January 25, 2010
Version 1.0

HITSP Communicate Unstructured Document Capability

HITSP/CAP120

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 7
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
Document Content Options 11
4.0 DESIGN SPECIFICATION 12
4.1 Requirements Mapped to Constructs 12
4.1.1 Constructs 12
4.2 Constraints and Assumptions 12
4.3 Specified Interfaces by System Role 13
5.0 STANDARDS 15
5.1 Standards Used 15
5.1.1 Regulatory Guidance 15
5.1.2 Selected Standards 15
5.1.3 Informative Reference Standards 19
5.2 Standards Gaps and Overlaps 19
6.0 APPENDIX 21
7.0 DOCUMENT UPDATES 22
7.1 November 9, 2009 22
7.2 January 18, 2010 22
7.3 January 25, 2010 22

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 Document Sender System Role Mapped to HITSP Construct Interfaces 13
Table 4-5 Specified Interfaces for Document Consumer System Role 13
Table 4-6 Specified Interfaces for Registry and Repository System Role 14
Table 4-7 Implementation Conditions 14
Table 5-1 Reader's Guide for Section 5.0 15
Table 5-2 Regulatory Guidance 15
Table 5-3 Selected Standards 15
Table 5-4 Informative Reference Standards 19
Table 5-5 Information Exchange Requirements (IER) and Associated Standards Gaps 20
Table 5-6 Information Exchange Requirements (IER) and Associated Standards Overlaps 20

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	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 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
	5.2 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 the communication of a set of unstructured health data related to a patient in the context of a document, the source of which can be attested. Two types of specific unstructured content are supported, both with a structured CDA header:

1. PDF-A supporting long-term archival
2. UTF-8 text

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.

The scope of this Capability is to support the exchange of notes and other documents which do not contain structured information, e.g. referral letter, patient consent. These documents may assist clinicians in providing additional information about a patient encounter or care plan that is pertinent to the understanding of the patient's condition or preferences.

Documents that are not typically authored by a clinician or generated for clinical purposes (e.g., patient forms, consents, administrative documents) and do not constitute clinical documentation of a patient encounter or service may be exchanged with this Capability. This Capability may also be used to exchange a signed and scanned copy of a clinician's note, until such time as a structured document is available to be exchanged. In addition, items that may accompany or support clinical notes, such as images and waveforms, are permitted uses for this Capability.

1.3 COPYRIGHT PERMISSIONS

1.4 REFERENCE DOCUMENTS

A list of key reference documents and background material is provided in the table below. HITSP-maintained reference documents can be retrieved from the HITSP Web Site.

Table 1-2 Reference Documents

Reference Document	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

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 4-7 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	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, exchange content, constraints mapped to the initiating and responding system roles that participate in these exchanges

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
Document Sender	The system which sends the document
Document Consumer	The system which receives the document and which initiates a query for documents in an HIE
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 forwards the document upon request

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.

