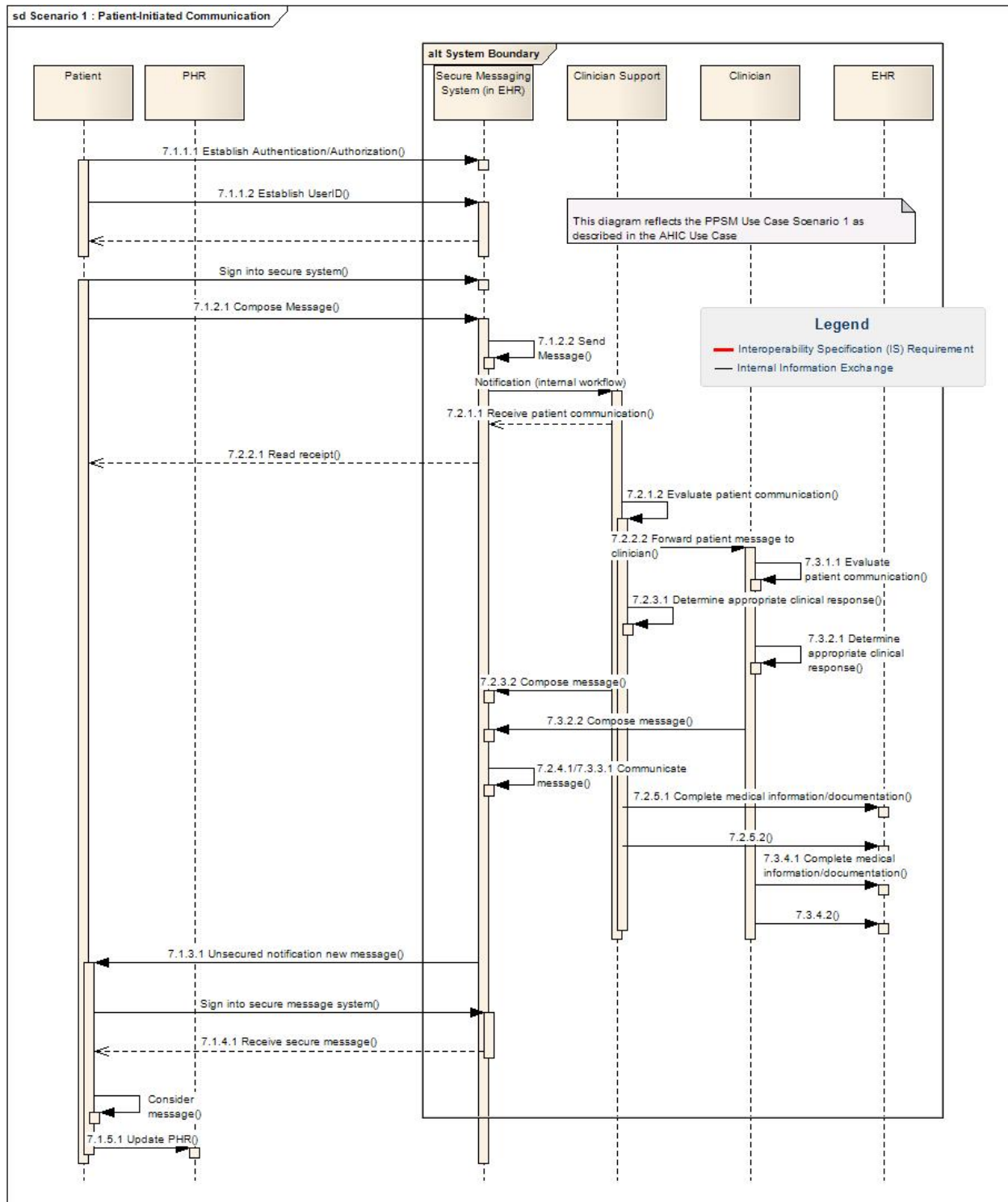
The high level sequence diagrams illustrate each Use Case scenario with a representation of a normal sequence of exchange between the primary actors. The event codes from the Use Case are annotated on the diagrams to show how the interactions relate to the Use Case. The interactions are supported by the various constructs which will be introduced in Section 3.0 of this Interoperability Specification.

