

HITSP Communicate Clinical Referral Request Capability

HITSP/CAP121



Healthcare Information Technology Standards Panel

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Capabilities Team



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
0.0.1	Review Copy	Capabilities Team	November 9, 2009
0.0.2	Review Copy	Selected Perspective, Domain and/or Tiger Team reviewers	January 18, 2010
1.0	Released for Implementation	Selected Perspective, Domain and/or Tiger Team reviewers	January 25, 2010



TABLE OF CONTENTS

1.0	INTRODUCTION.....	5
1.1	Capability Overview	6
1.2	Scope.....	6
1.3	Copyright Permissions.....	6
1.4	Reference Documents.....	6
1.5	Guidance For Use of a Capability.....	6
2.0	REQUIREMENTS ANALYSIS	8
2.1	Introduction	8
2.2	Requirements	8
2.2.1	Information Exchanges	8
3.0	EXTERNAL CAPABILITY OPTIONS	10
3.1	Security and Privacy	10
3.2	Information Exchange Options	10
4.0	DESIGN SPECIFICATION.....	12
4.1	Requirements Mapped to Constructs	12
4.1.1	Constructs.....	12
4.2	Constraints and Assumptions.....	13
4.3	Specified Interfaces by System Role.....	13
5.0	STANDARDS.....	16
5.1	Standards Used	16
5.1.1	Regulatory Guidance.....	16
5.1.2	Selected Standards	16
5.1.3	Informative Reference Standards.....	21
5.2	Standards Gaps and Overlaps	26
6.0	APPENDIX	27
7.0	DOCUMENT UPDATES	28
7.1	November 9, 2009	28
7.2	January 18, 2010	28
7.2.1	Updates from Public Comment	28
7.3	January 25, 2010	28



FIGURES AND TABLES

Figure 2-1 Information Exchanges Between System Roles	9
Table 1-1 Reader's Guide for Capability	5
Table 1-2 Reference Documents	6
Table 2-1 Reader's Guide for Section 2.0	8
Table 2-2 Capability System Roles	8
Table 2-3 Supported Information Exchanges	8
Table 3-1 Reader's Guide for Section 3.0	10
Table 3-2 Topology Related Options	11
Table 3-3 Content Import Options	11
Table 3-4 Document Content Options	11
Table 4-1 Reader's Guide for Section 4.0	12
Table 4-2 Information Exchanges Mapped to Constructs	12
Table 4-3 Context	13
Table 4-4 Message Sender System Role Mapped to HITSP Construct Interfaces	13
Table 4-5 Message Receiver System Role Mapped to HITSP Construct Interfaces	13
Table 4-6 Document Sender System Role Mapped to HITSP Construct Interfaces	14
Table 4-7 Document Receiver System Role Mapped to HITSP Construct Interfaces	14
Table 4-8 Document Registry and Repository System Roles Mapped to HITSP Construct Interfaces	14
Table 4-9 Implementation Conditions	15
Table 5-1 Reader's Guide for Section 5.0	16
Table 5-2 Regulatory Guidance	16
Table 5-3 Selected Standards	16
Table 5-4 Informative Reference Standards	22
Table 5-5 Information Exchange Requirements (IER) and Associated Standards Gaps	26
Table 5-6 Information Exchange Requirements (IER) and Associated Standards Overlaps	26



1.0 INTRODUCTION

This Healthcare Information Technology Standards Panel (HITSP) document is divided into Requirements Analysis, External Capability Options, Design Specifications and Standards sections which may be used by analysts, architects and implementers. Analysts refer to this document to determine if the Capability satisfies their requirements. Architects and system implementers refer to this document as the architectural specifications for a system design, while software developers will use a Capability as the source of the design for interoperable information exchange. The Appendix lists requirements satisfied by this Capability.

All sections may be useful to analysts and architects. However as shown in Table 1-1, different readers may find specific sections of greater interest and utility. This table is provided as an aid to readers to assist them in identifying sections to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

Table 1-1 Reader's Guide for Capability

Document Section	Section Number	Intended Audience	Information Contained
Section 2.0 Requirements Analysis	2.1 Introduction	Policy Managers Policy Analysts Executive Leadership	Provides an overview of the requirements which this Capability addresses, and identifies the system roles supported by the Capability
	2.2 Requirements	Program Managers Policy Analysts Executive Leadership Architects Business Analysts	Defines the actual information exchanges supported by the Capability in terms of exchange actions and exchange content. It shows how these roles can be assigned at a higher level to real world systems, such as an Electronic Health Record
Section 3.0 External Capability Options	3.1 Security and Privacy	Policy Analysts Architects Business Analysts Developers	Describes the integrated and optional security and privacy functions supported by the Capability
	3.2 Information Exchange Options	Architects Business Analysts Developers	Describes the external information exchange options associated with topology, or message and document content, as applicable
Section 4.0 Design Specification	4.1 Requirements Mapped to Constructs	Program Managers Architects Business Analysts Developers	Maps the information exchanges developed in requirements to the actual HITSP construct used by the Capability to support the exchange
	4.2 Constraints and Assumptions	Business Analysts Developers	Lists the context that is necessary to use the Capability, including constraints, assumptions, pre-conditions, post-conditions and triggers
	4.3 Specified Interfaces by System Role	Business Analysts Developers	Identifies the constructs and their interfaces assigned to each system role. It also lists the implementation conditions for use
Section 5.0 Standards	5.1 Standards Used	Program Managers Policy Analysts Architects Business Analysts Developers	Lists regulatory guidance, selected standards and informative references used by the Capability and all its supporting constructs
	0 Standards Gaps and Overlaps	Program Managers Policy Analysts Architects Business Analysts Developers	Identifies gaps or overlaps in standards to implement the Capability including a plan to resolve issues



1.1 CAPABILITY OVERVIEW

This Capability addresses interoperability requirements that support provider-to-provider (clinical) referral request interaction. It allows the bundling of the referral request document with other relevant clinical documents of interest by utilizing a “folder” designation to associate such documents as shared and that may be made available by other Capabilities such as:

- HITSP/CAP119 Communicate Structured Document
- HITSP/CAP120 Communicate Unstructured Document
- HITSP/CAP133 Communicate Immunization Summary

1.2 SCOPE

A Capability enables business and policy requirements for a business need to be implemented through information exchanges specified in HITSP constructs. The objective of a Capability is to provide the bridge between the business, policy and implementation disciplines by defining a set of information exchanges at a level relevant to policy and business decisions and specifying the use of HITSP constructs sufficiently for implementation. A Capability supports stakeholder requirements and business processes and includes information content, infrastructure, security and privacy. The design of Capabilities leverages existing HITSP constructs and communication methodologies. As new constructs become available, the scope of this Capability may be extended.

