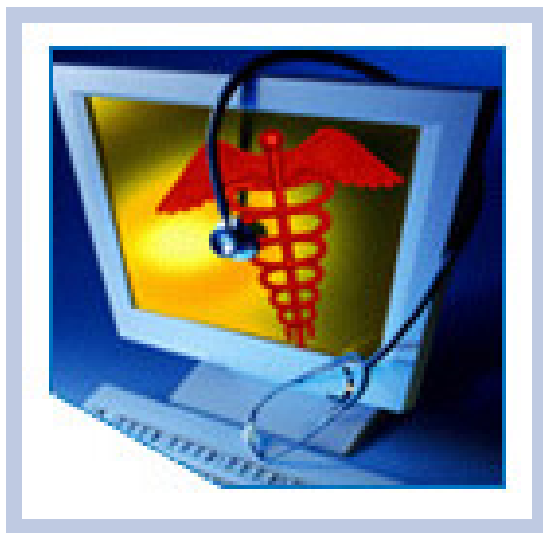


HITSP Patient-Provider Secure Messaging Use Case Requirements, Design and Standards Selection

HITSP/RDSS57



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

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

With input from:

**Administrative and Financial Domain Technical Committee
Care Management and Health Records Domain Technical Committee
Security, Privacy and Infrastructure Domain Technical Committee (Formerly Security and Privacy Technical Committee)**



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Review Copy	Consumer Perspective Technical Committee With input from: Administrative and Financial Domain Technical Committee Care Management and Health Records Domain Technical Committee Security, Privacy and Infrastructure Domain Technical Committee (Formerly Security and Privacy Technical Committee)	June 27, 2008



TABLE OF CONTENTS

1.0	INTRODUCTION	6
1.1	Purpose	6
1.2	Audience.....	6
1.3	How to Use this Requirements, Design and Standards Selection Document.....	6
1.3.1	Conventions, Acronyms and Resources/References.....	7
1.4	Copyright Permissions.....	7
2.0	REQUIREMENTS ANALYSIS	9
2.1	Use Case Synopsis	9
2.2	Use Case Requirements	11
2.2.1	Mapping of Use Case Requirements to Interoperability Requirements	11
2.2.2	Data and information Requirements Matrix.....	21
2.2.3	Identification of Business Actors, and Scenarios	23
2.2.4	High-Level UML Business Sequence Diagram	23
2.2.4.1	Implementation Variants on Business Actors and Their Relationships	24
3.0	DESIGN.....	32
3.1	Scope of Design	32
3.1.1	Assumptions	34
3.1.2	Constraints	35
3.1.3	Pre-conditions.....	35
3.1.4	Post-conditions.....	36
3.1.5	Process Triggers	36
3.2	Detailed Design	37
3.2.1	Technical Actor Role Descriptions	38
3.2.2	Sequence Diagram for Process Flow	40
3.2.3	Mapping of Business Actors to Technical Actors and Constructs with optionality	42
3.2.4	Data Detail.....	44
3.2.5	New HITSP Constructs.....	45
3.2.6	Modifications to Existing HITSP Constructs	45
3.2.7	Document Map	48
4.0	CANDIDATE STANDARDS.....	49
4.1	List of Selected and Candidate Standards	49
4.1.1	Regulatory and Guidance Standards	50
4.1.2	Selected and Candidate Standards.....	50
4.2	Gaps Where There Are No Standards	51
4.3	Standard Overlaps.....	51



5.0	NEXT STEPS	53
6.0	APPENDIX	54
6.1	Description of Standards	54
7.0	CHANGE HISTORY	55



FIGURES AND TABLES

Figure 2.2.4.1-1 Implementation Variants.....	25
Figure 2.2.4.1-2 Scenario 1: Patient-Initiated Communication	26
Figure 2.2.4.1-3 Scenario 2: Secure Communication Using Two Secure Messaging Systems.....	27
Figure 2.2.4.1-4 Scenario 1: Secure Communication Using a Third-Party Secure Messaging System	28
Figure 2.2.4.1-5 Scenario 2: Clinician Initiated Communication	29
Figure 2.2.4.1-6 Scenario 2: Secure Communication Using Two Secure Messaging Systems.....	30
Figure 2.2.4.1-7 Scenario 2: Secure Communication Using a 3rd-party Secure Messaging System	31
Figure 3.2.2-1 Detailed Sequence Diagram for Scenario 1	41
Figure 3.2.2-2 Detailed Sequence Diagram for Scenario 2	42
Figure 3.2.7-1 Requirements, Design and Standards Selection Document Map	48
Table 1.3.1-1 Reference Documents	7
Table 2.2.1-1 Mapping of Use Case Requirements to Interoperability Requirements	11
Table 2.2.2-1 Data Element and Information Requirements	22
Table 2.2.3-1 Business Actors	23
Table 3.1-1 Scoping Clarifications	32
Table 3.1.1-1 Assumptions	34
Table 3.1.2-1 Constraints.....	35
Table 3.1.3-1 Pre-conditions.....	35
Table 3.1.4-1 Post-conditions	36
Table 3.1.5-1 Process Triggers.....	36
Table 3.2.1-1 Technical Actor Role Descriptions.....	38
Table 3.2.3-1 Business-Technical Actor Mapping to Transaction and/or Content	43
Table 3.2.4-1 Data Element Constraints.....	45
Table 3.2.5-1 New HITSP Constructs.....	45
Table 3.2.6-1 Existing HITSP Constructs	45
Table 4.1.1-1 Regulatory and Guidance Standards	50
Table 4.1.2-1 Selected and Candidate Standards Linked to Requirements.....	50
Table 4.2-1 Use Case Events and Associated Gaps.....	51
Table 4.3-1 Standard Overlaps.....	52
Table 6.1-1 Description of Standards	54



1.0 INTRODUCTION

As an introduction to the HITSP Patient-Provider Secure Messaging (PPSM) Use Case Requirements, Design and Standards Selection, this section describes the purpose of the document, the intended audience for the technical content of the document, and how to use this document. It acknowledges the copyright protections that pertain, and provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0 Requirements Analysis.

1.1 PURPOSE

The Requirements, Design and Standards Selection document is used to define the requirements for the Use Case and the detailed HITSP Interoperability Specification design map of existing standards and specifications that will be used to meet the stated requirements. It is intended to describe the process by which the Use Case was analyzed, standards were selected and the design was developed.

1.2 AUDIENCE

The Requirements, Design and Standards Selection document is designed to be used by the HITSP Technical Committees or Work Groups to document their analysis and decisions, other analysts who need to understand and evaluate the requirements, design and selected standards, and by those intending to test the resulting Interoperability Specifications against the Use Case requirements. Understanding and using the relevant set of Interoperability Specifications is a key requirement for establishing interoperability compliance.

1.3 HOW TO USE THIS REQUIREMENTS, DESIGN AND STANDARDS SELECTION DOCUMENT

The Requirements, Design and Standards Selection document is divided into five main related sections. Each section provides background information for the Interoperability Specification. Section 1.0 provides a brief introduction to the document. Users of this document who are familiar with the content may choose to proceed to Section 2.0. In Section 2.0, the Requirements Analysis provides a general overview of the Use Case and the specific requirements of the Use Case including a mapping of the Use Case requirements to the extracted interoperability requirements, the data requirements of the Use Case, and an identification of the scenarios, business actors, their interactions, and data elements used in those interactions. The design for the Interoperability Specification is provided in Section 3.0. This includes the scope of the design, mapping of interoperability requirements to the specific technical requirements, actor interactions and groupings, detailed descriptions of data used by the Use Case actors, and a description of existing or new HITSP constructs that will be used by the Interoperability Specification. Section 4.0 describes the Standards Selection process, provides a table of the selected and candidate standards, a Gaps and Overlaps discussion and plan for resolution. Section 5.0 describes the next steps in the HITSP standards harmonization process and Section 6.0 provides relevant appendix material.



1.3.1 CONVENTIONS, ACRONYMS AND RESOURCES/REFERENCES

A list of key reference documents and background material is provided in the table below. These documents can be retrieved from the hitsp.org Web Site.

Table 1.3.1-1 Reference Documents

Reference Document	Document Description
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 product development or product refinement
HITSP Conventions List	Describes the conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications
HITSP Acronyms List	Lists and defines the acronyms used in this document
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
Patient-Provider Secure Messaging Detailed Use Case, March 21, 2008	AHIC Use Case that is the basis of this Interoperability Specification
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">• The scope, reference policy background, and Security and Privacy principles used in the development of the constructs• A detailed description and schematics of the conceptual relationship between the Security and Privacy constructs• A mapping of existing standards and constructs to be used in meeting the stated requirements of the AHIC Use Cases• A list of identified gaps and the recommended approaches to resolving those gaps• A roadmap for how the Security and Privacy constructs will evolve and eventually align with other HITSP Interoperability Specifications• A conceptual framework for Security and Privacy management, including reference information on privacy policies, risk assessment, and risk management• A glossary of terms used in all the Security and Privacy construct documents• 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 <p>HITSP will periodically update this Technical Note as required by the introduction of new contexts for use.</p>

1.4 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.



NOTE: HITSP will work with the appropriate standards organizations to obtain applicable copyright information for candidate standards.



2.0 REQUIREMENTS ANALYSIS

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

- Mapping from the Use Case Requirements to the Derived Interoperability Requirements – this table lists the requirements grouped by actor for each event and related action
- Data Element Requirements – this table further describes the data requirements for each specified interoperability requirement and the business actor that is responsible for the data
- Business Actors – this table defines the business actors that are included for the Interoperability Specification
- High-Level Unified Modeling Language (UML) Business Sequence 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 (PPSM) Use Case, including any applicable scenarios that are part of the Use Case.

Use Case Synopsis:

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. Similarly, the use of the term “provider” includes clinicians and clinician support staff. Since “provider” is also occasionally used in the healthcare industry to indicate a more generic service or capability provider, the term “clinician” will be used more extensively in this Use Case to promote clarity.