The diagram below reflects Implementation Variant 1 as described in the AHIC Patient – Provider Secure Messaging Use Case.



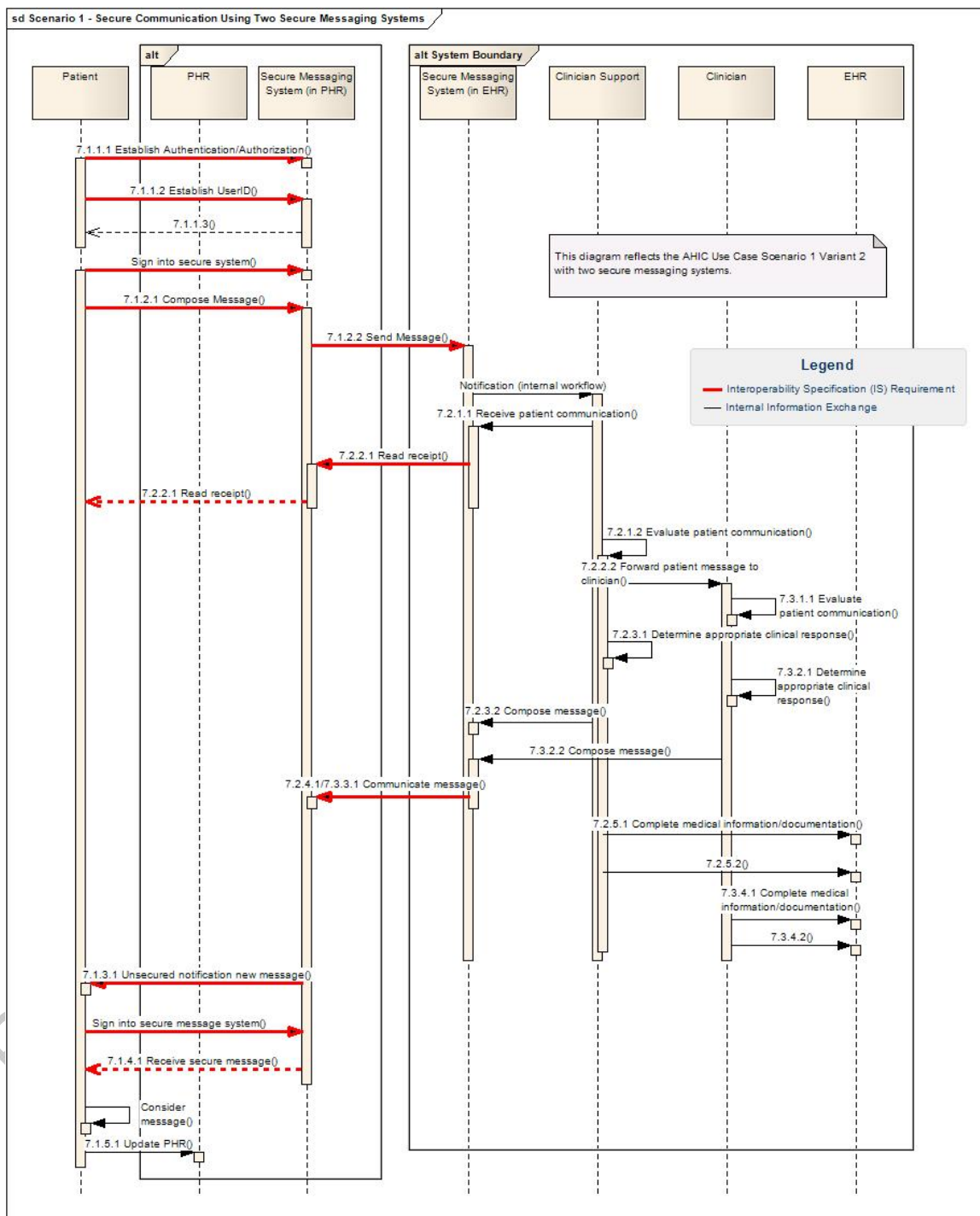


**Figure 6.3-1 Scenario 1: Patient-Initiated