1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2010 ANSI. This material may be copied without permission from ANSI only if and to the extent that the text is not altered in any fashion and ANSI's copyright is clearly noted.

1.4 REFERENCE DOCUMENTS

A list of key reference documents and background material is provided in the table below. These documents can be retrieved from [HITSP Web Site](#).

Table 1-2 Reference Documents

Reference Documents	Document Description
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
TN900 – Security and Privacy	TN900 is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs
TN901 - Clinical Documents	TN901 is a reference document that provides the overall context for use of the HITSP Care Management and Health Records constructs
TN903 – Data Architecture	TN903 is a reference document that provides the overall context for use of the HITSP Data Architecture constructs
TN904 – Harmonization Framework and Exchange Architecture	TN904 is a reference document that provides the overall context for use of the HITSP Harmonization Framework and Exchange Architecture constructs

1.5 GUIDANCE FOR USE OF A CAPABILITY

NOTE: For questions related to details on HITSP Capabilities and HITSP System Roles, please refer to HITSP/TN904 Harmonization Framework and Exchange Architecture Technical Note.

To use a HITSP Capability, a HITSP Interoperability Specification or an implementation conformance statement must assign specific systems to one or more HITSP Capability System Roles and identify how the HITSP Capability Options are to be addressed. In order to assign systems to HITSP System Roles, the reader uses Table 2-3 Supported Information Exchanges to determine what systems can support the



specific information exchanges required. For an example of how HITSP System Roles and systems are mapped, readers can consult a HITSP Interoperability Specification Table 3-3 Orchestration of Capabilities by System. In the case of an Implementation Guide, systems can be assigned to HITSP System Roles using a similar methodology.

The use of a HITSP Capability implies that these specific rules will be followed:

- For each HITSP Capability System Role listed in Table 2-2 Capability System Roles, the defined responsibilities of that HITSP Capability System Role are supported. Responsibilities for the HITSP Capability System Role are defined as support for the HITSP Construct interfaces listed in Section 4.3 Specified Interfaces by System Role. Support implies that the system assigned to the HITSP Capability System Role makes the associated HITSP construct interfaces available for use by other systems. For those HITSP construct interfaces in Section 4.3 that have associated content optionality, the HITSP Capability System Role must comply with the optionality condition listed in Table 4-9 Implementation Conditions.
- Responsibilities also include the constraints and assumptions associated with use of a Capability, as outlined in Table 4-3 Context. For those Capabilities with Section 3.2 options, the following additional rules apply:
 1. Each topology option listed in Table 3-2 Topology Related Options should be supported by the implementation
 2. Each content import option listed in Table 3-3 Content Import Options should be supported by the implementation
 3. Each document content option listed in Table 3-4 Document Content Options should be supported by the implementation



2.0 REQUIREMENTS ANALYSIS

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

Table 2-1 Reader's Guide for Section 2.0

Document Section	Section Number	Intended Audience	Information Contained
Section 2.0 Requirements Analysis	2.1 Introduction	Policy Managers Policy Analysts Executive Leadership	Provides an overview of the requirements which this Capability addresses, and identifies the system roles supported by the Capability
	2.2 Requirements	Program Managers Policy Analysts Executive Leadership Architects Business Analysts	Defines the actual information exchanges supported by the Capability in terms of exchange actions and exchange content. It shows how these roles can be assigned at a higher level to real world systems, such as an Electronic Health Record

2.1 INTRODUCTION

Table 2-2 summarizes the system roles of the Capability. Section 2.2 identifies how these system roles participate in the set of information exchanges.

Table 2-2 Capability System Roles

System Role	System Role Definition
Message Sender	The system which sends the clinical referral request message
Message Receiver	The system which receives the clinical referral request message
Document Registry	The system which registers the document within a repository and which responds to a query for documents
Document Repository	The system which stores a copy of the document and forward the document upon request
Document Sender	The system that generates the Clinical Referral Request and other clinical documents
Document Receiver	The system that receives/retrieves the clinical referral request and other clinical documents

2.2 REQUIREMENTS

2.2.1 INFORMATION EXCHANGES

Table 2-3 defines each of the Information Exchanges supported by this Capability in terms of the Exchange Action (EA) or Exchange Content (EC) used.

Table 2-3 Supported Information Exchanges

Information Exchange Identifier	Exchange Action	Exchange Content
A	Send	Clinical Referral Request Message
B	Send and Receive	Referral Summary
B	Send and Receive	Nonrepudiation of Origin Data
B	Send and Receive	Clinical Referral Request



3.0 EXTERNAL CAPABILITY OPTIONS

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

Table 3-1 Reader's Guide for Section 3.0

Document Section	Section Number	Intended Audience	Information Contained
Section 3.0 External Capability Options	3.1 Security and Privacy	Policy Analysts Architects Business Analysts Developers	Describes the integrated and optional Security and Privacy functions supported by the Capability
	3.2 Information Exchange Options	Architects Business Analysts Developers	Describes the external information exchange options associated with topology and message and document content as applicable

This section is primarily for architects, engineers and analysts. It allows those who consider using this Capability to evaluate and/or constrain the options that are externally made available for the Capability implementers.

Interoperability among system roles defined by this Capability often requires the selection of consistent options.

3.1 SECURITY AND PRIVACY

The application of Security and Privacy is highly influenced by the security and privacy policies. The HITSP Security and Privacy Technical Note (HITSP/TN900) provides a detailed discussion of the security and privacy constructs, including consideration and appropriate context for needed security and privacy related policy decisions. Security and privacy constructs are integrated comprehensively into the Service Collaborations. The actual constructs used and the way in which the constructs are used is dependent on the policies and physical setting. Conformance claims are against the security and privacy constructs that are chosen to enforce the policies.