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 secure 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 target 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 another tool 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 and promote wellness and patient 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 due consideration and review, the Provider, or 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 REQUIREMENTS TO INTEROPERABILITY REQUIREMENTS

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

Key: Considered out of scope

Table 2.2.1-1 Mapping of Use Case Requirements to Interoperability Requirements

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
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	Identification of Patient {Registry Patient Id/Id Domain OID} - Leverage Entity Identity Assertion HITSP/C19 {Authenticate Consumers-Partial Gap}	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
				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	<p>The interaction between the user (consumer) and the secure message system is through a secure connection</p> <p>The user interface is not an interoperability issue</p> <p>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)</p> <p>The secure messaging system will compose a complete message (from the required and optional information provided by the consumer) in the defined format</p> <p>The output must conform. The means to create that output is not within the scope of this Use Case</p>	1 Message Routing & envelope/metadata



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
				7.1.2.2 Send secure communication	<p>Query response/Retrieve Information</p> <p>In a two-system architecture (both the clinician and the consumer have secure message systems) the message object is transferred via secure connection to the secure messaging system associated with the designated receiver</p> <p>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</p>	
			7.1.3 Receive unsecured notification of secure message	7.1.3.1 Receive unsecured notification of secure message	<p>The notification must indicate where the secure message resides to enable the receiver of the notification take the appropriate action</p> <p>To reduce the potential of fraud, an unsecured electronic (web-based) notification should not contain a link directly to the secure message site</p> <p>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</p>	1 Message Routing & envelope/metada ta



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
			7.1.4 Receive response	7.1.4.1 Receive secure message from clinician	<p>The secure message system must establish integrity of the message through internal system functionality</p> <p>In a two-system architecture</p> <ul style="list-style-type: none"> The consumer/patient would request that the secure message be transported to their secure message system. The systems may permit the consumer/patient to retrieve just the "envelope" information in order to assess whether the entire message is necessary If requested, the secure message system will transmit a notification that the message has been received (delivery receipt) 	<p>1 Message Routing & envelope/metadata</p> <p>2 Message integrity UserID/password</p> <p>4 Read/Delivery Receipt</p>
			7.1.5 Update PHR	7.1.5.1 Update PHR or other patient tool with results of communication and response	<p>The secure message system will log that the message was received and/or viewed</p> <p>If requested, the secure message system will transmit a notification that the message has been accessed (read receipt)</p> <p>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)</p> <p>For a secure message system integrated in a PHR, the message will be added to the health record for the PHR owner</p> <p>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</p>	<p>1 Message Routing & envelope/metadata</p> <p>2 Message integrity</p> <p>4 Read/Delivery Receipt</p>



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
	7.2 Clinician Support	1 Patient Initiated Communication	7.2.1 Receive and evaluate patient communication	7.2.1.1 Receive patient communication	Secure message system authenticates user and verifies authorization. Identification of Patient {Registry Patient Id/Id Domain OID} -Leverage Entity Identity Assertion HITSP/C19 {Authenticate Consumers-Partial Gap} 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) If requested, the secure message system will transmit a notification that the message has been accessed (read receipt) The secure message system verifies the integrity of the message	1 Message Routing & envelope/metadata 2 Message integrity 4 Read/Delivery Receipt
				7.2.1.2 Evaluate patient communication	Cognitive process, out of scope	
			7.2.2 Request clinician input	7.2.2.1 Confirm receipt and evaluation of patient communication	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) If requested, the secure message system will transmit a notification that the message has been accessed (read receipt) Cognitive: evaluation of message – out of scope	4 Read/Delivery Receipt
				7.2.2.2 Forward patient communication to clinician(s)	Internal operation – out of scope. (assumes that the support and clinician are on the same system)	
			7.2.3 Formulate response	7.2.3.1 Determine appropriate clinical response	Cognitive process: formalize response – out of scope	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
				7.2.3.2 Compose communication response	Cognitive process/user input: draft formalized response as communication message – out of scope	1 Message Routing & envelope/metadata
					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)	2 Message integrity
					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)	
			7.2.4 Communicate response	7.2.4.1 Transmit communication response	In a 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"	1 Message Routing & envelope/metadata 2 Message integrity
			7.2.5 Complete information and documentation of communication event	7.2.5.1 Complete medical information related to this communication exchange	Secure system audit log Updates to patient clinical record (out of scope – user process or internal integration)	
	7.2.5.2 Complete documentation of communication	"Other workflow issues" Out of scope				
	7.3 Clinician	1 Patient Initiated Communication	7.3.1 Evaluate clinical situation	7.3.1.1. Evaluate patient communication and clinical situation	Cognitive process, out of scope access to clinical systems	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
			7.3.2 Formulate response	7.3.2.1 Determine appropriate clinical response	Cognitive process: formalize response – out of scope	
				7.3.2.2 Compose communication response	<p>Cognitive process/user input: draft formalized response as communication message</p> <p>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)</p> <p>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)</p>	1 Message Routing & envelope/metadata
			7.3.3 Communicate response	7.3.3.1 Transmit communication response	<p>In a two-system architecture (both the clinician and the consumer have secure messaging systems) the message object is transferred via secure connection to the secure messaging system associated with the designated receiver</p> <p>In a one-system architecture, "sending" is an internal process such as saving the message object to the receiver's "inbox"</p>	<p>1 Message Routing & envelope/metadata</p> <p>2 Message integrity</p>
			7.3.4 Complete information and documentation of communication event	7.3.4.1 Complete medical information related to this communication exchange	<p>Secure system audit log</p> <p>Updates to patient clinical record (out of scope – user process or internal integration)</p>	
				7.3.4.2 Complete documentation of communication	"Other" workflow processes out of scope	
	8.1 Patient	2 Clinician-Initiated Communication	8.1.1 Establish secure messaging ability	8.1.1.1 Establish required authorization and authentication	Identification of Patient {Registry Patient Id/Id Domain OID} - Leverage Entity Identity Assertion HITSP/C19 (Authenticate Consumers-Partial Gap)	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
				8.1.1.2 Establish user identification code, password, and other security measures to enable access to secure message	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	<p>The notification must indicate where the secure message resides to enable the receiver of the notification take the appropriate action</p> <p>To reduce the potential of fraud, an unsecured electronic (web-based) notification should not contain a link directly to the secure message site</p> <p>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</p>	1 Message Routing & envelope/metadata
			8.1.3 Receive and consider communication	8.1.3.1 Receive secure message from clinician	<p>The secure messaging system must establish integrity of the message through internal system functionality</p> <p>In a two-system architecture</p> <ul style="list-style-type: none"> The consumer/patient would request that the secure message be transported to their secure messaging system The systems may permit the consumer/patient to retrieve just the "envelope" information in order to assess whether the entire message is necessary If requested, the secure messaging system will transmit a notification that the message has been received (delivery receipt) 	<p>1 Message Routing & envelope/metadata</p> <p>2 Message integrity UserID/password</p> <p>4 Read/Delivery Receipt</p>
				8.1.3.2 Consider communication	Patient cognitive process – out of scope	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
			8.1.4 Update PHR	8.1.4.1 Update PHR or other patient tool with results of communication and response	<p>The secure messaging system will log that the message was received and/or viewed</p> <p>If requested, the secure messaging system will transmit a notification that the message has been accessed (read receipt)</p> <p>If requested, and if a two-system architecture is being used, the secure messaging system will transmit a notification that the message has been received (delivery receipt)</p> <p>For a secure messaging system integrated in a PHR, the message will be added to the health record for the PHR owner</p> <p>For a secure messaging 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</p>	<p>1 Message Routing & envelope/metadata</p> <p>2 Message integrity</p> <p>4 Read/Delivery Receipt</p>
	8.2 Clinician Support	2 Clinician-Initiated Communication	8.2.1 Configure decision support for clinical reminders	8.2.1.1 Receive decision support information on clinical reminders	Receive information from DSS vendor – out of scope (pending work in Quality Work Group)	3 Decision Support
				8.2.1.2 Incorporate decision support for clinical reminders	Internal process for provider system – out of scope	
			8.2.2 Trigger need for clinical reminder	8.2.2.1 Activate a clinical reminder message based on patient data	Internal trigger process – out of scope	3 Decision Support



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
			8.2.3 Communicate clinical reminder	8.2.3.1 Compose a clinical reminder	<p>Cognitive process/user input: draft formalized response as communication messaging – out of scope</p> <p>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)</p> <p>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)</p>	<p>1 Message Routing & envelope/metadata</p> <p>2 Message integrity</p>
				8.2.3.2 Transmit communication response	<p>In a two-system architecture (both the clinician and the consumer have secure messaging systems) the message object is transferred via secure connection to the secure messaging system associated with the designated receiver</p> <p>In a one-system architecture, "sending" is an internal process such as saving the message object to the receiver's "inbox"</p>	<p>1 Message Routing & envelope/metadata</p> <p>2 Message integrity</p>
			8.2.4 Complete information and documentation of communication event	8.2.4.1 Complete medical information related to this communication exchange	<p>Secure system audit log</p> <p>Updates to patient clinical record (out of scope – user process or internal integration)</p>	
				8.2.4.2 Complete documentation of communication	<p>"other workflow issues"</p> <p>Out of scope</p>	
			8.3.1 Configure decision support for clinical reminders	8.3.1.1 Receive decision support information on clinical reminders	<p>Receive information from DSS vendor</p> <p>– out of scope (pending work in Quality Work Group)</p>	
	8.3 Clinician	2 Clinician-Initiated Communication				



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
				8.3.1.2 Implement decision support for clinical reminders	Internal process for provider system – out of scope	
			8.3.2 Initiate secure communication to the patient	8.3.2.1 Compose a secure communication	<p>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)</p> <p>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)</p>	<p>1 Message Routing & envelope/metadata</p> <p>2 Message integrity</p>
				8.3.2.2 Transmit a secure communication	<p>In a two-system architecture (both the clinician and the consumer have secure messaging systems) the message object is transferred via secure connection to the secure messaging system associated with the designated receiver</p> <p>In a one-system architecture, "sending" is an internal process such as saving the message object to the receiver's "inbox"</p>	<p>1 Message Routing & content</p> <p>2 Message integrity</p>
			8.3.3 Complete information and documentation of communication event	8.3.3.1 Complete medical information related to this communication exchange	<p>Secure system audit log</p> <p>Updates to patient clinical record (out of scope – user process or internal integration)</p>	
				8.3.3.2 Complete documentation of communication	"Other workflow issues" out of scope	

2.2.2 DATA AND INFORMATION REQUIREMENTS MATRIX

This section contains an extraction of data and information requirements with a listing of the actual data elements and information that meet the described data requirements.