Communication High Level Sequence Diagram**



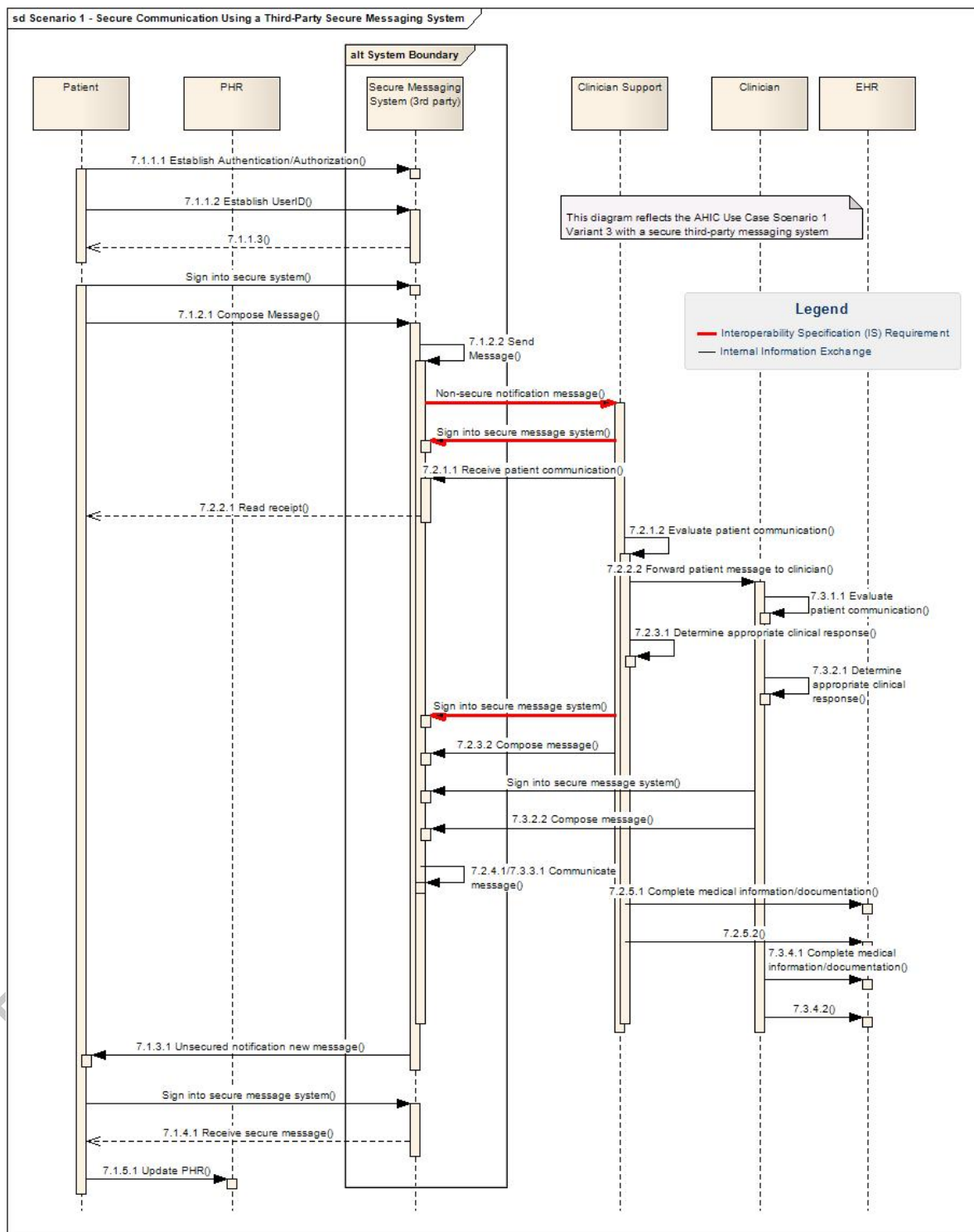
The diagram below shows Implementation Variant 2: Secure Communication Between Patient-Provider Using Two Secure Messaging Systems.