3.2 INFORMATION EXCHANGE OPTIONS

Three types of information exchange options are externally offered by this Capability:

- Topology Related Options
- Content Import Options
- Document Content Options

The HITSP Exchange Architecture adds topology to the HITSP Harmonization Framework. Topology is the arrangement or mapping of networked Systems, especially the physical (real) and logical (virtual) interconnections between Systems. A Health Information Exchange¹ (HIE) is a special network system that provides intermediary services, such as directories, registries or translations. HITSP supports the following topologies:

¹ The terms "RHIO" and "Health Information Exchange" or "HIE" are often used interchangeably. An HIE is a more general instance of a RHIO (Regional Health Information Organization). Both are a grouping of organizations with a business stake in improving the quality, safety and efficiency of healthcare delivery. NHIEs are HIEs that support the building blocks of the Nationwide Health Information Network (NHIN) initiative proposed by the Office of the National Coordinator (ONC) for Health Information Technology (HIT). To build a nationwide network of interoperable healthcare records, the effort must first develop at the local and state levels. The concept of NHIN requires extensive collaboration by a diverse set of stake holders. The challenges are many to achieve success for an HIE or a RHIO.



- Portable Media (non-connected)
- System to System (point-to-point)
- System to HIE
- HIE to HIE

The following matrix portrays which of the typical network topologies (see HITSP/TN904 for details on topologies) are addressed within the Capability. Within each cell, “Available” indicates that the topology is supported while “Not Available” indicates that the topology is not supported.

Table 3-2 Topology Related Options

Topology	Available or Not Available
Point-to-Point Direct	Available
E-mail	Available
Portable Media	Available
Document Share/Community	Available

In addition to providing topology options, a Capability may provide Information Content Import Options (see Table 3-3 Content Import Options). Note that subsets of the data content can be sent as appropriate for the Capability; but the responding system must be able to address the entire data content corresponding to the Exchange Content supported. Content subsets should be specified in the document that uses this Capability – either an Interoperability Specification or an implementation design document.

Table 3-3 Content Import Options

Document Display	Document Import	Document Discrete Data Import
Integrated	Option	Option

Two content import options are offered:

- **Document Import Option** impacts the import of Documents processed by a Content Consumer interface. It requires the Document Consumer to have the ability to import into the healthcare record one or more of the received documents as a whole and display it as requested
- **Discrete Data Import Option** impacts the import of the HL7 CDA Documents processed by a Content Consumer interface. It requires the Document Consumer to have the ability to import the discrete data from one or more of the data modules in a structured form into the healthcare record. Coded values shall be maintained

This Capability supports the HITSP/C83 Clinical Document Architecture (CDA) Modules document profiles listed in Table 3-4. Any use of this Capability by either an Initiating or a Responding System MUST support at least one of the HITSP CDA documents listed below.

Table 3-4 Document Content Options

Optionality	Supported Document Types
R	Encounter Document Using IHE Medical Summary (XDS-MS) (HITSP/C48)
O	Nonrepudiation of Origin Document Component (HITSP/C26)

Optionality Legend: “R” for Required, “O” for Optional, or “C” for Conditional

Please note that at least one of the options shall be supported either by the Initiating System or the Responding System.



4.0 DESIGN SPECIFICATION

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

Table 4-1 Reader's Guide for Section 4.0

Document Section	Section Number	Intended Audience	Information Contained
Section 4.0 Design Specification	4.1 Requirements Mapped to Constructs	Program Managers Architects Business Analysts Developers	Maps the information exchanges developed in requirements to the actual HITSP construct used by the Capability to support the exchange
	4.2 Constraints and Assumptions	Business Analysts Developers	Lists the context that is necessary to use the Capability, including constraints, assumptions, pre-conditions, post-conditions and triggers
	4.3 Specified Interfaces by System Role	Business Analysts Developers	Identifies the constructs and their interfaces assigned to each system role. It also lists the implementation conditions for use

4.1 REQUIREMENTS MAPPED TO CONSTRUCTS

4.1.1 CONSTRUCTS

Table 4-2 defines the mapping of the Information Exchanges supported by this Capability in terms of the Exchange Action (EA), Exchange Content (EC) and any Constraints applied to the Information Exchange with specific initiating and/or responding system interfaces. This provides the traceability of constructs to the information exchanges identified in Section 2.0 above. Content modules and terminology Components are not listed here because they are referenced by other constructs, but do not provide an interface. HITSP/TN903 discusses how content modules and terminology Components are referenced by other constructs.

Table 4-2 Information Exchanges Mapped to Constructs

Information Exchange Identifier	Exchange Type	Construct Identifier	Description
A – Send and Receive Clinical Referral Trigger	Action	HL7 Messaging (HITSP/SC115)	The HITSP HL7 Messaging Service Collaboration provides the Capability to send and receive HL7 messages. This Service Collaboration applies the necessary Security and Privacy constructs
A – Send and Receive Clinical Referral Trigger	Content	Clinical Referral Request Message Transaction (HITSP/T67)	The HITSP Clinical Referral Request Transport Transaction will be used to transport the provider to provider (clinical) referral request interaction. It is based on the IHE Document-based Referral Request (DRR) profile which is used to bundle a referral request document with other relevant clinical documents of interest and optionally to send a trigger message to the receiving provider system
B – Send and Receive Clinical Referral Request	Action	Healthcare Document Management (HITSP/SC112)	The HITSP Healthcare Document Management Service Collaboration provides the ability to share healthcare documents using a set of topologies, such as Media, e-Mail, Point-to-Point, Shared within a Health Information Exchange, and Shared within a larger community (made up of potentially diverse Health Information Exchanges)



Information Exchange Identifier	Exchange Type	Construct Identifier	Description
B – Send and Receive Clinical Referral Request	Content	Encounter Document Using IHE Medical Summary (XDS-MS) Document Component (HITSP/C48)	The Encounter Document Using IHE Medical Summary (XDS-MS) Component supports the process of sending patient encounter data (excluding laboratory and radiology) in a document sharing functional flow scenario. Patient encounter data are captured as part of the normal process of care performed by healthcare providers, such as hospitals, emergency departments and outpatient clinics
B – Send and Receive Clinical Referral Request	Content	Clinical Referral Request Message Transaction (HITSP/T67)	The HITSP Clinical Referral Request Transport Transaction will be used to transport the provider to provider (clinical) referral request interaction. It is based on the IHE Document-based Referral Request (DRR) profile which is used to bundle a referral request document with other relevant clinical documents of interest and optionally to send a trigger message to the receiving provider system
B – Send and Receive Clinical Referral Request	Content	Nonrepudiation of Origin Document Component (HITSP/C26)	The Nonrepudiation of Origin Component provides the mechanisms to support Nonrepudiation of Origin, which refers to both the proof of the integrity and origin of documents in a high-assurance manner, which can be verified by any party. This Component does not provide Nonrepudiation of Receipt

4.2 CONSTRAINTS AND ASSUMPTIONS

Table 4-3 specifies the context that must be provided in order to use the Capability, identifying any assumptions, pre-conditions, post-conditions, and triggers relevant for use of the Capability.