Table 2.2.2-1 Data Element and Information Requirements

Requirement Number	Description
Data Requirement 1	<p>Message routing and content/envelope/metadata of the secure message, including (but not limited to):</p> <ul style="list-style-type: none"> • Message ID • From (ID/name?) • To (ID/Name?) • Subject (in the secure message, this may contain sensitive information) • Timestamps(s) • Keywords(billing, appt, medication, allergy, to nurse, lab result – list may vary based upon provider setting) – aka “Payload type” • Message Priority • Payload ID(s) • Body (structured/unstructured) – may include payload by reference • Consider metadata requirements from SMTP, X.400, CORE Phase II, and similar • (the specific metadata attributes are somewhat flexible depending on what the available constructs/standards have available)
Data Requirement 2	<p>Secure Message Integrity data is provided, including (but not limited to):</p> <ul style="list-style-type: none"> • Message integrity information (hash, etc.)
Data Requirement 3	<p>Decision Support data is provided, including (but not limited to):</p> <ul style="list-style-type: none"> • Look at other decision support Use Case requirements • This may not be needed from an interoperability perspective. The CDS information is presented to the clinician/support staff and they use that in setting up triggers in the EHR
Data Requirement 4	<p>Read/Delivery Receipt data is provided, including (but not limited to):</p> <ul style="list-style-type: none"> • <i>Read Receipt Request</i> • <i>Delivery Receipt Request</i>



2.2.3 IDENTIFICATION OF BUSINESS ACTORS, AND SCENARIOS

This section describes the business actors that impact interoperability requirements for each scenario. A HITSP business actor should generally be an IT system that is directly engaged, and benefits from the real world information interchange defined within a business Use Case action. A business actor may also be a person or organization, however, only IT systems have associated technical actors (see Section 3.2 for technical actors). The table below identifies the significant Use Case business actors, their descriptions and the Use Case scenarios in which they are used.

Table 2.2.3-1 Business Actors

Business Actor	Description	Use Case Scenario
Patient (PHR System)	Members of the public who receive healthcare services	Patient-Provider Secure Messaging (1) Patient Initiated Communication (2) Clinician Initiated Communication
Clinician Support	Individuals who support the workflow of clinicians. For this Use Case, this may be by receiving and evaluating communications from consumers or patients, and then engaging the appropriate clinician in the response to the patient	Patient-Provider Secure Messaging (1) Patient Initiated Communication (2) Clinician Initiated Communication
Clinician (EHR System)	Healthcare providers with patient care responsibilities, including physicians, advance practice nurses, physician assistants, nurses, psychologists, pharmacists, and other licensed and credentialed personnel involved in treating patients	Patient-Provider Secure Messaging (1) Patient Initiated Communication (2) Clinician Initiated Communication
Secure Message Provider	Included for discussion. The idea here is that there is the architectural variant where a third party "holds" the secure message. In a sense, this business actor in Variant 2 encompasses the Locator Service and Repository business actors outside of the EHR and PHR Aside from illustrating this actor in Variant 2, this actor is not included in further discussion or in Section 3.0 Design	Patient-Provider Secure Messaging (1) Patient Initiated Communication (2) Clinician Initiated Communication
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 An element of overall design, but not explicit stated in the Use Case	Patient-Provider Secure Messaging (1) Patient Initiated Communication (2) Clinician Initiated Communication

2.2.4 HIGH-LEVEL UML BUSINESS SEQUENCE DIAGRAM

This section contains an explanation of the relationship between the business actors and data interactions between the primary actors and alternative actors for each Use Case scenario. The UML diagrams that follow illustrate each scenario with a representation of a normal sequence of exchange between the primary actors.



2.2.4.1 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 2.2.4.1-1. 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 "Third Party Secure Messaging 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) log into the third system to create and retrieve secure messages. While 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.

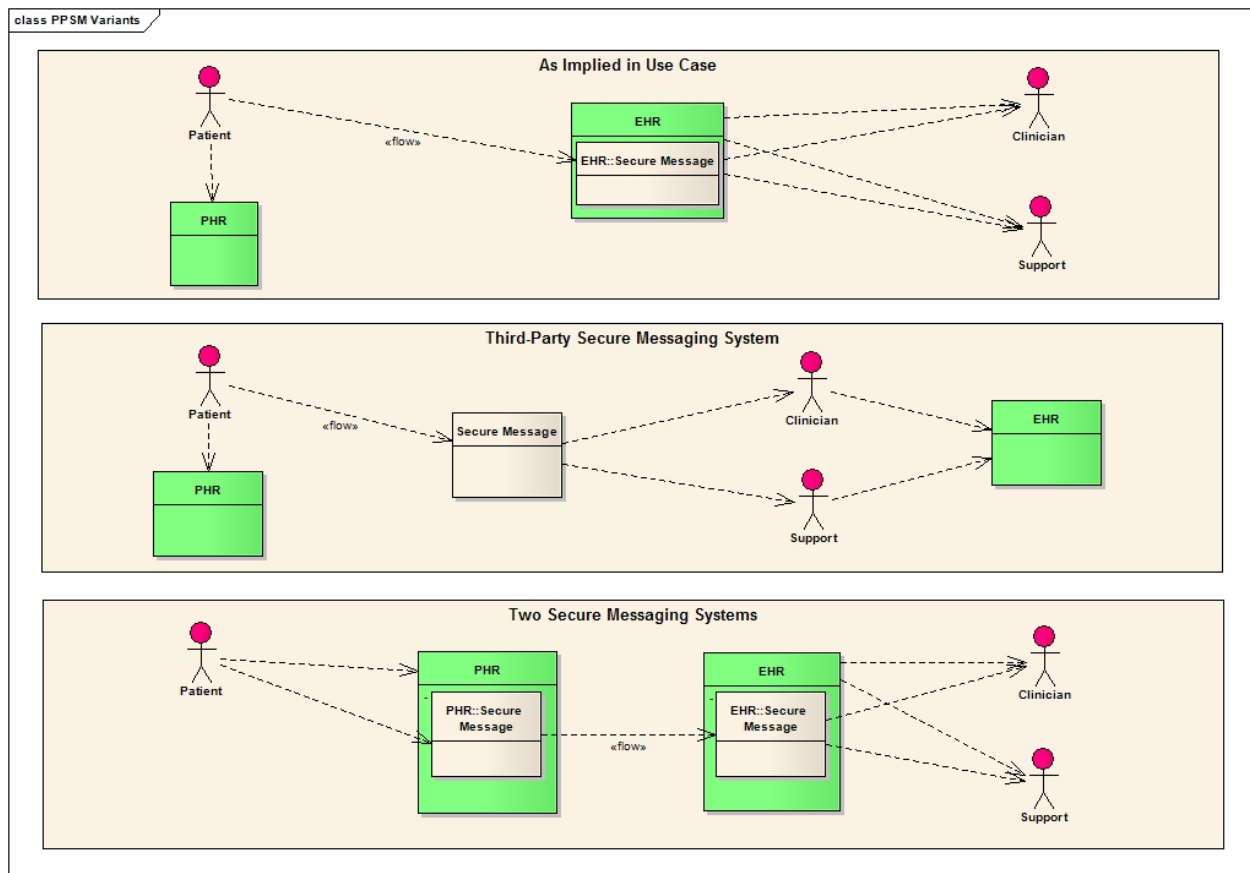
The third variant, "Two Secure Messaging Systems," has Secure Message capability built into both the PHR and EHR. In this variant, the Patient interacts with the PHR and its secure messaging capability, while the Clinician and Support staff interacts with the EHR and its secure messaging capability. 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 Messaging Systems" variant requires system-to-system information exchange. In this sense, only the "Two Secure Messaging 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 Messaging 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.