**Figure 6.3-2 Scenario 1: Secure Communication Using Two Secure Messaging Systems High Level Sequence Diagram**



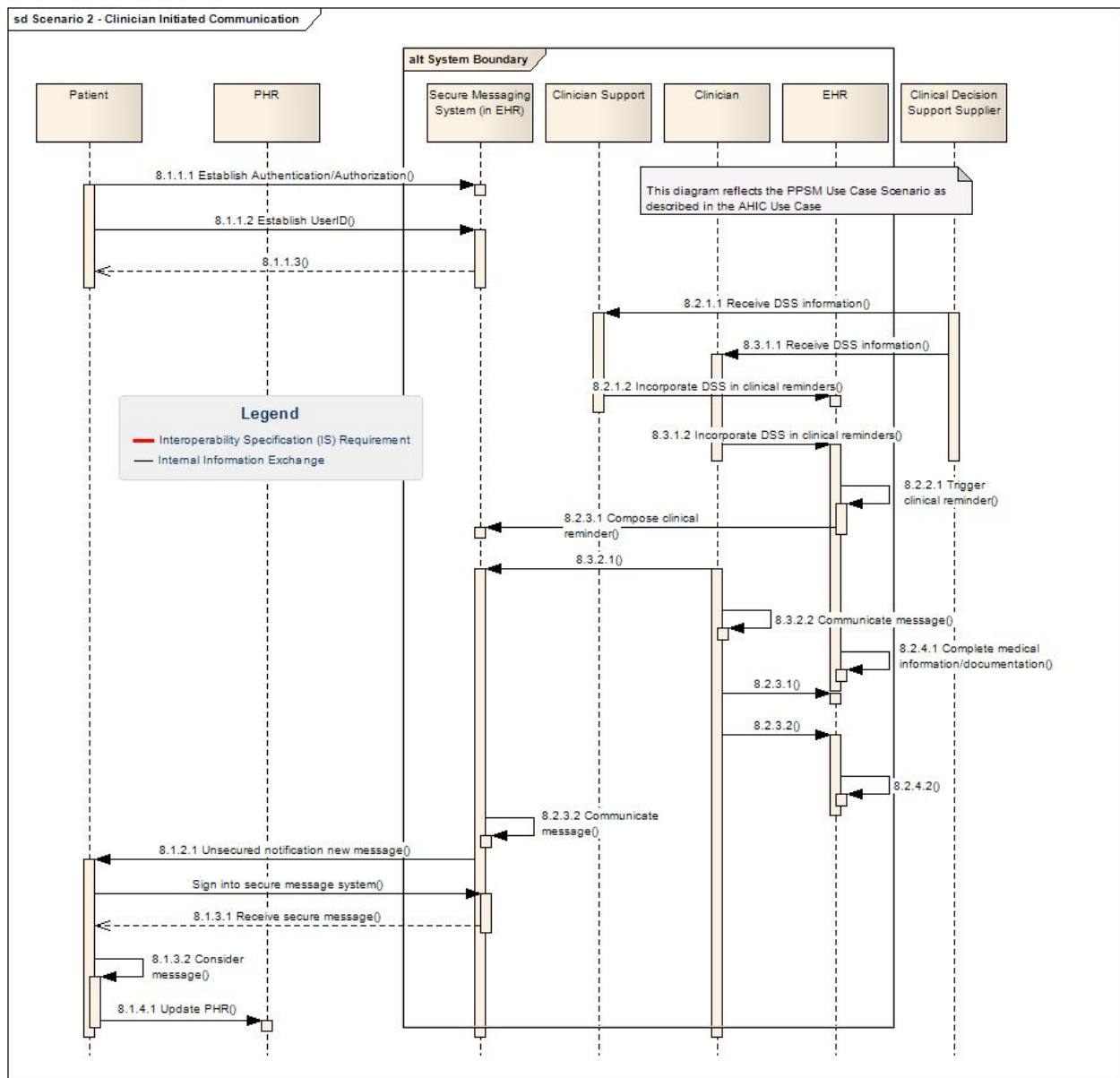
The diagram below shows Implementation Variant 3: Secure Communication between Patient-Provider Using a Third-Party Secure Messaging System.