Table 4-3 Context

Assumptions, Pre-conditions, Post-conditions, and Triggers	Type of Context
Need for patient referral has been identified	Trigger
Pre-authorization or approval already received or determined not to be required	Assumption

4.3 SPECIFIED INTERFACES BY SYSTEM ROLE

This section specifies the HITSP Capability interfaces in terms of the System Roles identified in Table 2-2 Capability's System Roles.

Table 4-4 below specifies interfaces for the message sender system role as defined in Table 2-2.

Table 4-4 Message Sender System Role Mapped to HITSP Construct Interfaces

Construct Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Send HL7 Message	Initiating	HL7 Messaging (HITSP/SC115)	R
N/A	Initiating	Clinical Referral Request (HITSP/T67)	R

Optionality Legend: "R" for Required, "O" for Optional, or "C" for Conditional

Table 4-5 below specifies interfaces for the message receiver system role as defined in Table 2-2.

Table 4-5 Message Receiver System Role Mapped to HITSP Construct Interfaces

Construct Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
---------------------	----------------	--------------------	--------------------------



Receive HL7 Message	Responding	HL7 Messaging (HITSP/SC115)	R
N/A	Responding	Clinical Referral Request Transport (HITSP/T67)	R

Optionality Legend: "R" for Required, "O" for Optional, or "C" for Conditional

Table 4-6 below specifies interfaces for the document sender system role as defined in Table 2-2.

Table 4-6 Document Sender System Role Mapped to HITSP Construct Interfaces

Construct Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Send Document	Initiating	Healthcare Document Management (HITSP/SC112)	C[101]
N/A	Initiating	Encounter Document Using IHE Medical Summary (HITSP/C48)	R
N/A	Initiating	Nonrepudiation of Origin (HITSP/C26)	C[102]
Referral Requestor	Initiating	Clinical Referral Request (HITSP/T67)	R

Optionality Legend: "R" for Required, "O" for Optional, or "C" for Conditional

Table 4-7 below specifies interfaces for the document receiver system role as defined in Table 2-2.

Table 4-7 Document Receiver System Role Mapped to HITSP Construct Interfaces

Construct Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Receive Document	Responding	Healthcare Document Management (HITSP/SC112)	C[103]
N/A	Responding	Encounter Document Using IHE Medical Summary (HITSP/C48)	R
N/A	Responding	Nonrepudiation of Origin (HITSP/C26)	C[102]
Referral Dispatcher	Responding	Clinical Referral Request (HITSP/T67)	R

Optionality Legend: "R" for Required, "O" for Optional, or "C" for Conditional

Table 4-8 below specifies interfaces for the document registry and repository system role as defined in Table 2-2.

Table 4-8 Document Registry and Repository System Roles Mapped to HITSP Construct Interfaces

Construct Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Send Document	Initiating	Healthcare Document Management (HITSP/SC112)	C[104]
N/A	Initiating	Encounter Document Using IHE Medical Summary (HITSP/C48)	R
N/A	Initiating	Nonrepudiation of Origin (HITSP/C26)	C[102]
Receive Document	Responding	Healthcare Document Management (HITSP/SC112)	C[104]
N/A	Responding	Encounter Document Using IHE Medical Summary (HITSP/C48)	R
N/A	Responding	Nonrepudiation of Origin (HITSP/C26)	C[102]

Optionality Legend: "R" for Required, "O" for Optional, or "C" for Conditional

Table 4-9 specifies optionality conditions referenced in Table 4-4 through Table 4-8 above.



Table 4-9 Implementation Conditions

Condition ID	Condition Description
C[101]	The implementation SHALL support the appropriate specializations of the Send Document interface for each topology supported
C[102]	SHALL apply HITSP/C26 where nonrepudiation is required by the jurisdiction or information sharing agreements
C[103]	The implementation SHALL support the appropriate specializations of the Receive Document interface for each topology supported
C[104]	This system role and interface is required if the information exchange topology utilized deploys one or more HIE's which SHALL support the Send/Consume Documents via Share interface described in HITSP/SC112



5.0 STANDARDS

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

Table 5-1 Reader's Guide for Section 5.0

Document Section	Section Number	Intended Audience	Information Contained
Section 5.0 Standards	5.1 Standards Used	Program Managers Policy Analysts Architects Business Analysts Developers	List regulatory guidance, selected standards and informative references used by the Capability and all its supporting constructs
	0 Standards Gaps and Overlaps	Program Managers Policy Analysts Architects Business Analysts Developers	Identifies gaps or overlaps in standards to implement the Capability including a plan to resolve issues

5.1 STANDARDS USED

5.1.1 REGULATORY GUIDANCE

Table 5-2 lists any regulatory guidance that determines or constrains use of standards.

Table 5-2 Regulatory Guidance

Regulation	Description
Health Insurance Portability and Accountability Act (HIPAA) -- Administrative Simplification	A listing of national standards plus rules adopted by federal regulation for electronically communicating specified administrative and financial healthcare transactions, and protecting the security and privacy of healthcare information, as applied to the three types of defined covered entities: health plans, healthcare clearinghouses, and healthcare providers who conduct any of the specified healthcare transactions. See the Code of Federal Regulations, Title 45, Parts 160, et. seq. for more information

5.1.2 SELECTED STANDARDS

Table 5-3 lists the standards selected as relevant to this Capability.