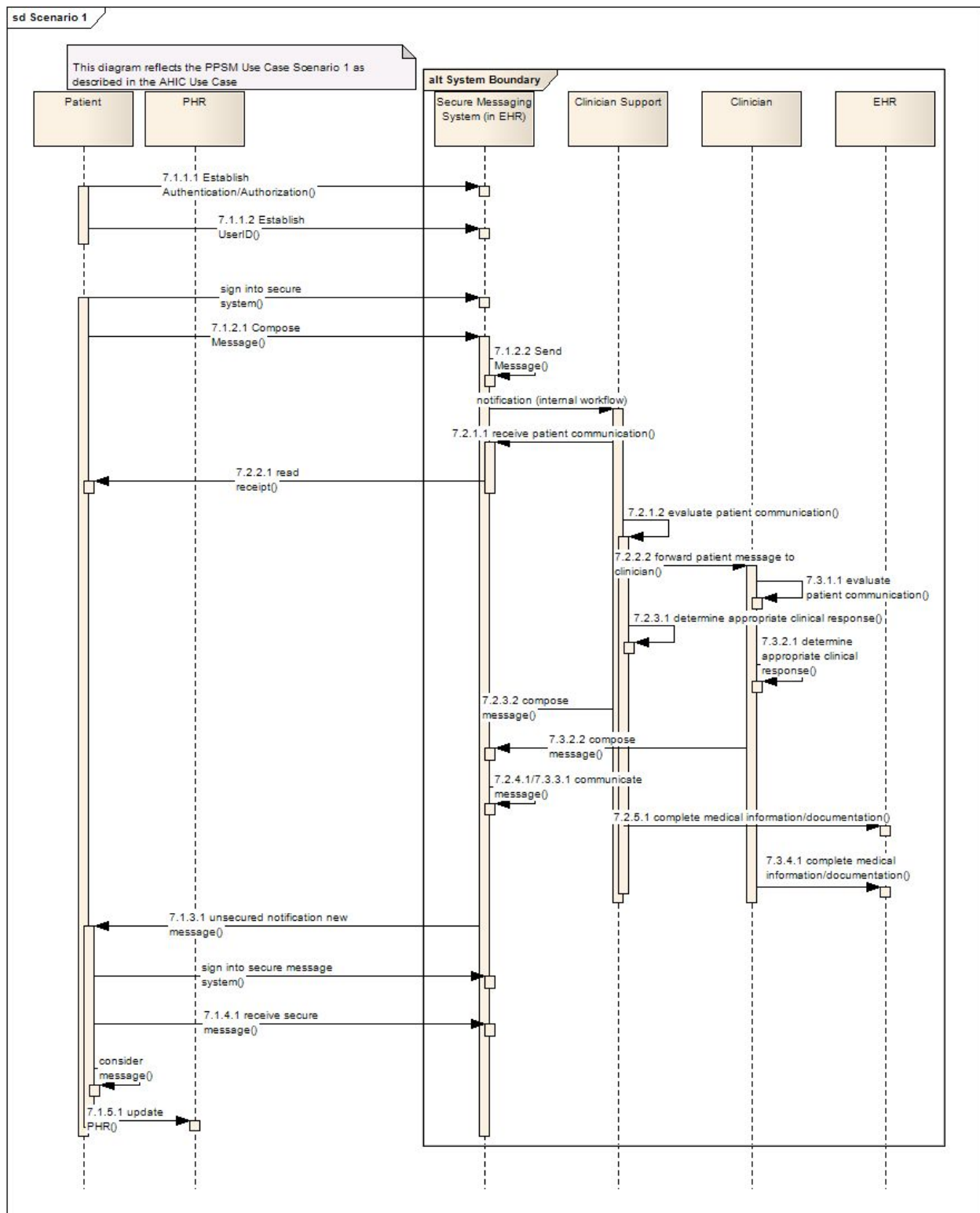


Figure 2.2.4.1-1 Implementation Variants



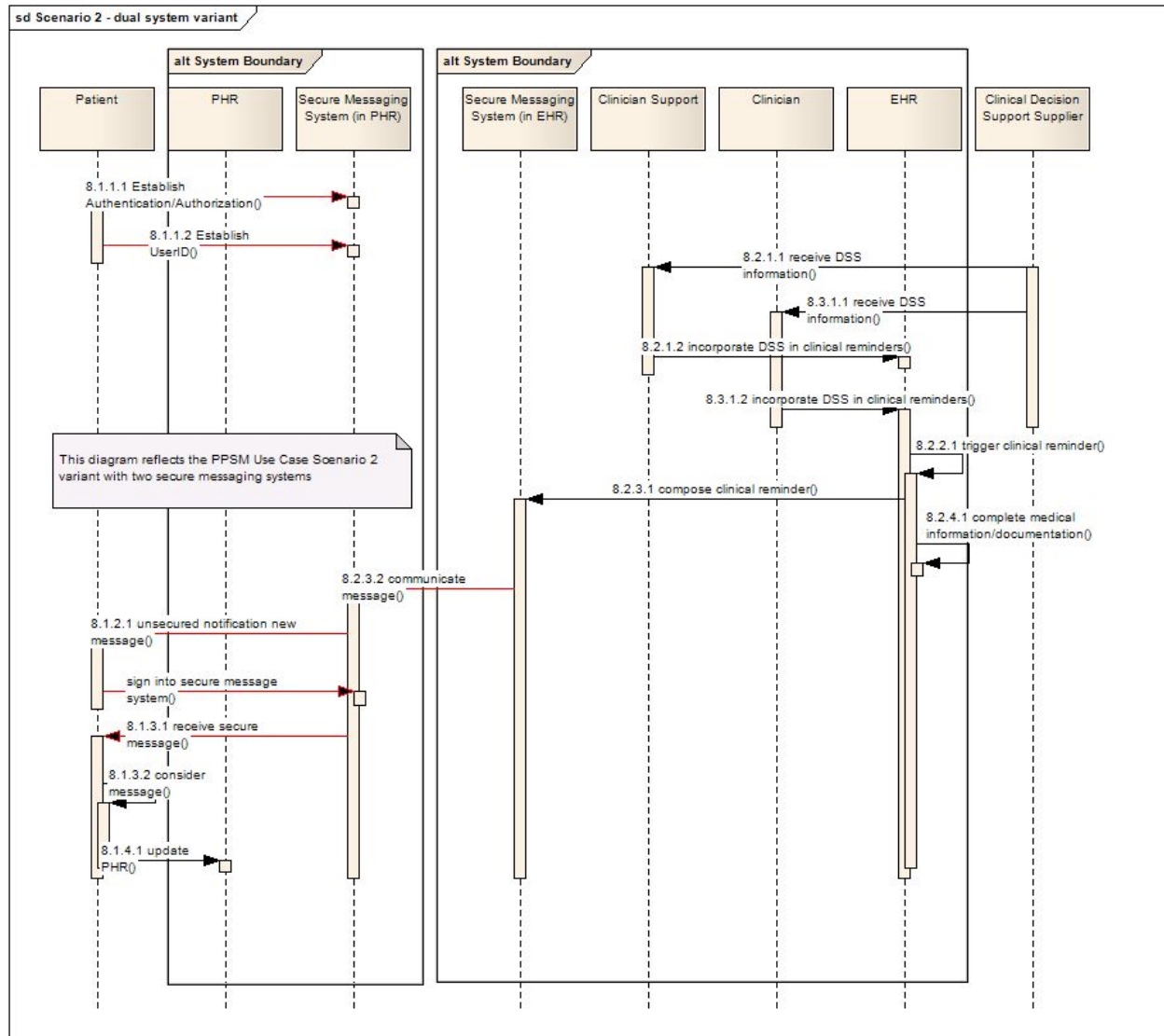
The diagram below reflects Implementation Variant 1 as described in the AHIC PPSM Use Case.

Figure 2.2.4.1-2 Scenario 1: Patient-Initiated Communication



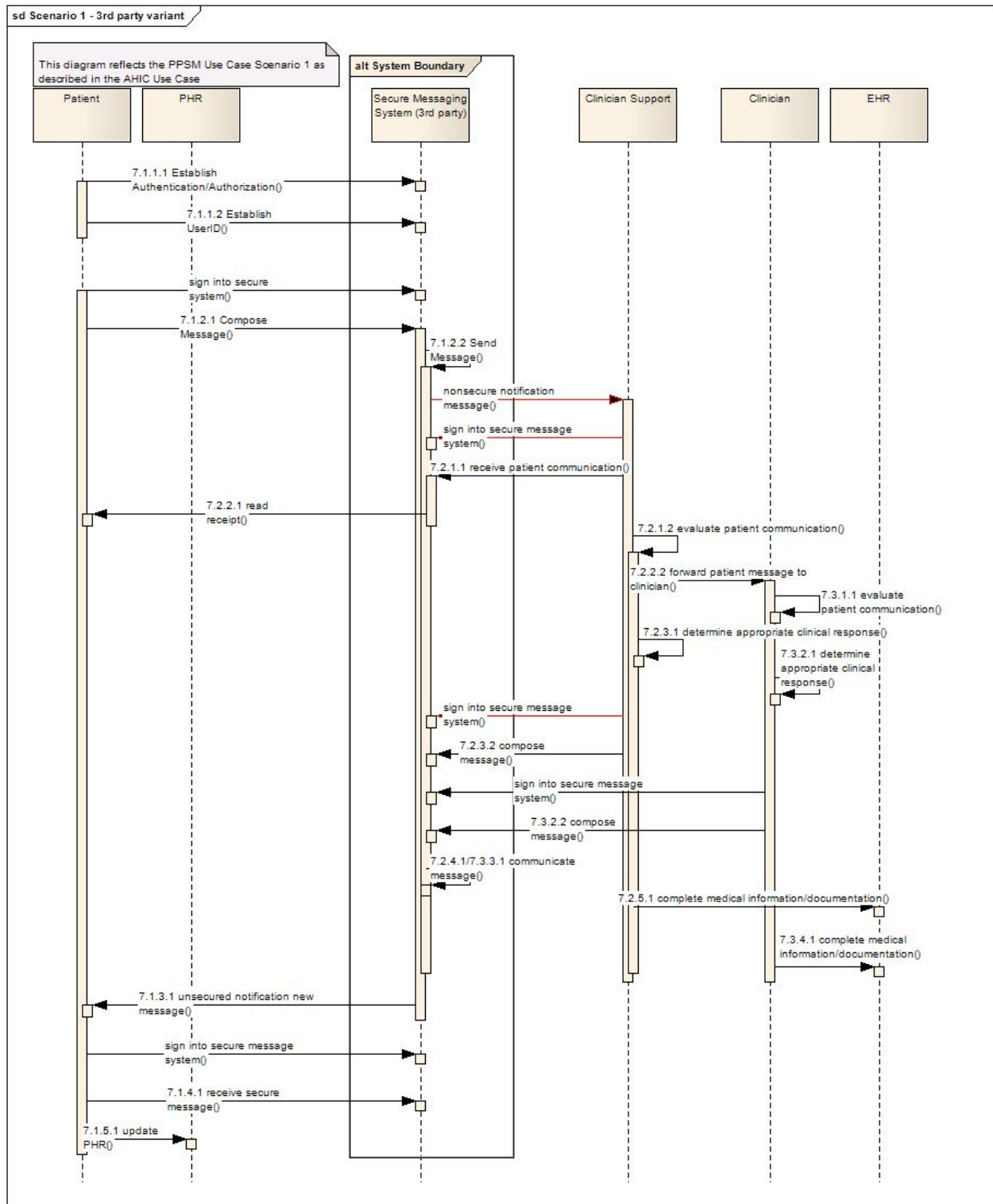
The diagram below shows Implementation Variant 2: Secure Communication Between Patient-Providing Using Two Secure Messaging Systems.

Figure 2.2.4.1-3 Scenario 2: Secure Communication Using Two Secure Messaging Systems



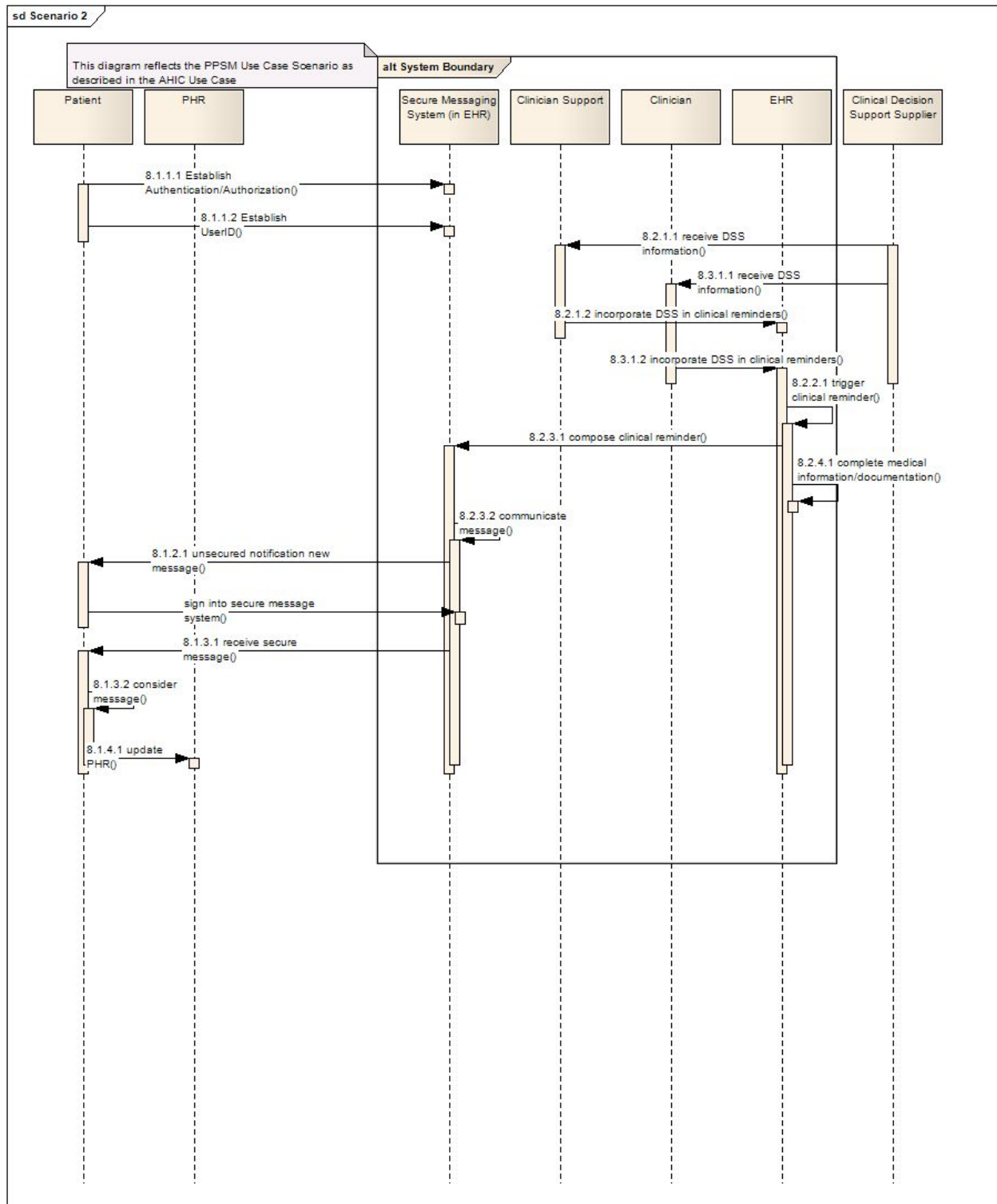
The diagram below shows Implementation Variant 3: Secure Communication between Patient-Provider Using a Third-Party Secure Messaging System