**Figure 6.3-3 Scenario 1: Secure Communication Using a Third-Party Secure Messaging System High Level Sequence Diagram**



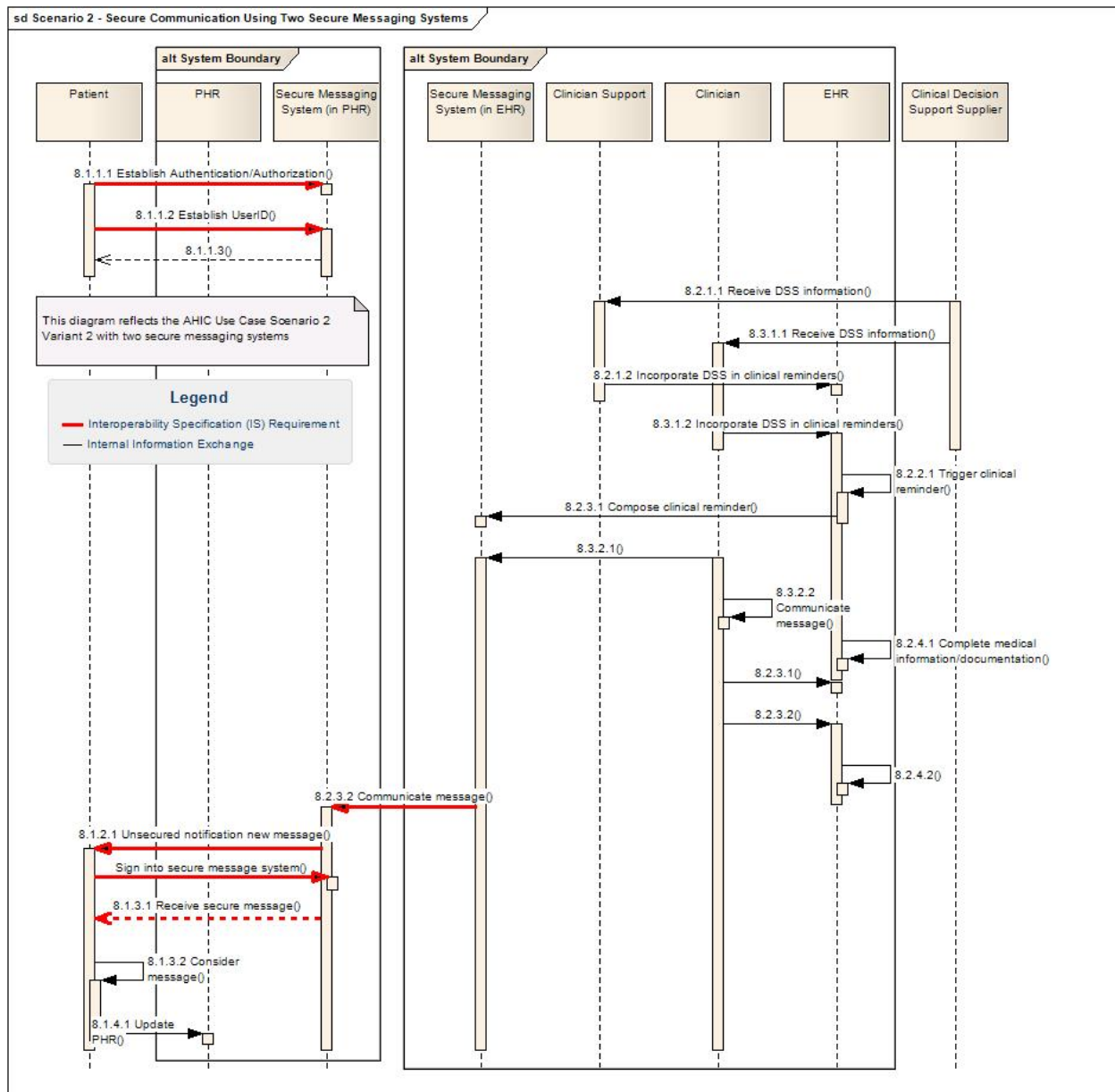
The diagram below reflects Scenario 2 from the Patient – Provider Secure Messaging Use Case, Scenario 2: Clinician-to-Patient Communication:

**Figure 6.3-4 Scenario 2: Clinician Initiated Communication High Level Sequence Diagram**



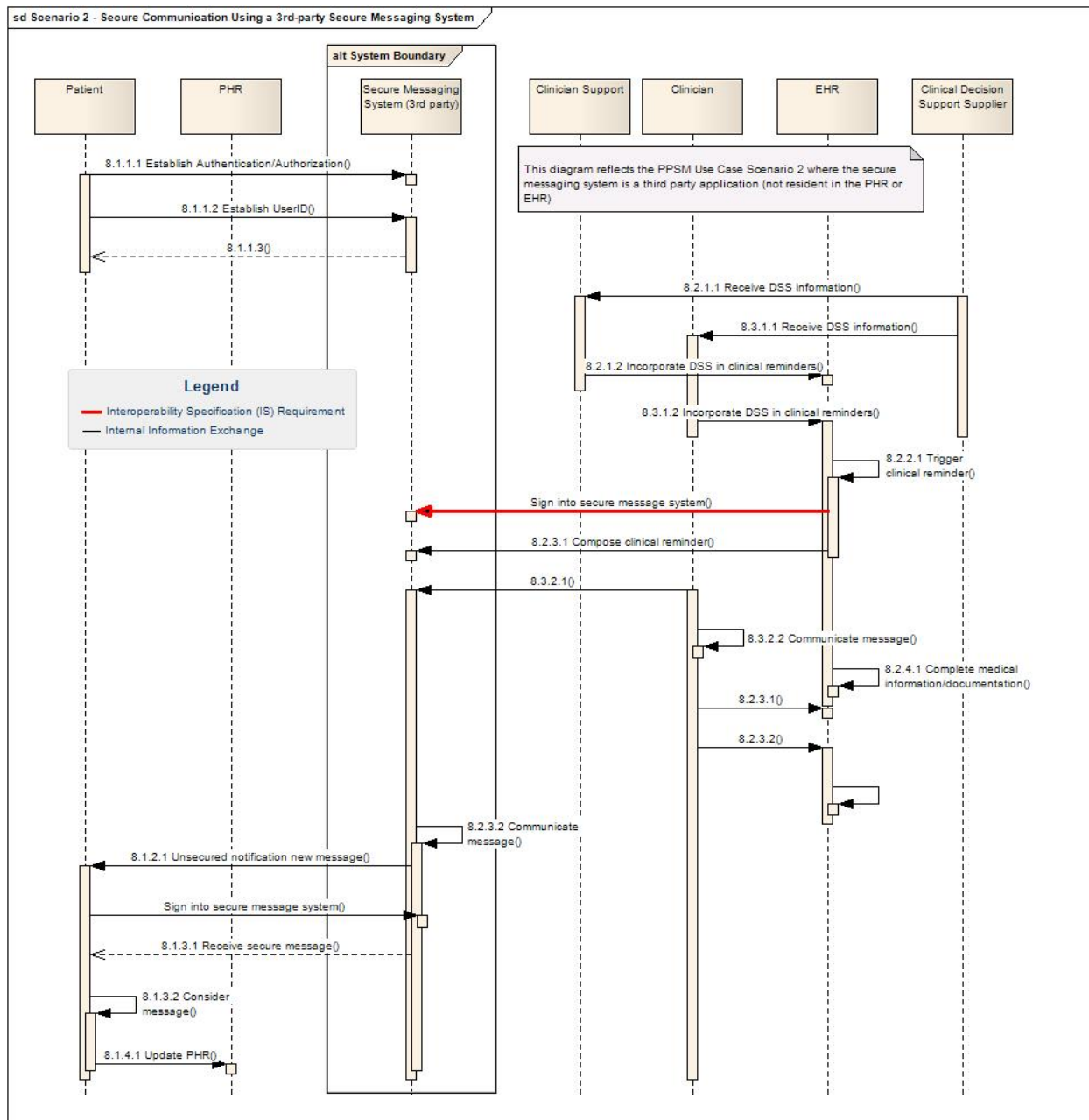
The diagram below describes Implementation Variant 2: Secure Communication between Patient-Provider using two Secure Messaging Systems.