Table 5-3 Selected Standards

Standard	Description
American Society for Testing and Materials (ASTM International) Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	Defines a document structure for use by electronic signature mechanisms, describes the characteristics of an electronic signature process. Defines minimum requirements for different electronic signature mechanisms, defines signature attributes for use with electronic signature mechanisms, describes acceptable electronic signature mechanisms and technologies, defines minimum requirements for user identification, access control, and other security requirements for electronic signatures, and outlines technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism. For more information visit www.astm.org
Digital Imaging and Communications in Medicine (DICOM) Part 3.12: Media Formats and Physical Media for Media Interchange	This DICOM Standard describes the services and the data necessary for the interchange of information between digital imaging computer systems found in healthcare settings. PS 3.12 of the DICOM Standard articulates the structure between the Media Storage Model and specific media. Media physical characteristics are also covered. For more information visit medical.nema.org



Standard	Description
European Telecommunications Standards Institute (ETSI) Technical Specification TS 101 903: XML Advanced Electronic Signatures (XAdES)	Extends the IETF/W3CXML-Signature Syntax and Processing specification [XMLDSIG] into the domain of nonrepudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the European Directive. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature. An advanced electronic signature aligned with this document can, in consequence, be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later. For more information visit www.etsi.org
Health Level Seven (HL7) HL7 Version 3 Standard: Clinical Document Architecture (CDA), Release 2	The HL7 Clinical Document Architecture is an XML-based document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA is one instantiation of HL7's Version 3.0 Reference Information Model (RIM) into a specific message format. Of particular focus for HITSP Interoperability Specifications are message formats for Laboratory Results and Continuity of Care (CCD) documents. Release 2 of the HL7 Clinical Document Architecture (CDA) is an extension to the original CDA document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA R2 includes a prose document in HTML, XML schemas, data dictionary, and sample CDA documents. CDA R2 further builds upon other HL7 standards beyond just the Version 3.0 Reference Information Model (RIM) and incorporates Version 3.0 Data Structures, Vocabulary, and the XML Implementation Technology Specifications for Data Types and Structures. For more information visit www.hl7.org
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	The Healthcare Permission Catalog provides the necessary content for creating interoperable roles facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit www.hl7.org
Health Level Seven (HL7) Version 2.3.1 Chapter 2 – Control, Chapter 3 – Patient Administration	The HL7 Version 2.3.1 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets/code tables are contained in the standard. For more information visit www.hl7.org
Health Level Seven (HL7) Version 2.5, Chapter 2 – Control, Chapter 3 – Patient Administration, Chapter 5 - Query	The HL7 Version 2.5 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets/code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. For more information visit www.hl7.org
Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	The Data Consent RMIM captures the data and associations needed to (1) record or report a consumer's consent or dissent to authorize the access, collection, use, or disclosure of personally identifiable information; (2) convey a provider's request or intent to override a patient's recorded consent or dissent; (3) convey a type of consent directive associated with a privacy policy; or (4) to record or report a consumer's consent directive, which is to be applied to future access, collection, use or disclosure of personally identifiable information. For more information visit www.hl7.org
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	Specifies the use of digital signatures for documents that are shared between organizations. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2008-2009 Document-based Referral Request (DRR)	This profile describes how to relate a referral request document with relevant clinical documents, communicate the group of documents to a referral dispatcher with an optional online transaction to trigger the referral and communicate acceptance. For more information visit www.ihe.net



Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Section 10 Cross-Enterprise Document Sharing (XDS.a)	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. Section 10, Cross-Enterprise Document Sharing facilitates the registration, distribution and access across health enterprises of patient electronic health records. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The Registry Stored Query Transaction Trial Implementation Supplement specifies an IHE transaction that provides optimization and implementation simplification. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2008-2009, Cross-Community Access (XCA), Trial Implementation, October 10, 2008	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The trial implementation version of the XCA Supplement to the ITI-Technical Framework, specifies the IHE transactions that support access between communities in a manner compatible with the XDS Integration profile. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	The Cross-Enterprise Document Sharing-B Profile (XDS.b) supplement provides a new implementation choice for the Cross-Enterprise Document Sharing (XDS) Integration Profile based on use of the Web Services and ebXML Reg/Rep standards that is consistent with current developments and best practices in the industry. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) 2007-2008 Trial Implementation Supplement Cross-enterprise Document Reliable Interchange (XDR) Release 3	This Supplement to the IHE IT Infrastructure Technical Framework provides a generic, standards based mechanism for conveying a set of medical documents in a point-to-point networked based communication. The current version of the XDR is specified in the XDR Trial Implementation Supplement to the ITI-TF, rev. 5.0, which is consistent with IHE XDS.b Supplement in term of document entry metadata. For more information visit www.ihe.net/technical_framework NOTE: off-line mode transaction expected to be updated once standards are available for Web Services Off-line
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 or later, Cross-Enterprise Document Media Interchange (XDM) Integration Profile	Provides document interchange using a common file and directory structure over several standard media types. This permits the patient to use physical media to carry medical documents. This also permits the use of person-to-person email to convey medical documents. XDM supports the transfer of data about multiple patients within one data exchange. Visit www.ihe.net for more information
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement 2007 – 2008, Notification of Document Availability Integration Profile, Draft for Trial Implementation, October 10, 2008	The Notification of Document Availability Profile (NAV) introduces a mechanism allowing notifications to be sent point-to-point to systems within a Cross-Enterprise Document Sharing affinity domain (See IHE IT Infrastructure XDS Integration Profile), eliminating the need for manual steps or polling mechanisms for a Document Consumer to be aware that documents that may be of interest have been registered with an XDS Document Registry Interface. For further information, visit www.ihe.net



Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially interface specific requirements. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework, Revision 4.0 or later, Personnel White Pages profile	The Personnel White Pages (PWP) Profile provides access to basic directory information on human workforce members to other workforce members within the enterprise. This information has broad use among many clinical and non-clinical applications across the healthcare enterprise. This Personnel White Pages Profile specifies a method of finding directory information on the User Identities (user@realm) supplied by the Enterprise User Authentication (EUA) Integration Profile. For more information, visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially interface specific requirements. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Consistent Time (CT) Integration Profile	The Consistent Time Integration Profile (CT) provides a means to ensure that the system clocks and time stamps of the many computers in a network are well synchronized. This profile specifies synchronization with a median error less than 1 second. This is sufficient for most purposes. The current version of the ITI-TF Final Text, specifies the IHE CT Integration Profile, and other transactions defined and implemented as of October 10, 2008. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 or later, Patient Demographics Query (PDQ) Integration Profile	Provides ways for multiple distributed applications to query a central patient information server for a list of patients, based on user-defined search criteria, and retrieve a patient's demographic (and, optionally, visit or visit-related) information directly into the application. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2008 - 2009, Pediatric Demographics, Draft for Trial Implementation (August 22, 2008)	The experience of immunization registries and other public health population databases has shown that matching and linking patient records from different sources for the same individual person in environments with large proportions of pediatric records requires additional demographic data. Pediatric Demographics makes use of the following six additional demographic fields to aid record matching in databases with many pediatric records. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles, offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. The latest version of the IHE Technical Framework is available at www.ihe.net



Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Patient Identifier Cross-Referencing Integration Profile (PIX)	The Patient Identifier Cross-referencing Integration Profile (PIX) is targeted at healthcare enterprises of a broad range of sizes (hospital, a clinic, a physician office, etc.). It supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains via the following interactions: 1) The transmission of patient identity information from an identity source to the Patient Identifier Cross-reference Manager. 2) The ability to access the list(s) of cross-referenced patient identifiers either via a query/response or via update notification. By specifying the above transactions among specific interfaces, this integration profile does not define any specific enterprise policies or cross-referencing algorithms. By encapsulating these behaviors in a single interface, this integration profile provides the necessary interoperability while maintaining the flexibility to be used with any cross-referencing policy and algorithm as deemed adequate by the enterprise. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2008 - 2009, Pediatric Demographics, Draft for Trial Implementation (August 22, 2008)	The experience of immunization registries and other public health population databases has shown that matching and linking patient records from different sources for the same individual person in environments with large proportions of pediatric records requires additional demographic data. Pediatric Demographics makes use of the following six additional demographic fields to aid record matching in databases with many pediatric records. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. Section 10, Cross-Enterprise Document Sharing facilitates the registration, distribution and access across health enterprises of patient electronic health records. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	The Cross-Enterprise Document Sharing-B Profile (XDS.b) supplement provides a new implementation choice for the Cross-Enterprise Document Sharing (XDS) Integration Profile based on use of the Web Services and ebXML Reg/Rep standards that is consistent with current developments and best practices in the industry. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The Registry Stored Query Transaction Trial Implementation Supplement specifies an IHE transaction that provides optimization and implementation simplification. This supplement is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The trial implementation version of the XCA Supplement to the ITI-TF, rev. 4.0 Final Text, specifies the IHE transactions that support access between communities in a manner compatible with the XDS Integration profile. This supplement is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) – Trial Implementation	The Basic Patient Privacy Consents (BPPC) profile provides a mechanism to record the patient privacy consent(s), a method to mark documents published to XDS with the patient privacy consent that was used to authorize the publication, and a method for XDS Consumers to use to enforce the privacy consent appropriate to the use. This profile complements XDS by describing a mechanism whereby an XDS Affinity Domain can develop and implement multiple privacy policies, and describes how that mechanism can be integrated with the access control mechanisms supported by the XDS Interfaces (e.g. systems). There are two key parts of the profile: 1) It provides a document content specification for capturing a patient acknowledgement of a privacy consent policy or policies. 2) It describes the method by which XD* Interfaces can enforce the privacy policies determined by the document confidentialityCode related to the patient privacy consents. The latest version of specification is available at www.ihe.net



Standard	Description
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC), Revision 4.0, 2008 - 2009, Cross-Enterprise Sharing of Medical Summaries (XDS-MS) Integration Profile	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementations (called Integration Profiles) of established standards to deal with integration issues that cross providers, patient problems or time. The Cross Enterprise Document Sharing of Medical Summaries (XDS-MS) Integration Profile enables sharing of health information between enterprises of a regional health network, and further describes how to map content in a CDA medical document into registry metadata. In the registry, healthcare providers publish pointers to documents stored in distributed repositories. Other healthcare providers may search and retrieve these and other documents. For more information visit www.ihe.net
International Organization for Standardization (ISO) Health informatics - 9660 Level 1	Defines a common logical format for files and directories so discs written to ISO 9660 specifications can be read by a wide array of computer operating systems. For more information visit www.iso.org
International Organization for Standardization (ISO) Health Informatics - Pseudonymization, Technical Specification # 25237 (ISO TS25237)	Health Informatics – Pseudonymization. Approved as a Technical Specification March, 2007. Visit www.iso.org for more information
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	Describes the Network Time Protocol (NTP): the mechanisms to synchronize time and coordinate time distribution in a large, diverse Internet operating at rates from mundane to lightwave. For more information visit www.ietf.org
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996	Describes the Simple Network Time Protocol (SNTP) Version 4, which is an adaptation of the Network Time Protocol (NTP). SNTP can be used when the ultimate performance of the full NTP implementation is not needed or justified. When operating with current and previous NTP and SNTP versions, SNTP Version 4 involves no changes to the NTP specification or known implementations, but is rather a clarification of certain design features of NTP. For more information visit www.ietf.org
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) Core v2.0 OASIS Standard; ITU-T X.1141	SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	Defines extensions that build on [WS-Security] to provide a framework for requesting and issuing security tokens, and to broker trust relationships. Defines Security Token Service (STS) model for security tokens including requesting, issuing, renewing, canceling and validating. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	The Organization for the Advancement of Structured Information Standards (OASIS) standards group developed the eXtensible Access Control Markup Language (XACML) as a language to express and evaluate access decisions. The XACML technical specification includes a profile for RBAC using XACML that complies with the ANSI RBAC standard. The HL7 RBAC Permission Catalog provides a standard vocabulary that can be used for cross-enterprise access control. For more information visit www.oasis-open.org
USB Removable Device Type 2.0 (USB Implementers Forum)	The USB-IF was formed to provide a support organization and forum for the advancement and adoption of Universal Serial Bus technology. The Forum facilitates the development of high-quality compatible USB peripherals (devices), and promotes the benefits of USB and the quality of products that have passed compliance testing. For more information visit www.usb.org

5.1.3 INFORMATIVE REFERENCE STANDARDS

Table 5-4 includes reference standards that inform the overall semantic interoperability.