Figure 2.2.4.1-4 Scenario 1: Secure Communication Using a Third-Party Secure Messaging System



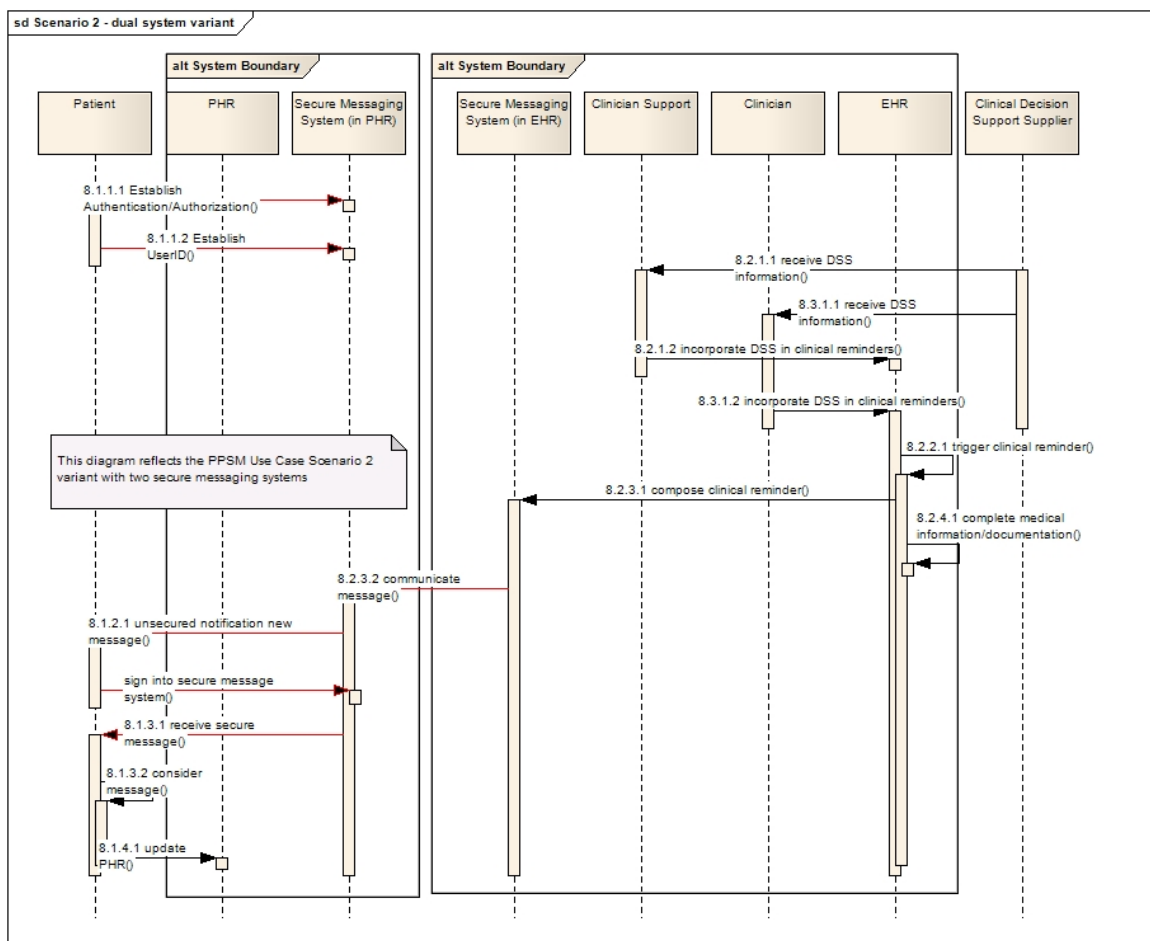
The diagram below reflects Scenario 2 from the AHIC PPSM Use Case, Scenario 2: Clinician-to-Patient Communication:

Figure 2.2.4.1-5 Scenario 2: Clinician Initiated Communication



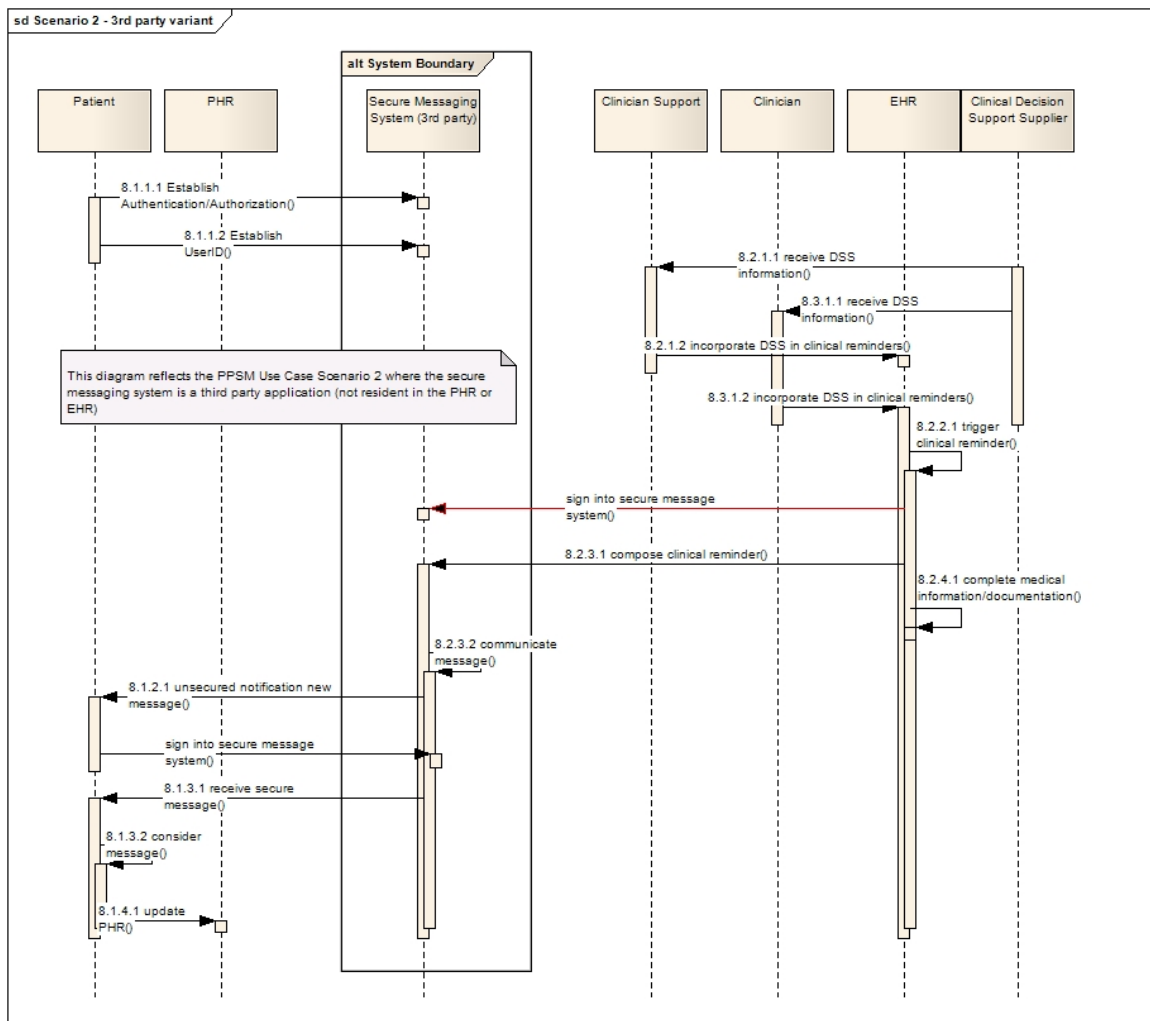
The diagram below describes Implementation Variant 2: Secure Communication between Patient-Provider using two Secure Messaging Systems.