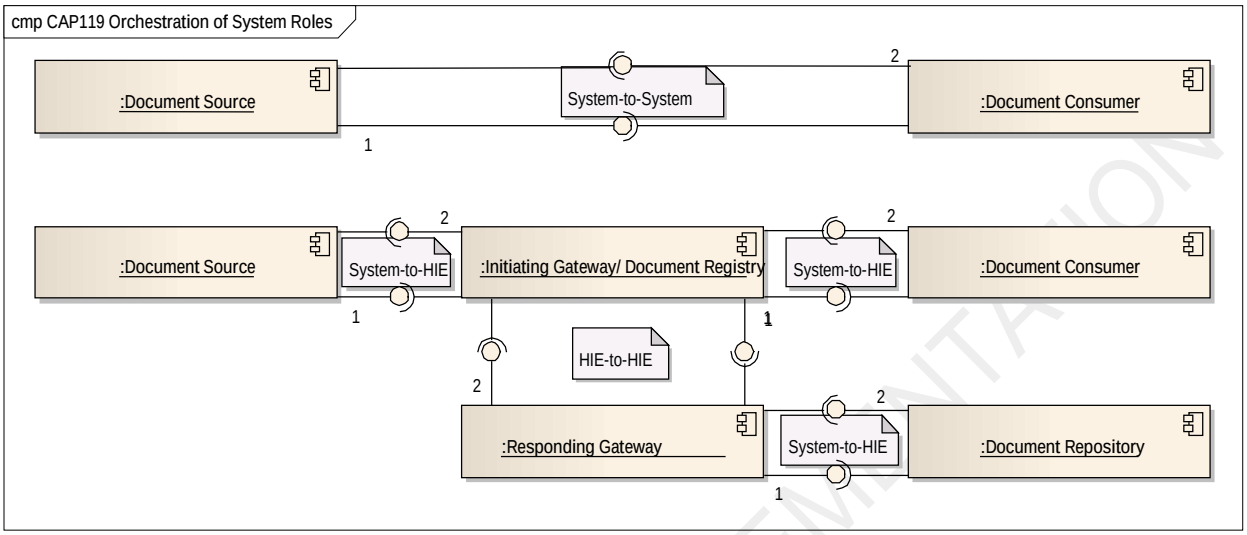
Table 2-3 Supported Information Exchanges

Information Exchange Identifier	Exchange Action	Exchange Content
A	Send and Receive	Unstructured Document
A	Send and Receive	Clinical Document Metadata

Figure 2-1 identifies how this Capability supports various system roles within multiple system architectures. For example, either an Electronic Health Record (EHR) system or a Health Information Exchange (HIE) might fill a document repository system role in an information exchange). In an implementation architecture, system roles may be combined locally (e.g., Hospital EHR System) and in

others, the system roles may be provided by multiple-distributed trusted third parties (e.g., pharmacies within an HIE).

Figure 2-1 Information Exchanges Between System Roles



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	Number	Intended Audience	information Contained
Section 3.0 External Capability Options	3.1 Security and Privacy	Policy Analysts Architects Business Analysts Developers	Defines 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

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

- Topology Related Options
- Content Import 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 Exchange[1] (HIE) is a special network system that provides intermediary services, such as directories, registries or translations. HITSP supports the following topologies.

- Portable Media (non-connected)

[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 groupings 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 health records, the effort must first develop at the local and state levels. The concept of NHIN requires extensive collaboration by a diverse set of stakeholders. The challenges are many to achieve success for an HIE or a RHIO.

- 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 Harmonization Framework and Exchange Architecture 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	Availability
Point-to-Point	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	Not Applicable

One content import option is offered:

- Document Import Option impacts the import of Documents processed by an application Content Consumer function of a Document Consumer system. It requires the Document Consumer to have the ability to import into the health record one or more of the received documents as a whole and display it as requested

DOCUMENT CONTENT OPTIONS

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	HITSP/C62 - Unstructured Document

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

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 assumptions, pre-conditions, triggers and 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 each of the Information Exchanges supported by this Capability in terms of the Exchange Action (EA) or Exchange Content (EC) used 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 Data Architecture 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/Receive Unstructured Document	Content	HITSP/C62 – Unstructured Document	The HITSP Unstructured Document Component is provided for the capture and storage of patient identifiable, unstructured document content, such as text, PDF, and images rendered in PDF. It is based on the Cross-Enterprise Sharing of Scanned Documents (XDS-SD) profile from the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF)
A – Send/Receive Unstructured Document	Action	HITSP/SC112 – Healthcare Document Management	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)

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
Systems store patient data as an encounter. A patient has one too many encounters linked into episodes of care. Each encounter holds documents. Each document holds data. This is analogous to each encounter being a report holding many paper document sections and each document section containing many data pieces. An episode of care contains many reports on the same incident. The file folder also contains incident information on the same topic (e.g., patient). We assume data are communicated in both document and message forms	Assumption
Ability to identify and request corrections to errors is available	Pre-condition
Method to query other organizations for data and matching to the consumer is available	Pre-condition
If physical media is used for the transport, when the media is read the consent directives stored on the portable media need to be enforced by the portable media importer. The validity of these content directives may need to be checked	Post-condition

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 specifies interfaces for document sender system roles as defined in Table 2-2.