Table 5-4 Informative Reference Standards

Standard	Description
American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS), #359-2004	This standard describes RBAC features that have achieved acceptance in the commercial marketplace. It includes a reference model and functional specifications for the RBAC features defined in the reference model. It is intended for (1) software engineers and product development managers who design products incorporating access control features; and (2) managers and procurement officials who seek to acquire computer security products with features that provide access control capabilities in accordance with commonly known and understood terminology and functional. For more information visit www.ansi.org
American Society for Testing and Materials ASTM International #E1986 -98 (2005) Standard Guide for Information Access Privileges to Health Information	The guide covers the process of granting and maintaining access privileges to health information. In particular, Table 2 Healthcare Personnel that Warrant Differing Levels of Access Control provides the necessary content for structural roles per ASTM International E2595 and for user-based access controls enforcing patient consent directives
ASTM International Standard Guide for Privilege Management Infrastructure (PMI) Guidelines: #E2595-07	Defines interoperable mechanisms to manage privileges in a distributed environment. This standard is oriented towards support of a distributed or service-oriented architecture (SOA) where security services are themselves distributed and applications are consumers of distributed services. This standard incorporates privilege management mechanisms alluded to in a number of existing standards (e.g., E1986, E2084). The privilege mechanisms in this standard support policy-based access control (including role, entity and contextual-based access control) including the application of policy constraints, patient requested restrictions and delegation. Finally, the standard supports hierarchical, enterprise-wide privilege management. The mechanisms defined in this standard may be used to support a privilege management infrastructure (PMI) using existing public key infrastructure (PKI) technology. This standard does not specifically support mechanisms based on secret-key cryptography. Mechanisms involving privilege credentials are specified in International Organization for Standardization (ISO) 9594-8:2000 (attribute certificates), and Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) (attribute assertions); however, this standard does not mandate or assume the use of such standards. Many current systems require only local privilege management functionality (on a single computer system). Such systems frequently use proprietary mechanisms. This standard does not address this type of functionality; rather, it addresses an environment where privileges and capabilities (authorizations) must be managed between computer systems across the enterprise, and with business partners. For more information visit www.astm.org http://www.astm.org/
ASTM International Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems: # E2147-01	E2147-01 "is for the development and implementation of security audit/disclosure logs for health information. It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of health information to external users for use in manual and computer systems. The process of information disclosure and auditing should conform, where relevant, with the Privacy Act of 1974 (1)." For more information visit www.astm.org
Health Level Seven (HL7) Consent related vocabulary including Confidentiality Codes	HL7 concept domains, including ConfidentialityCodes, ActInformationCategoryCode, ActInformationAccessType, ActInformationAccessContextCode, AuthorizedParticipationFunctionCode, ActPolicyType, ActConsentType, and ActMaskableCode For more information visit www.hl7.org
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	The Healthcare Permission Catalog provides the necessary content for creating interoperable roles facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit www.hl7.org



Standard	Description
Health Level Seven (HL7) Version 2.5.2	The HL7 Version 2.5 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets/code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. Of particular focus for HITSP Interoperability Specifications are message formats described in Chapters 2, 3, 5, and 7 including patient demographic (ADT) and lab result reporting. These are also used within composite standards from IHE for Patient Identity Cross-Referencing and Feed (PIX), Patient Demographics Query (PDQ), and Acknowledgements. Visit www.hl7.org for more information
In International Organization for Standardization (ISO) Health Informatics – Functional and Structural Roles (ISO SF Roles), Technical Specification #21298 , Draft May, 2007	This document contains a specification for encoding information related to roles for health professionals and consumers. At least four areas have been identified where a model for encoding role information is needed. 1. Privilege management and access control: role-based access control is not possible without an effective means of recording role information for healthcare interfaces. 2. Directory services: structural roles are usefully recorded within directories of healthcare providers (see for example, ISO TS 21091 Health Informatics – Directory services for security, communications, and identification of professionals and patients). 3. Audit trails: functional roles are usefully recorded within audit trails for health information applications. 4. Public key infrastructure (PKI): The three part ISO standard 17090 Health Informatics – Public Key Infrastructure (PKI) allows for the encoding of healthcare roles in certificate extensions, but no structured vocabulary for such roles is specified. This technical specification identifies such a coded vocabulary. For more information visit http://www.iso.org/www.iso.org
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 or later	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, Final Text, specifies the IHE transactions defined and implemented as of October 10, 2008. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Volume 2 Transactions, Appendix M Using Patient Demographics Query in a Multi-Domain Environment	Appendix M - Using Patient Data Query (PDQ) in a Multi-Domain Environment, provides an architectural discussion of how Query Parameter Definition, QPD-8 is processed
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication Profile (ATNA)	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially interface specific requirements. For more information visit www.ihe.net

² HITSP references HL7 2.5.1 messaging for lab results reporting and HL7 2.5 for other messages. Future maintenance work will move toward referencing a single HL7 version across HITSP documents.



Standard	Description
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC), Revision 4.0, 2008 - 2009, Emergency Department Referral Integration ProfileNo applicable informative reference standards	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementations (called Integration Profiles) of established standards to deal with integration issues that cross providers, patient problems or time. The Emergency Department Referral (EDR) Integration Profile enables the emergency department to provide information including the nature of the current problem, past medical history and medications with the person who will ultimately care for the patient. For more information visit www.ihe.net
International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®)	SNOMED CT consists of a technical design, core content architecture, and Core content. SNOMED CT Core content includes the technical specification of SNOMED CT and fully integrated multi-specialty clinical content. The Core content also includes a concepts table, description table, relationships table, history table, ICD-9-CM mapping, and Technical Reference Guide. Additionally, SNOMED CT provides a framework to manage language dialects, clinically relevant subsets, qualifiers and extensions, as well as concepts and terms unique to particular organizations or localities. For more information visit www.ihtsdo.com
International Organization for Standardization (ISO) Health Informatics -- Information technology -- Open Systems Interconnection -- Systems Management: Security alarm reporting function, Technical Specification #10164-- Part 7: Security Alarm Reporting Function, 1992	Establishes user requirements for the service definition needed to support the security alarm reporting function, defines the service provided by the security alarm reporting function, specifies the protocol that is necessary in order to provide the service, defines the relationship between the service and management notifications, defines relationships with other systems management functions, specifies conformance requirements. The security alarm reporting function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information for the purpose of systems management. For more information visit www.iso.org
International Organization for Standardization (ISO) Health Informatics -- Information technology -- Text and office systems - Office Document Architecture (ODA) and interchange format, Technical Report on ISO 8613 implementation testing, Technical Specification # ISO/IEC CD 10183 -- Part 3: Testing procedure	Specifies a general framework for the provision of access control. The purpose of access control is to counter the threat of unauthorized operations involving a computer or communication system. For more information visit www.iso.org
International Organization for Standardization (ISO) Health Informatics -- Privilege management and access control (PMAC), Technical Specification #22600 -- Part 1: Overview and policy management, July 2006	Supports the needs of healthcare information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, their patients, staff members and trading partners. It is also intended to support inquiries from both individuals and application systems. For more information visit www.iso.org
Internet Engineering Task Force (IETF), HTTP HyperText Transfer Protocol HTTP/1.1 (RFC 2616)	The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol, which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers [47]. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred. For more information visit www.ietf.org
Internet Engineering Task Force (IETF), MIME Multipurpose Internet Message Extensions (RFC 2045 to RFC 2049)	The first and second documents in this set define MIME header fields and the initial set of MIME media types. The third document describes extensions to RFC 822 formats to allow for character sets other than US-ASCII. The fourth document describes what portions of MIME must be supported by a conformant MIME implementation. It also describes various pitfalls of contemporary messaging systems as well as the canonical encoding model MIME is based on. For more information visit www.ietf.org
Internet Engineering Task Force (IETF), SMTP Simple Mail Transfer Protocol (RFC 2821)	The objective of the Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently. SMTP is independent of the particular transmission subsystem and requires only a reliable ordered data stream channel. While this document specifically discusses transport over TCP, other transports are possible. For more information visit www.ietf.org
Internet Engineering Task Force (IETF), The MIME Multipart/Related Content-type (RFC 2387)	The Multipart/Related content-type provides a common mechanism for representing objects that are aggregates of related MIME body parts. This document defines the Multipart/Related content-type and provides examples of its use. For more information visit www.ietf.org