Figure 2.2.4.1-6 Scenario 2: Secure Communication Using Two Secure Messaging Systems



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

Figure 2.2.4.1-7 Scenario 2: Secure Communication Using a 3rd-party Secure Messaging System



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 events and actions of the design from the specified requirements. It also provides a detailed mapping of the specified requirements to the business and technical actors, and data elements. Groupings of specific actions and actors are illustrated to further describe the relevant interactions as 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	Our solution does not prohibit the use of secure email but we 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	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
5	7.2.1 Receive and evaluate patient communication	7.2.1.2 Evaluate patient communication	Cognitive processes are not interoperability issues
6	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)



Scope Item	Event	Scoping Action	Recommended Resolution
7	7.2.3 Formulate response	7.2.3.1 Determine appropriate clinical response	Cognitive processes are not interoperability issues
8	7.2.3 Formulate response	7.2.3.2 Compose communication response	<p>Cognitive processes/user input are not interoperability issues</p> <p>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)</p> <p>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)</p>
9	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
10		7.2.5.2 Complete documentation of communication	Workflow processes are not interoperability issues.
11	7.3.1 Evaluate clinical situation	7.3.1.1. Evaluate patient communication and clinical situation	Cognitive processes are not interoperability issues
12	7.3.2 Formulate Response	7.3.2.1 Determine appropriate clinical response	Cognitive processes are not interoperability issues
13	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
14		7.3.4.2 Complete documentation of communication	Workflow processes are not interoperability issues
15	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
16	8.1.3 Receive and consider communication	8.1.3.2 Consider communication	Cognitive processes are not interoperability issues
17	8.2.1 Configure decision support for clinical reminders	8.2.1.1 Receive decision support information on clinical reminders	Receiving information from DSS vendor is considered out of scope, pending further work in the Quality Work Group
18		8.2.1.2 Incorporate decision support for clinical reminders	Internal processes for provider systems are not an interoperability issue
19	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



Scope Item	Event	Scoping Action	Recommended Resolution
20		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)
21	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.
22		8.2.4.2 Complete documentation of communication	Workflow processes are not interoperability issues.
23	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 Quality Workgroup.
24		8.3.1.2 Implement decision support for clinical reminders	Internal processes for provider systems are not interoperability issues.
25	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.
26		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	
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	
Notifications (the non-secure notification that a secure message is available) are transient messages in that they are not intended to persist	



Assumption	Use Case Scenario
This Use Case employs networking capabilities available to the consumer, e.g., DSL and dial-up access to internet/world-wide web	
The nature of the notification message is out of scope (could be an email, a phone call, a text message)	
"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	
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)	

3.1.2 CONSTRAINTS

This section describes the constraints that limit the use of the Requirements and Design, or to which the design must conform in order to be used within the described context. 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 scenario. 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 Use Case scenario.

Table 3.1.2-1 Constraints

Constraint	Use Case Scenario
Appropriate communication and network technologies (broadband, dial-up, WiFi) must be available to the patient.	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 preconditions 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 preconditions 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
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



Pre-condition	Use Case Scenario
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 – Provide assertion HITSP/T16 Consistent Time – Maintain time HITSP/T17 Secured Communication Channel – Authenticate node HITSP/T15 Collect and Communicate Security Audit Trail – Record audit event in repository HITSP/TP30 Manage Consent Directives – Capture/Request consent directive HITSP/TP20 Access Control – Access control request	All
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

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 their/a Health Care Provider	(1) Patient Initiated Communication
Clinician, or clinician support, 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 will provide 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 planned constructs used to meet the business and technical requirements for this Use Case. Opportunities for reuse of existing HITSP constructs are outlined, along with a description of any necessary updates to existing constructs. Any variances in the security and privacy implementation are also described here.

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 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 (See TN900 for a discussion on the challenges with PKIs).

The interoperability problem that this Use Case solves is between two systems. The following example illustrates the functional and interoperability requirements placed on these two systems. Note that this illustration is not the only method available to implement the solution.

Example 1: Consumer interaction with the Secure Messaging System.

- The Patient uses a web-browser to connect to a 'secure messaging portal'
- The system is functionally responsible for identifying, authenticating, and providing appropriate access controls and audit logs
- The secure messaging portal represents a user-interface that allows the Patient to see new messages that they have not read along with older messages
- This user-interface also allows the Patient to create a new message to send to their Provider
- This user-interface also allows the Patient to manage a list of contacts, such as their primary care provider, and other specialists that they have worked with. These contacts each have potentially unique end-point addresses

Example 2: Provider interaction with Secure Messaging System

- The Provider has the Secure Messaging System integrated into his EHR system
- In this way, the EHR system still has the same functionality of authentication, authorizations, audit logs, contacts, new/old messages, and controls to start a new message

As the above examples illustrate, there is a Secure Messaging System used by a Patient, and a Provider, and they need to interact. It is this interaction that makes up the core of this interoperability specification. The following sections provide more detailed descriptions of the requirements of the interaction.



Patient to Provider Communication:

The Patient's Secure Messaging System places the message into an unstructured document, and communicates this document, and any related documents, using either a document sharing environment or directly to the Provider's Secure Messaging System (with appropriate security, consent checking, and properly labeling of the message). The metadata within the document sharing environment holds all of the special data requirements found in Table 2.2.2-1, including the identity of the Patient's Provider. When using a document sharing environment, a notification message is sent to the Provider's Secure Messaging System based on pre-configuration of the relationship between Provider/Patient. This message may trigger the Provider's Secure Messaging System to pull the metadata and/or the document out of the document sharing environment, as well as the functional routing and alerting of the Provider. The Provider Secure Messaging system is responsible for providing a way for the Provider to view and/or respond to a message.

Provider to Patient Communication:

When the Provider responds to the message, the Provider Secure Messaging System uses the same mechanism to respond to the Patient.

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 implement real world business actor information interchanges (see Section 2.2.3). The table below identifies the technical actors and gives 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
Access Control Service (ACS)	This is the enterprise security service that supports and implements user-side access control capabilities. This is an initiator actor
Audit Record Repository	Provides a repository for audit events
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
Consent Directive Requestor	The Consent Directive Requestor accesses Consent Directives located through a Consent Registry from Consent Repositories
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
Consent Registry	Responsible for providing location information and sender notification regarding consent directives. The Consent Registry receives a Manage Consent Directive Metadata Request
Consent Repository	Responsible for both the persistent storage of consent directives as well as for their registration with the appropriate Consent Registry. It assigns a Uniform Resource Identifier (URI) and Metadata such as confidentiality codes to the consent directive for subsequent retrieval by an authorized consumer, e.g., for association with published personal health information or for evaluation at a policy decision point



Technical Actor(s)	Actor Role
Content Consumer	A Content Consumer is responsible for viewing, import, or other processing of content created by a Content Creator
Content Creator	The Content Creator is responsible for the creation of content and transmission to a Content Consumer
Document Consumer	Queries a Document Registry Actor for documents meeting certain criteria, and retrieves selected documents from one or more Document Repository actors
Document Registry	Maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumer actors about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration
Document Repository	Responsible for both the persistent storage of these documents as well as for their registration with the appropriate Document Registry. It assigns a Uniform Resource Identifier (URI) to documents for subsequent retrieval by a Document Consumer
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
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
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)
Node	Receives notifications of availability for documents in an XDS registry, and may optionally send acknowledgments of them
Notification Receiver	Sends notifications of availability for documents in an XDS registry, and receives acknowledgements of these notifications
Notification Sender	Queries the Patient Demographics Supplier to obtain patient demographic data. It may receive matches for one or more patients that enable the selection of the desired patient
Patient Demographics Consumer	Receives patient registration and update messages from other systems in the enterprise (e.g., ADT Patient Registration systems), which may or may not represent different Patient ID Domains. It responds to queries for information
Patient Demographics Supplier	Queries a Patient Identifier Cross Reference Manager for a set of identifiers for a patient
Patient Identifier Cross-Reference Consumer	Responsible for creating, maintaining and providing lists of identifiers that are aliases of one another across different Patient Identifier Domains
Patient Identifier Cross-Reference Manager	Provider of unique identifiers for each patient
Patient Identity Source	Represents the system providing a protected resource and relies on the provided security service
Service Provider (SP)	Represents the system providing a protected resource and relies on the provided security service
Service User	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 transaction. Any Service User may also be a Service Provider
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



Technical Actor(s)	Actor Role
Time Server	Provides NTP time services to Time Clients. It is either directly synchronized to a UTC master clock (e.g., satellite time signal) or is synchronized by being grouped with a Time Client to other Time Server(s)

3.2.2 SEQUENCE DIAGRAM FOR PROCESS FLOW

This section incorporates the comprehensive business and technical requirements and a detailed analysis of the interactions and decisions undertaken for the primary actions in each Use Case scenario. The 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 HITSP constructs). The detailed actor Transactions described in these diagrams show all common or independent actors, data, and the actual 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 C62 Unstructured Document, with metadata containing all of the special data requirements shown below:

Message ID/Payload ID	XDSDocumentEntry.uniqueID
From (ID/name?)	XDSDocumentEntry.Author
To (ID/Name?)	XDSDocumentEntry.IntendedRecipient
Subject (in the secure message, this may contain sensitive information)	XDSDocumentEntry.Title
Timestamps(s)	XDSDocumentEntry.CreationTime
Keywords	XDSDocumentEntry.ClassCode
Message Priority	XDSDocumentEntry.EventCodeList
Confidentiality Code*	XDSDocumentEntry.ConfidentialityCode
--indicates that this is a C62 Unstructured Document (simple text message) --	XDSDocumentEntry.FormatCode

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

2. For Point-to-Point Document communications environments



- The PHR Secure Messaging System (Document Source) communicates this document using T31 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.
- The location of the Providers Document Recipient is based on pre-configuration of the relationship between Provider/Patient.
- The reception by the Provider's Document Recipient would trigger then the functional routing and alerting of the Provider. The Provider Secure Messaging System is responsible for providing a way for the Provider to view and/or respond to a message.

