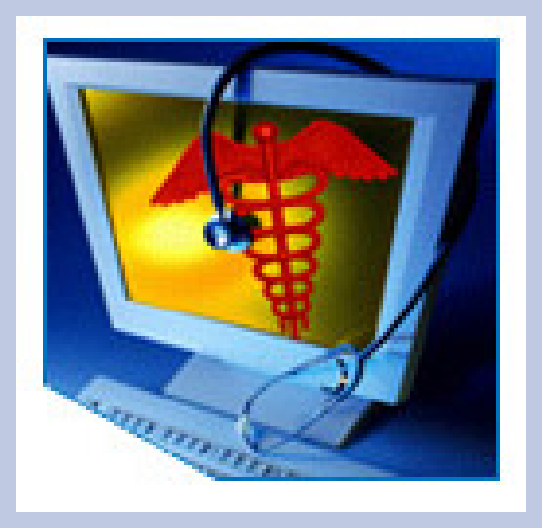
December 13, 2007
Version 2.2

HITSP Manage Sharing of Documents Transaction Package

HITSP/TP13



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Population Health Technical Committee
Consumer Empowerment Technical Committee
Care Delivery Technical Committee
Security and Privacy Technical Committee

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Final Draft	Electronic Health Record Technical Committee	August 18, 2006
1.1	Ready for Public Comment	Biosurveillance Technical Committee Consumer Empowerment Technical Committee Electronic Health Record Technical Committee	September 12, 2006
1.2	Ready for Implementation Testing	Biosurveillance Technical Committee Consumer Empowerment Technical Committee Electronic Health Record Technical Committee	October 20, 2006
1.3	Review Copy	Population Health Technical Committee Consumer Empowerment Technical Committee Care Delivery Technical Committee	April 27, 2007
2.0	Released for Implementation	Population Health Technical Committee Consumer Empowerment Technical Committee Care Delivery Technical Committee	May 11, 2007
2.0.1	Review Copy	Security and Privacy Technical Committee	July 20, 2007
2.0.2	Review Copy	Population Health Technical Committee Consumer Empowerment Technical Committee Care Delivery Technical Committee Security and Privacy Technical Committee	October 5, 2007
2.1	Released for Implementation	Population Health Technical Committee Consumer Empowerment Technical Committee Care Delivery Technical Committee Security and Privacy Technical Committee	October 15, 2007
2.1.1	Review Copy	Population Health Technical Committee Consumer Empowerment Technical Committee Care Delivery Technical Committee Security and Privacy Technical Committee	November 6, 2007
2.1.2	Review Copy	Population Health Technical Committee Consumer Empowerment Technical Committee Care Delivery Technical Committee Security and Privacy Technical Committee	December 5, 2007
2.2	Released for Implementation	Population Health Technical Committee Consumer Empowerment Technical Committee Care Delivery Technical Committee Security and Privacy Technical Committee	December 13, 2007