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

Construct Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Send Documents Directly	Initiating	HITSP/SC112 - Healthcare Document Management	C[101]
Send Document through email	Initiating	HITSP/SC112 - Healthcare Document Management	C[101]
Publish Document Through Media	Initiating	HITSP/SC112 - Healthcare Document Management	C[101
Send Document Through Share	Initiating	HITSP/SC112 - Healthcare Document Management	C[101]
Publish Document Through Share	Initiating	HITSP/SC112 - Healthcare Document Management	C[101]
N/A	Initiating	HITSP/C62 - Unstructured Document	R

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

Table 4-5 specifies interfaces for document consumer system roles as defined in Table 2-2.

Table 4-5 Specified Interfaces for Document Consumer System Role

Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Receive Documents	Responding	HITSP/C62 – Unstructured Document + HITSP/SC112 - Healthcare Document Management	C120[102]
Receive Documents Directly	Responding	HITSP/SC112 - Healthcare Document Management	C[102]
Receive Document through email	Responding	HITSP/SC112 - Healthcare Document Management	C[102]
Publish Document Through Media	Responding	HITSP/SC112 - Healthcare Document Management	C[102]
Receive Document Through Share	Responding	HITSP/SC112 - Healthcare Document Management	C[102]
Publish Document Through Share	Responding	HITSP/SC112 - Healthcare Document Management	C[102]
N/A	Responding	HITSP/C62 - Unstructured Document	R

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

Table 4-6 specifies interfaces for registry and repository system roles as defined in Table 2-2.

Table 4-6 Specified Interfaces for Registry and Repository System Role[2]

Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Send Document Through Share	Initiating	HITSP/SC112 - Healthcare Document Management	C[103]
N/A	Initiating	HITSP/C62 - Unstructured Document	R
Receive Document Through Share	Responding	HITSP/SC112 - Healthcare Document Management	C[103]
Publish Document Through Share	Responding	HITSP/SC112 - Healthcare Document Management	C[103]
N/A	Responding	HITSP/C62 - Unstructured Document	R

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

Table 4-7 specifies optionality conditions referenced in Table 4-4 through Table 4-6 above.

Table 4-7 Implementation Conditions

Condition Code	Condition Description
[101]	The implementation shall support the appropriate specializations of the Send Document interface for each topology supported
[102]	The implementation shall support the appropriate specializations of the Receive Document interface for each topology supported
C [103]	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 – Healthcare Document Management

[2] Any system may optionally choose to implement a document registry and/or document repository or use an external registry and/or repository for the Send Documents through Share options of HITSP/SC112 Healthcare Document Management.

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	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
	5.2 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
No applicable regulatory guidance	

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 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
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
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 E2595 and for user-based access controls enforcing patient consent directives

Standard	Description
ASTM International Standard Guide for Privilege Management Infrastructure (PMI) Guidelines: #E2595-07 (2003)	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
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
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) 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
Health Level Seven (HL7) Version 3.0 Clinical Document Architecture (CDA) Release 2.0	The HL7 Clinical Document Architecture is an XML-based document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA is one instantiation of HL7's Version 3.0 Reference Information Model (RIM) into a specific message format. Of particular focus for HITSP Interoperability Specifications are message formats for Laboratory Results and Continuity of Care (CCD) documents. Release 2 of the HL7 Clinical Document Architecture (CDA) is an extension to the original CDA document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA R2 includes a prose document in HTML, XML schemas, data dictionary, and sample CDA documents. CDA R2 further builds upon other HL7 standards beyond just the Version 3.0 Reference Information Model (RIM) and incorporates Version 3.0 Data Structures, Vocabulary, and the XML Implementation Technology Specifications for Data Types and Structures. For more information visit www.hl7.org