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

These main 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

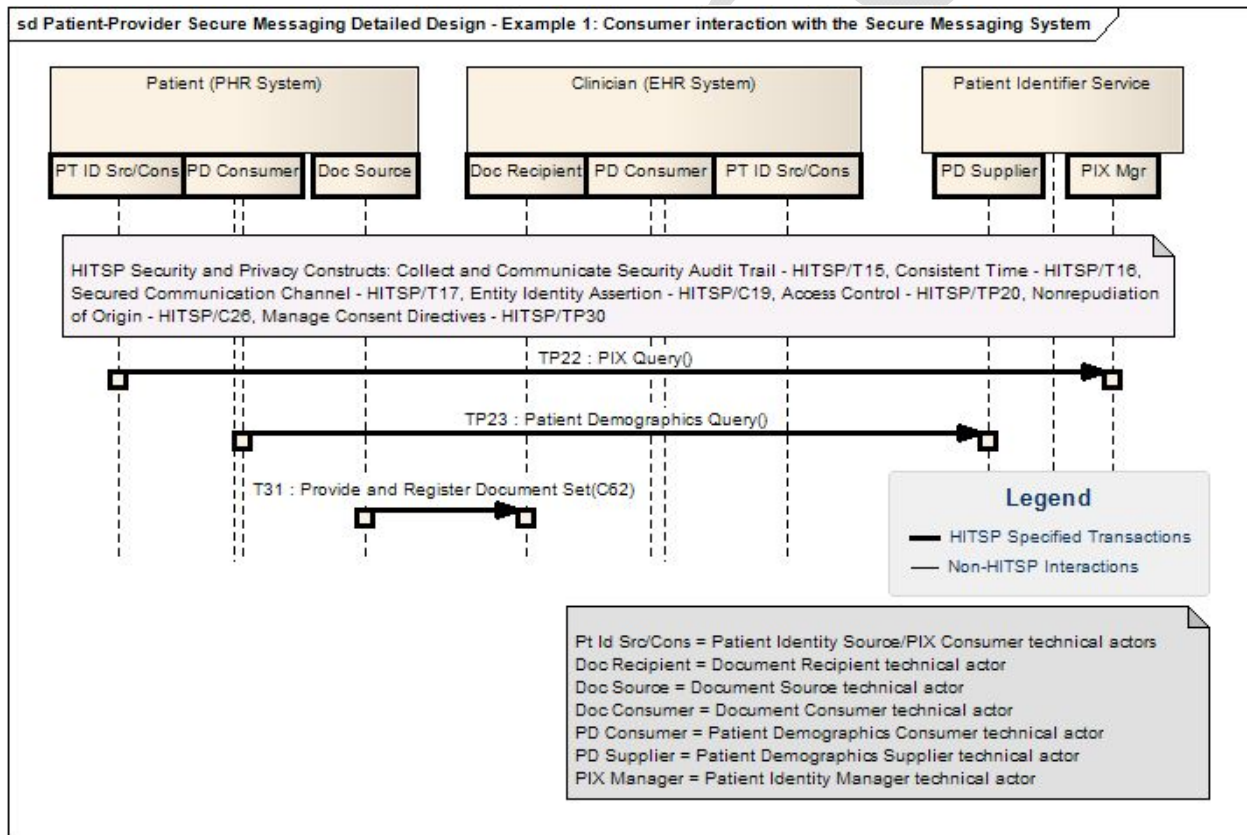
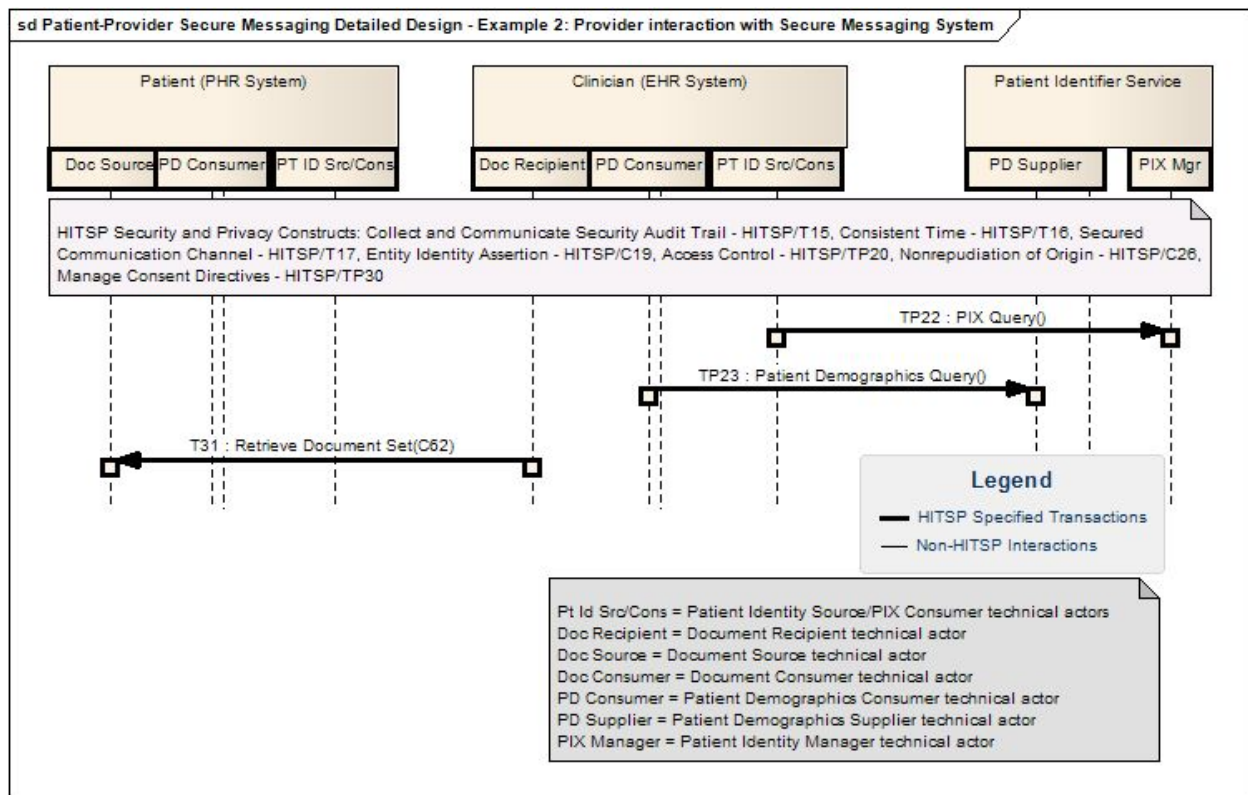


Figure 3.2.2-2 Detailed Sequence Diagram for Scenario 2



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

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

- The Required or Conditionally Required technical actors that shall be supported as specified in the associated construct.
- The Optional technical actors that may be supported as specified in the associated construct.
- All Required or Conditionally Required transactions and content subsets for each implemented technical actor assigned to the business actor that shall be supported as specified in the associated construct.
- The Optional transactions and content subsets for each implemented technical actor assigned to the business actor that 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.



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*
EHR System (Clinician)	Document Recipient	R	HITSP/T31	Provide & Register Document Set-b	R
	Patient Identifier Cross Reference Consumer	C[105]	HITSP/TP22	PIX Query	R
	Patient Demographics Consumer	C[105], [106]	HITSP/T23	Patient Demographics Query	R
	Audit Record Source	R[103]	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 Component	R
			HITSP/C62	Unstructured Document	R
	Time Client	R[103]	HITSP/T16	Maintain Time	R
	Node	R[103]	HITSP/T17	Secured Communication Channel	R
	Consent Directive Requester	R[103]	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	Service User	R	HITSP/C19	Convey Assertion	R
			HITSP/TP20	Provide Assertion	O
				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
PHR (Patient)	Document Source	R	HITSP/T31	Provide & Register Document Set-b	R
	Patient Identity Source	C[105]	HITSP/TP22	Patient Identity Feed	R
	Patient Identifier Cross-Reference Consumer (PIX Consumer)	C[105]	HITSP/TP22	PIX Query	R
				PIX Update Notification	O
	Patient Demographics Consumer	C[105]	HITSP/T23	Patient Demographic Query	R
	Content Creator	R	HITSP/TP30	Consent Document Component	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/C19	Convey Assertion	R
				Provide Assertion	O
			HITSP/TP20	Access Control Request	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
Patient Identifier Service	Access Control Service (ACS)	R	HITSP/TP20	Access Control Request	O
	Service Provider (SP)	R	HITSP/TP20	Access Control Request	O
	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

***NOTE:** Optionality = “R” for Required, or “O” for Optional, or “C” for Conditional. Conditional footnotes are further described below.

Actor Optionality Conditions

C [103] - Shall be grouped with Document Consumer when implemented

C [105] - Shall support (Patient Identity Source plus PIX Consumer) and/or Patient Demographics Consumer

C [106] - Shall only be implemented when supporting a Document Consumer Technical Actor

3.2.4 DATA DETAIL

This section details the data elements and related Transactions that were extracted from the selected standards and describes any corresponding HITSP imposed constraints (e.g., required or optional).



Table 3.2.4-1 Data Element Constraints

Data Element	Transaction	Constraint	Constraint Type (Pre-condition, post-condition, general)	Purpose (Reason for this constraint)
No applicable constraints				

3.2.5 NEW HITSP CONSTRUCTS

This section describes the new HITSP constructs (including Interoperability Specifications, Transaction Packages, Transactions and Components) that are expected to be used for this Use Case. A current list of all existing HITSP constructs that are being used can be found in Section 3.2.6.

The table below provides a description of the new HITSP constructs that will be created for this Use Case.

Table 3.2.5-1 New HITSP Constructs

New Construct	Construct Description	Technical Actors	Interoperability or Data Requirement
HITSP/C62 - Unstructured Document Component	Document that contains simple text such as a note to the patient or a note from the patient. This document could include an unstructured, presentation preserved format, such as PDF	Content Creator Content Consumer	The construct has the following data requirement: Meta-data for the payload/image is required

3.2.6 MODIFICATIONS TO EXISTING HITSP CONSTRUCTS

The table below provides a description of the existing HITSP constructs that will be used for this Use Case. It also specifies whether the construct will require modification based on the new sets of requirements that are being satisfied by the construct.

Table 3.2.6-1 Existing HITSP Constructs

HITSP Construct	Construct Description	Technical Actors	Interoperability or Data Requirement Number	Modification Required
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	Time Server Time Client	Secure Messaging System will log that the message was received and/or viewed (7.1.1.1, 7.1.5.1, 7.2.1.1, 8.1.1.1, 8.1.4.1)	No



HITSP Construct	Construct Description	Technical Actors	Interoperability or Data Requirement Number	Modification Required
HITSP/TP17 - Secured Communication Channel	The Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of Transactions, and the mutual trust between communicating parties. It supports both application and machine credentials, and user machines (user nodes)	Node	Interaction between user and secure messaging system is through a secure connection (7.1.2.1, 7.2.4.1, 7.3.3.1, 8.2.3.2, 8.3.2.1, 8.3.2.2)	No
HITSP/TP20 - Access Control	The Access Control Transaction Package provides the mechanism to administer 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. In an emergency, this construct supports the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents	Access Control Service Service Provider Service User	Identification of Patient, Secure Messaging System authenticates user and verifies authorization (7.1.1.1, 7.2.1.1, 8.1.1.1)	No
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	Consent Originator Consent Repository Consent Registry Consent Directive Requestor	Identification of Patient, Secure Messaging System authenticates user and verifies authorization (7.1.1.1, 7.2.1.1, 8.1.1.1)	No
HITSP/TP15 - 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	Audit Record Source Audit Record Repository	Secure Messaging System will log that the message was received and/or viewed (7.1.1.1, 7.1.5.1, 7.2.1.1, 8.1.1.1, 8.1.4.1)	No