TABLE OF CONTENTS

1.0 FOREWORD 6

2.0 INTRODUCTION 9

2.1 Overview 9

2.2 Technical Assumptions and Scope 11

2.2.1 Interoperability Specifications Not Functional Specifications 11

2.2.2 Architectural Neutrality 11

2.2.3 The Use of Messages and Documents as Appropriate 11

2.2.4 Security and Privacy 12

2.3 Copyright Permissions 13

2.4 Acronyms 13

2.5 Conventions 13

2.6 Reference Documents 13

3.0 REFERENCED STANDARDS 14

3.1 List of Standards 14

3.2 List of Transactions 15

3.2.1 List of Transactions for XDS.a Option 16

3.2.2 List of Transactions for XDS.b Option 17

3.2.3 List of Transactions for XCA Option 19

3.3 Dependencies 19

3.4 Constraints 19

4.0 TRANSACTION PACKAGE 20

4.1 Context Overview 20

4.1.1 Overview of IHE XDS Integration Profile 20

4.1.2 Overview of the IHE XCA Integration profile 21

4.1.3 Contextual Constraints 25

4.1.4 Technical Actors 26

4.1.5 Actor Interactions 27

4.2 Process Flows 28

4.2.1 Process Pre-conditions within a Community 28

4.2.2 Process Post-conditions within a Community 29

4.2.3 Process Pre-conditions across Communities 29

4.2.4 Process Post-conditions across Communities 30

4.3 Data Flows 30

5.0 TECHNICAL IMPLEMENTATION 31
5.1 Conformance 31
5.1.1 Conformance Criteria 31
5.1.2 Conformance Scoping, Subsetting and Options 31
5.2 Supporting Documents 33
6.0 APPENDIX 34
6.1 Gaps 34
6.1.1 Terminology 34
6.1.2 Cross-Affinity Domain Document Sharing 34
7.0 CHANGE HISTORY 37
7.1 May 11, 2007 37
7.2 July 20, 2007 37
7.3 September 25, 2007 37
7.4 October 5, 2007 37
7.5 October 15, 2007 37
7.6 November 6, 2007 37
7.6.1 Version Compatibility: 37
7.7 December 5, 2007 38
7.8 December 13, 2007 38

FIGURES AND TABLES

Figure 1.0-1 HITSP Harmonization Process Steps 8
Figure 2.1-1 Intra and Cross-Community Document Sharing 9
Figure 3.2.1-1 Cross-Enterprise Document Sharing – XDS.a Diagram 17
Figure 3.2.2-1 Cross-Enterprise Document Sharing – XDS.b Diagram 18
Figure 18.1-1 – XCA Actor Diagram 22
Figure 4.1.5.1-1 Optional Document Integrity Sequence Diagram 27
Figure 6.1.2-1 XDS Affinity Domain 35

Table 2.1-1 Related Documents 10
Table 3.1-1 List of Standards 15
Table 3.2.1-1 List of Transactions for XDS.a 16
Table 3.2.2-1 List of Transactions for XDS.b 17
Table 3.2.3-1 List of Transactions for XCA 19
Table 3.3-1 Dependencies 19
Table 4.1.3.1-1 Data Mapping 25
Table 5.1.2.1-1 XDS.a – Options by Actors 31
Table 5.1.2.2-1 XDS.b – Options by Actors 32
Table 5.1.2.3-1 XCA – Options by Actors 32

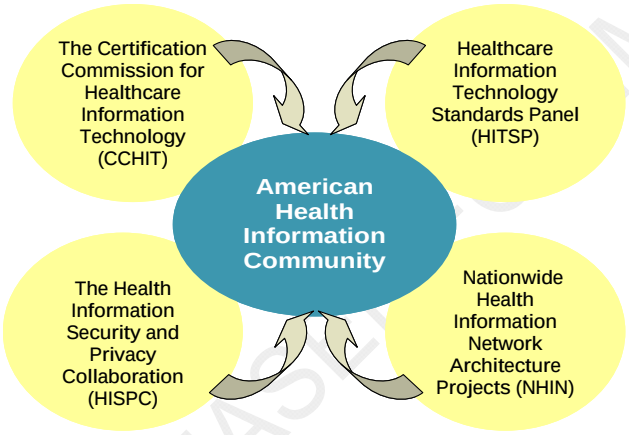
1.0 FOREWORD

This document is referred to as a Transaction Package and is an artifact of the Healthcare Information Technology Standards Panel (HITSP).

The following paragraphs provide background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. It also describes the HITSP process for healthcare standards harmonization and explains how to use this document and other related documents to inform your health IT product development or product refinement. If you are familiar with HITSP and HITSP artifacts, please proceed to Section 2.0.