**Figure 6.3-5 Scenario 2: Secure Communication Using Two Secure Messaging Systems High Level Sequence Diagram**



The diagram below describes Implementation Variant 3: Secure Communication between Patient-Provider Using a Third-Party Secure Messaging System.

**Figure 6.3-6 Scenario 2: Secure Communication Using a Third-Party Secure Messaging System High Level Sequence Diagram**





## 6.4 MAPPING OF CONSTRUCTS TO INFORMATION EXCHANGE AND DATA REQUIREMENTS

Table 6.4-1 below provides a mapping of the HITSP constructs that will be used in the design of the Interoperability Specification, and the data and information exchange requirements that are being satisfied by the construct. These requirements are limited to those that are deemed within scope for this Interoperability Specification, which are described in Section 3.1.

**Table 6.4-1 Mapping of Requirements to HITSP Constructs**

Construct Name	Information Exchange Requirement Number (IER#)	Data Requirement Number (DR#)
HITSP/C19 - Entity Identity Assertion	<a href="#">IER10</a> Identify Patient <a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER8</a> Generate a Delivery Receipt	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
HITSP/C62 - Unstructured Document	<a href="#">IER35</a> Store Message into PHR <a href="#">IER8</a> Generate a Delivery Receipt <a href="#">IER9</a> Generate a Read Receipt <a href="#">IER33</a> Send/Receive Message <a href="#">IER32</a> Request Message <a href="#">IER7</a> Verify Message Integrity <a href="#">IER3</a> Create Audit Log Entry <a href="#">IER30</a> Compose Message <a href="#">IER31</a> Provide Message Routing/Description Information <a href="#">IER34</a> Retrieve Message 'Envelope' Data	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
HITSP/T15 - Collect and Communicate Security Audit Trail	<a href="#">IER10</a> Identify Patient <a href="#">IER3</a> Create Audit Log Entry <a href="#">IER9</a> Generate a Read Receipt <a href="#">IER8</a> Generate a Delivery Receipt <a href="#">IER35</a> Store Message into PHR <a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER7</a> Verify Message Integrity	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
HITSP/T16 - Consistent Time	<a href="#">IER10</a> Identify Patient <a href="#">IER3</a> Create Audit Log Entry <a href="#">IER9</a> Generate a Read Receipt <a href="#">IER8</a> Generate a Delivery Receipt <a href="#">IER35</a> Store Message into PHR <a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER7</a> Verify Message Integrity	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation



Construct Name	Information Exchange Requirement Number (IER#)	Data Requirement Number (DR#)
HITSP/T17 - Secured Communication Channel	<a href="#">IER33</a> Send/Receive Message <a href="#">IER2</a> Send Data over Secured Communication Channel <a href="#">IER31</a> Provide Message Routing/Description Information <a href="#">IER30</a> Compose Message	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity
HITSP/T23 - Patient Demographics Query	<a href="#">IER10</a> Identify Patient <a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER8</a> Generate a Delivery Receipt	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
HITSP/T31 - Document Reliable Interchange	<a href="#">IER7</a> Verify Message Integrity <a href="#">IER32</a> Request Message <a href="#">IER34</a> Retrieve Message 'Envelope' Data <a href="#">IER9</a> Generate a Read Receipt <a href="#">IER33</a> Send/Receive Message <a href="#">IER3</a> Create Audit Log Entry <a href="#">IER8</a> Generate a Delivery Receipt <a href="#">IER35</a> Store Message into PHR <a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER10</a> Identify Patient <a href="#">IER31</a> Provide Message Routing/Description Information <a href="#">IER30</a> Compose Message	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
HITSP/TP20 - Access Control	<a href="#">IER10</a> Identify Patient <a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER8</a> Generate a Delivery Receipt	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
HITSP/TP22 - Patient ID Cross-Referencing	<a href="#">IER10</a> Identify Patient <a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER8</a> Generate a Delivery Receipt	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation
HITSP/TP30 - Manage Consent Directives	<a href="#">IER10</a> Identify Patient <a href="#">IER1</a> Provide Authorization and Consent <a href="#">IER5</a> Verify Entity Identity <a href="#">IER8</a> Generate a Delivery Receipt	<a href="#">DR27</a> Message Routing & Content/Envelope/Metadata <a href="#">DR28</a> Secure Message Integrity <a href="#">DR29</a> Read/Delivery Confirmation





## 7.0 DOCUMENT UPDATES

The following sections provide the details of updates made to this document.

### 7.1 DECEMBER 10, 2008

The changes in this construct address the following comments received during the Public Comment and Inspection Testing period (September 29 – October 24, 2008).

5030,5155,5156,5157,5158,5395,5414,5564,5565,5566,5567,5568,5569,5570,5571,5572,5683,5684,5685,5686,5687,5688,5689,5690,5691,5692,5693,5694,5695,5696,5697,5698,5699,5700,5701,5702,5703

The full text of the comments along with the Technical Committee's disposition can be reviewed on the [HITSP Public Web Site](#).

#### 7.1.1 UPDATES FROM PUBLIC COMMENT

- Incorporated all of the 37 Public Comment TC dispositions into the document
- Acknowledged difficulties in navigating the IS, particularly with mapping requirements into constructs. Suggestions have been passed on to the Project Management team.
- Updated section 3.1.2 to reflect a case where access originates from a public computer (assumption), and to ensure that a user's computer maintains standard virus protection (pre-condition).
- Table 6.2-1 has been updated to ensure consistency of IER's and DR's to reflect proper sequencing of events and actions.
- All references to business actors, technical actors, interoperability exchange requirements (IER's) and data requirements (DR's) have been update to align with a library of objects that have been harmonized across all IS'.
- Left-over references to TP13, TP49 and T29 from earlier versions have been removed.
- Several glossary-related items have been referred to Project Management to ensure consistency of definitions.
- All punctuation and formatting inconsistencies have been corrected.
- Updates have been made to Table 3.1-1 to clarify Use Case scoping statements, particularly to exclude various forms of "live" communications, and to clarify the use of read and delivery receipts.
- Labeling on UML diagrams in Figure 2.2.4-1 have been corrected for consistency and accuracy.

Minor editorial changes were made to this construct.



## 7.2 DECEMBER 18, 2008

Upon approval by the HITSP Panel on December 18, 2008, this document is now Released for Implementation.

RELEASED FOR IMPLEMENTATION