Standard	Description
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) Revision 4.0 or later, Patient Identifier Cross-Referencing (PIX) Integration Profile	The Patient Identifier Cross-referencing (PIX) Integration Profile is targeted at healthcare enterprises of a broad range of sizes (hospital, a clinic, a physician office, etc.). It supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains via the following interactions: 1) The transmission of patient identity information from an identity source to the Patient Identifier Cross-reference Manager. 2) The ability to access the list(s) of cross-referenced patient identifiers either via a query/ response or via update notification By specifying the above transactions among specific actors, this integration profile does not define any specific enterprise policies or cross-referencing algorithms. By encapsulating these behaviors in a single actor, this integration profile provides the necessary interoperability while maintaining the flexibility to be used with any cross-referencing policy and algorithm as deemed adequate by the enterprise. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 6.0 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) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a) Integration Profile	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. Section 10, Cross-Enterprise Document Sharing facilitates the registration, distribution and access across health enterprises of patient electronic health records. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. For more information visit 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) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile	The Audit Trail and Node Authentication (ATNA) Integration Profile establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. 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) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) Integration Profile – Trial Implementation	The Basic Patient Privacy Consents (BPPC) Integration Profile provides a mechanism to record the patient privacy consent(s), a method to mark documents published to XDS with the patient privacy consent that was used to authorize the publication, and a method for XDS Consumers to use to enforce the privacy consent appropriate to the use. This profile complements XDS by describing a mechanism whereby an XDS Affinity Domain can develop and implement multiple privacy policies, and describes how that mechanism can be integrated with the access control mechanisms supported by the XDS Actors (e.g. systems). There are two key parts of the profile: 1) It provides a document content specification for capturing a patient acknowledgement of a privacy consent policy or policies. 2) It describes the method by which XD* Actors can enforce the privacy policies determined by the document confidentialityCode related to the patient privacy consents. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 2.0 XDM Supplement	This Supplement to the IHE IT Infrastructure Technical Framework defines the means to store and interchange personal medical documents on portable media. The current version of the XDM is specified in the XDM Trial Implementation Supplement to the ITI-TF, rev. 2.0, which is consistent with IHE XDS.b Supplement in term of document entry metadata. For more information visit www.ihe.net
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 - ITI-25 Notification of Document Availability (NAV) Jun 28, 2005	The Capability for automation of critical workflows used in healthcare has been greatly advanced by the introduction of the Cross-Enterprise Document Sharing Integration Profile. However, without point-to-point notification of document availability, these workflows still require manual interactions between parties using document sharing. The Notification of Document Availability Integration Profile (NAV) introduces a mechanism allowing notifications to be sent point-to-point to systems and users within an affinity domain, eliminating the need for manual steps or polling mechanisms. This basic mechanism is only intended to facilitate the common part of a large range of workflows related to notifying a remote party (user or system) that one or more documents have been registered in an XDS Registry and may be retrieved if the notified party wishes. For further 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) Integration Profile	The Cross-Enterprise Document Sharing-B (XDS.b) Integration Profile 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. 4.0, which is consistent with IHE XDS.b Supplement in term of document entry metadata. For more information visit www.ihe.net 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 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
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

Standard	Description
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
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) 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 XCML 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
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) 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

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
CDA Quick Start Guide (v1.5)	The CDA Quick Start Guide was created by Alschuler Associates, LLC. The guide helps implementers create a simple CDA document and then as they increase their knowledge of CDA, go on to create more complex versions using the resources cited in this *QSG* and their own experience. For more information visit www.alschulerassociates.com/library/documents/cda_qsg_v1.5.zip

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
None					

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.

7.0 DOCUMENT UPDATES

This section provides the history of changes 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

Conversion of document to the latest Capability Template Version 2.3.

7.3 JANUARY 25, 2010

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