U.S. Nationwide Health Information Interoperability

Studies published by the Institute of Medicine and others have raised awareness of the extent to which the fragmented nature of clinical information adversely impacts the quality of care across the U.S. Health Information Technology (IT) can be used to enable better integration of clinical information. However, as of 2007, only a small number of U.S. healthcare providers have fully adopted health IT due, in part, to technical barriers associated with a lack of unambiguous and nationally recognized interoperability standards.



The American Health Information Community[1] (AHIC), a 2005 federally-chartered commission made up of leaders from public and private health sectors, was formed to provide recommendations on how to make health records digital and interoperable, and assure that the privacy and security of those records are protected, in a smooth, market-led way. At the same time, The Department of Health and Human Services, through the Office of the National Coordinator for Health IT (ONC) awarded contracts to 1) identify interoperability standards to facilitate the exchange of patient data (HITSP), 2) define a process for certifying that health IT products comply with appropriate standards through the Certification Commission for Healthcare Information Technology (CCHIT), and 3) develop a series of prototypes to establish the requirements of a Nationwide Health Information Network (NHIN). Under a renewed second year contract, HITSP scheduled activities included identifying and constraining the standards needed for a standards-based security framework that provides the mechanisms needed to protect patient privacy and maintain confidentiality of information about the patient, as well as further work in additional Use Case priority areas recommended by AHIC. This year, CCHIT is expanding its certification efforts to inpatient, or hospital, electronic health record products. In January 2007, four NHIN prototypes were delivered

[1] http://www.hhs.gov/healthit/ahic.html

based on the requirements for health information exchange. The next phase will be to connect the prototypes and state and regional health information exchange efforts in trial implementations. These activities share the goal of widespread adoption of interoperable electronic health records (EHR) within 10 years through public-private collaboration.

HITSP's Role within Nationwide Interoperability Efforts

The HITSP[2] is a multi-stakeholder coordinating body designed to provide the process within which affected parties can identify, select, and harmonize standards for communicating healthcare information throughout the healthcare spectrum. As used by HITSP, the term "standard" refers, but is not limited to Specifications, Implementation Guides, Code Sets, Terminologies, and Integration Profiles. A standard should be produced through a well-defined approach that supports a business process and

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

HITSP functions as a partnership of the public and private sectors and operates with a neutral and inclusive governance model administered by the American National Standards Institute. The goal of the Panel is to:

- Facilitate the development of harmonized Interoperability Specifications and information policies, including Standards Development Organization (SDO) work products (e.g. standards, technical reports). These policies, profiles and work products are essential for establishing privacy, security and interoperability among healthcare software applications
- Coordinate, as appropriate, with other national, regional and international groups addressing healthcare information to ensure that the resulting standards are globally relevant
- Be Use Case driven, using information from stakeholders and basing decisions on industry needs

The work of the HITSP is conducted through formally chartered Technical Committees and Work Groups. The artifact of the Technical Committee and Work Group activities is an Interoperability Specification (IS) and related constructs referred to as Transaction Packages, Transactions, or Components. For additional information on these constructs, please refer to the HITSP Harmonization Framework.

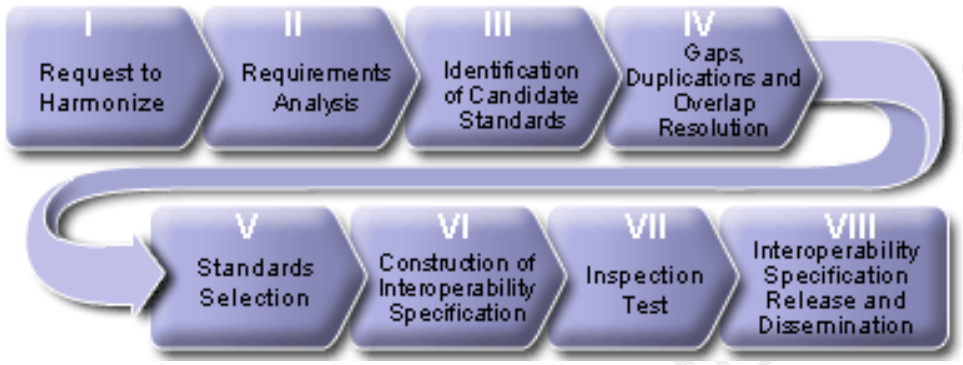
How Use Cases and HITSP Interoperability Specifications are Developed