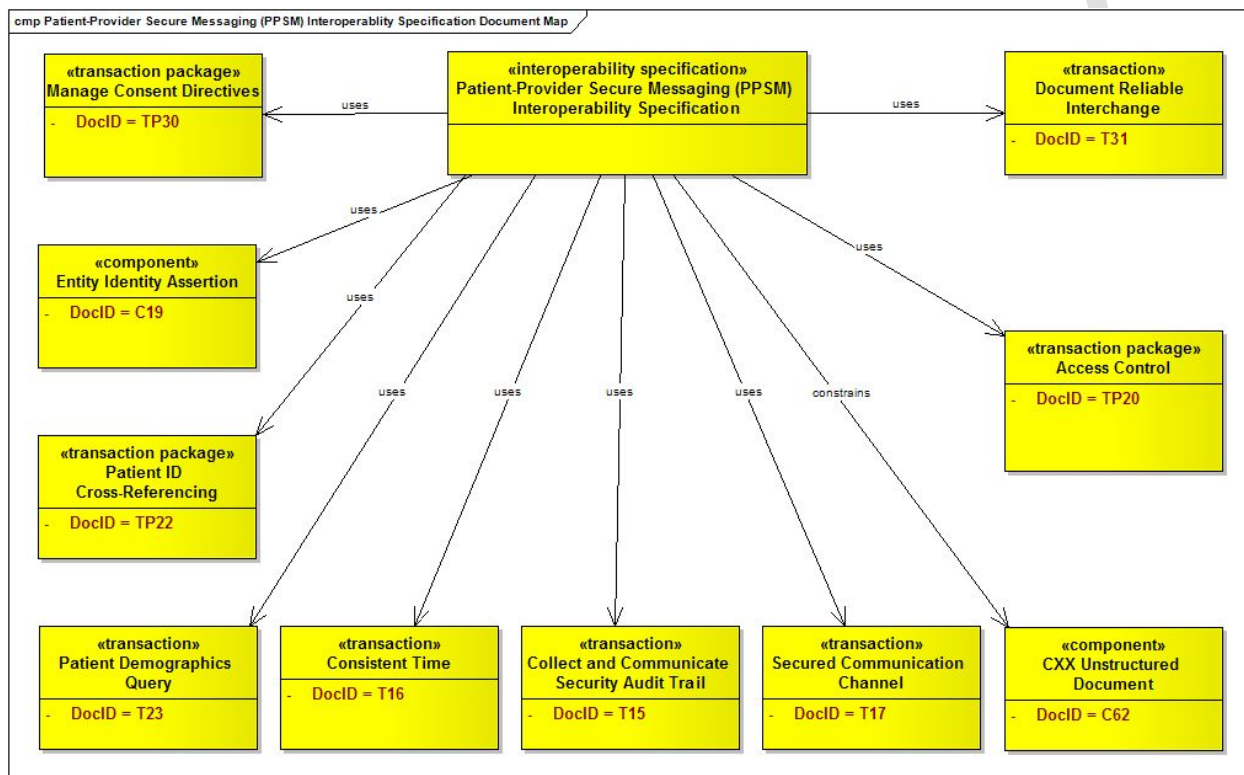
HITSP Construct	Construct Description	Technical Actors	Interoperability or Data Requirement Number	Modification Required
HITSP/TP22 - Patient ID Cross-Referencing	This specification includes by reference the transactions and components that comprise the Patient ID Cross-Referencing Transaction Package. The two transactions within this package are: * The IHE Patient ID Cross-Referencing (PIX) transaction * The IHE Patient Identity Feed transaction	Patient Identifier Cross-Reference Consumer Patient Identifier Cross-Reference Manager Patient Identity Source	Identification of Patient (7.1.1.1, 7.2.1.1, 8.1.1.1)	No
HITSP/T23 - Patient Demographics Query	This PDQ Transaction is intended to provide a 'list patients and their demographics' query / 'patient(s) and their demographics identified' response message pair (QBP^Q22, 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, Volume 2 (ITI TF-2), Revision 3.0: "Patient Demographics Query"	Patient Demographics Consumer Patient Demographics Supplier	Identification of Patient (7.1.1.1, 7.2.1.1, 8.1.1.1)	No
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	Service User Identity Provider Service Provider	Identification of Patient, Secure Messaging System authenticates user and verifies authorization (7.1.1.1, 7.2.1.1, 8.1.1.1)	No
HITSP/T31 – Document Reliable Interchange	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 to support a healthcare delivery organization or clinician who may need to communicate a clinical document to a recipient through direct communication	Document Source Document Recipient	Sharing of Documents, Transmit communication Response, Retrieve Information, Secure messaging system must establish integrity of the message, Message integrity, Notification must indicate where the secure message resides (7.1.4.1, 7.1.3.1, 7.1.5.1, 7.1.2.2, 7.2.1.1, 7.2.3.2, 7.2.4.1, 7.3.3.1, 8.1.2.1, 8.1.3.1, 8.1.4.1, 8.2.3.1, 8.2.3.2, 8.3.2.1, 8.3.2.2)	No



3.2.7 DOCUMENT MAP

The document map summarizes the suite of constructs that are the detailed map to existing standards and specifications used to satisfy the requirements imposed by the Patient-Provider Secure Messaging Use Case. The most effective way to see the construct breakdown is to begin with the document indicated at the top of the diagram.

Figure 3.2.7-1 Requirements, Design and Standards Selection Document Map



4.0 CANDIDATE STANDARDS

This section presents the candidate standards that may support the major Use Case events described in the requirements analysis. During Interoperability Specification development, standards selection will be based on the following process:

- **Evaluation:** The Technical Committee evaluates the standards using the Tier 2 Readiness Criteria. Standards considered for use may include provisional or to be named standards
- **Selection:** Based on the Tier 2 evaluations, named standards are selected and listed in Table 4.1.2-1. 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. During the actual construction of Interoperability Specifications, the Technical Committee may need to refine this listing based on detailed analysis
- **Gap and Overlap Analysis and Recommendations:** The Technical Committee also identifies, and analyzes gaps and overlaps within the standards industry as they related to the specific Use Case. The TC will provide a description of the gaps, including missing or incomplete standards, provide a description of all overlaps, or competition among standards for the relevant Use Cases, and recommendations for resolving these gaps and overlaps

Thus the following section lists a summary of the standards that will be further refined during the Interoperability Specification development phase.

4.1 LIST OF SELECTED AND CANDIDATE STANDARDS

This section presents the selected, and candidate standards that may support the Use Case events described in the requirements analysis. As used by HITSP, the term “standard” refers, but is not limited to Specifications, Implementation Guides, Code Sets, Terminologies, and Integration Profiles. A standard should be produced through a well-defined approach that supports a business process and

1. has been agreed upon by a group of experts
2. has been publicly vetted
3. provides rules, guidelines, or characteristics
4. helps to ensure that materials, products, processes, and services are fit for their intended purpose
5. is available in an accessible format
6. is subject to an ongoing review and revision process

Candidate standards are then evaluated using the HITSP Tier 2 Readiness Criteria. Final selection does not occur until the Interoperability Specifications are completed. Thus there may be additions or deletions to this list.

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



- Regulatory and guidance standards are legal or other authoritative declarations that HITSP must abide by. These may also be guidelines and recommendations that HITSP has adopted to aid in the selection of standards (see Section 4.1.1)
- Selected candidate standards are those candidate standards that are selected within the context of the specific Use Case requirements, and are evaluated for inclusion as part of the Interoperability Specification (see Section 4.1.2)

4.1.1 REGULATORY AND GUIDANCE STANDARDS

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 the Interoperability Specification.

Table 4.1.1-1 Regulatory and Guidance Standards

Standard	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 AND CANDIDATE STANDARDS

This section provides a mapping of candidate standards that may be required to implement the requirements of the Interoperability Specification to the Use Case action codes which are supported.

Section 3.2 provides a description and listing of the new and existing constructs that are used by this Requirements, Design, and Standards Selection specification. Section 3.2.6 describes existing constructs that are expected to be used in this specification without changes (reused), or modified to include additional requirements (repurposed). Selected standards that are used by existing constructs are provided in the published construct specifications available from www.hitsp.org, and are not duplicated in this document. The following table only lists candidate standards that may be selected to meet Use Case requirements for new or repurposed constructs used in this specification. A detailed description of each standard is also provided in the appendix.

Table 4.1.2-1 Selected and Candidate Standards Linked to Requirements

SDO and Standard Name	Event/Action Code	Category (Construct)	Remarks/ Minor Gaps
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Cross Enterprise Sharing of Scanned Documents (XDS-SD)	7.1.2.1, 7.2.3.2, 7.3.2.2, 8.2.3.1, 8.3.2.1	HITSP/C62 – Unstructured Document Component	



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 endorsement 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 Patient Provider Secure Messaging (PPSM) Use Case event. Recommended resolutions were developed through a series of steps including the committee's initial recommendations, cross team validation of the gap, provisional recommendations and peer review by the team.

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

Table 4.2-1 Use Case Events and Associated Gaps

Event Code	Event Description	Identified Gaps	Recommended Resolution
7.1.3 8.1.2	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
7.1.1 7.2.1 8.1.1	Secure messaging system authenticates user and verifies authorization	Partial gap for authenticate consumers (HITSP/C19)	A work item exists in SPI to address the authentication of individuals, and specifically consumers
7.1.5 7.2.1 7.2.2 8.1.4	If requested, system will transmit a notification that the message has been accessed (Read Receipt)	Read receipt is not supported at this time by T31 (XD-R). In addition, this may be a system functionality issue (functional requirement of the PHR or EHR application system) and not an interoperability issue	

4.3 STANDARD OVERLAPS

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



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

Table 4.3-1 Standard Overlaps

Event Code	Event Description	Standard Overlap	Recommended Resolution
No applicable overlaps			



5.0 NEXT STEPS

The first step in the HITSP harmonization process is requirements analysis and design. Upon completion of the Requirements, Design and Standards Selection for the Patient Provider Secure Messaging Use Case, the following steps will occur:

- This document will be submitted to the HITSP Panel and interested Public for comment
- After the comment period, the Technical Committee or Work Group will disposition the comments, maintaining a written log of all dispositions assigned to the TC/WG
- Persuasive comments will be used to inform the construction of the Interoperability Specification (IS)
- Non-persuasive comments or comments that are not applicable to the construction of the IS will be deferred with reason/explanation (e.g., need additional information or further analysis during construction)
- In parallel to the steps described above, the Technical Committee/Work Group will begin the construction of the Interoperability Specifications



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 standards that are referenced by this Requirements, Design, and Standards Selection Specification:

Table 6.1-1 Description of Standards

Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Cross Enterprise Sharing of Scanned Documents (XDS-SD)	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. The latest version of the IHE Technical Framework is available at www.ihe.net .



7.0 CHANGE HISTORY

The following sections provide the history of all changes made to this document since the last publication.

No changes at this time. This is the first published version.