Standard	Description
Organization for the Advancement of Structured Information Standards (OASIS) - ebMS OASIS/ebXML Messaging Services Specifications v2.1	Defines a Message Service protocol for reliable Business-to-Business data interchange. ebMS v2.1 adds quality of service features on top of transfer protocols such as HTTP and SMTP. Key qualities of service features include guaranteed delivery and nonrepudiation of receipt. ebMS v2.1 can reliably transfer any data type including XML, X12, EDIFACT, or binary data between two parties over the Internet. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) - ebRIM OASIS – ebXML Registry Information Model v2.1	The Registry Information Model provides a blueprint or high-level schema for the ebXML Registry. Its primary value is for implementers of ebXML Registries. It provides these implementers with information on the type of metadata that is stored in the Registry as well as the relationships among metadata Classes. The Registry information model: a) Defines what types of objects are stored in the Registry; b) Defines how stored objects are organized in the Registry. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) - ebRS OASIS – ebXML Registry Services Specifications v2.1	The ebXML Registry provides a set of services that enable sharing of information between interested parties for the purpose of enabling business process integration between such parties based on the ebXML specifications. The shared information is maintained as objects in a repository and managed by the ebXML Registry Services defined in this document. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) – ebXML Registry Information Model (3.0)	The Registry Information Model provides a blueprint or high-level schema for the ebXML Registry. Its primary value is for implementers of ebXML Registries. It provides these implementers with information on the type of metadata that is stored in the Registry as well as the relationships among metadata Classes. The Registry information model: a) Defines what types of objects are stored in the Registry; b) Defines how stored objects are organized in the Registry. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) – ebXML Registry Services Specification (3.0)	The ebXML Registry provides a set of services that enable sharing of information between interested parties for the purpose of enabling business process integration between such parties based on the ebXML specifications. The shared information is maintained as objects in a repository and managed by the ebXML Registry Services defined in this document. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) WS-Federation Web Services Federation Language (WS- Federation), Version 1.2 Committee Draft 01 June 23, 2008	Defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. This includes mechanisms for brokering of identity, attribute, authentication and authorization assertions between realms, and privacy of federated claims. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare, Committee Draft, 13 October 2008	The XSPA SAML profile provides the necessary content for exchange interoperable access control information facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners
Organization for the Advancement of Structured Information Standards (OASIS) Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of WS-Trust for Healthcare, Committee Draft, 14 October 2008	The XSPA WS-Trust profile provides the necessary content for exchange interoperable access control information facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners
Organization for the Advancement of Structured Information Standards (OASIS) Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of eXtensible Access Control Markup Language (XACML) for Healthcare, Committee Draft, 14 October 2008	The XSPA XACML profile provides the necessary content for evaluating principal access control information against established security policy and making access control decisions enforcing established security policy



5.2 STANDARDS GAPS AND OVERLAPS

Table 5-5 identifies the information exchange requirements and known standards gaps, along with the recommended resolutions to the gaps.

Table 5-5 Information Exchange Requirements (IER) and Associated Standards Gaps

IER Gap Description	Responsible HITSP TC	Design Approach	Required Standards Now Unavailable for Constructs	SDO Working on Unavailable Standards	Expected Availability
<p>B – Send and Receive Clinical Referral Request</p> <p>Identify/Select a consulting clinician or next setting of care, based on capability and health plan association</p> <p>Identify provider based on patient preference</p>	ADFTC and Consumer Preference and Provider PTC	New construct and possibly new capability needed	There is currently no standard available for a provider registry from which to select a provider based on patient preferences or on Health Plan Eligibility. Candidate standards in HL7 and ASC X12 are awaiting harmonization.	HL7 and X12	Wave III

Table 5-6 lists any standards overlaps and describes plans to resolve each of the overlaps.

Table 5-6 Information Exchange Requirements (IER) and Associated Standards Overlaps

IER Number	Summary Description	Standard Overlap	Recommended Resolution
None			



6.0 APPENDIX

This section may include additional materials referenced throughout this document, such as requirements analysis tables and figures. If the Capability is yet to be implemented, it may contain the candidate standards for Tier 2 evaluations.

Legacy Interoperability Specifications were used to derive this Capability:

- HITSP/IS04 Emergency Responder Electronic Health Record
- HITSP/IS09 Consultations and Transfers of Care
- HITSP/IS92 Newborn Screening



7.0 DOCUMENT UPDATES

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

7.1 NOVEMBER 9, 2009

No changes. This is the first published version of the document.

7.2 JANUARY 18, 2010

This document was updated to HITSP Capability Template Version 2.3

7.2.1 UPDATES FROM PUBLIC COMMENT

The changes in this cycle address the following comments received during the November 2009 public comment period:

- Incorporated all of the 6 Public Comment TC dispositions into the document
- Added trigger and assumption to Table 4-3.
- Added Interfaces from HITSP/T67 to tables in Section 4.0
- Updated Information Exchange Identifiers
- Reformatted the document content to adhere to the new HITSP document template
- Added diagrams and tables based on the new HITSP document templates

The associated comment numbers for these updates are as follows:

- 8212, 8213, 8214, 8215, 8216, 8972

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

7.3 JANUARY 25, 2010

Upon approval by the HITSP Panel on January 25, 2010, this document is now Released for Implementation.