The American Health Information Community, as the representative of public and private health sector stakeholders, identified the three Use Cases (available at www.hitsp.org) that drove the initial efforts of the HITSP. Nationwide public and private health sector priorities continue to focus the efforts of the

[2] www.hitsp.org

HITSP. The Use Case driven HITSP harmonization process is implemented by formally chartered Technical Committees. The volunteers that comprise a Technical Committee followed an 8 step process, depicted below.

Figure 1.0-1 HITSP Harmonization Process Steps



How to Read this Interoperability Specification

Each HITSP specification describes a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications that will satisfy the requirements for the HITSP construct. There are four types of HITSP constructs called Interoperability Specifications (IS), Transaction Packages (TP), Transactions (T), and Components (C). Interoperability Specifications define the context(s) in which any other HITSP construct may be used. The current Manage Sharing of Documents Transaction Package specification is used with other constructs to meet the requirements of one or more ISs. Review Section 1.2 (Interoperability Specification Construct Roadmap) from the relevant IS to better understand the context, dependencies, and relationships between the constructs used to meet the IS requirements. The roadmap in Figure 1.2-1 depicts how this construct integrates and constrains HITSP constructs and existing standards selected or referenced to support the information exchange between two or more systems, within the defined context of this document. Implementers should read the documents that describe the constructs depicted in the diagram for their details and specific uses.

2.0 INTRODUCTION

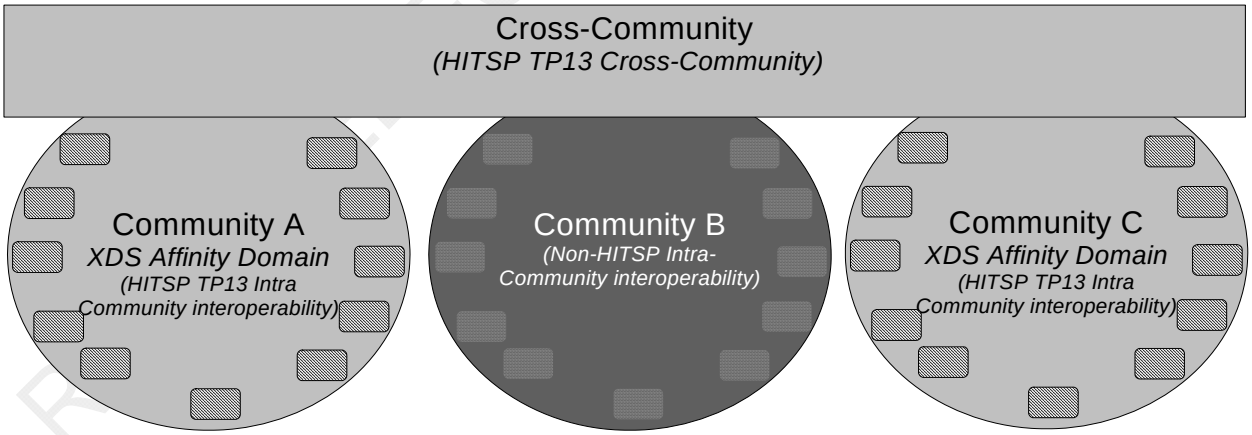
As an introduction to the Manage Sharing of Documents Transaction Package, this section provides a high level overview of the information sharing scenario enabled by following this specification, outlines the technical scope of the specification, describes the intended audience for the technical content of the document, acknowledges the copyright protections that pertain, provides Internet links to the HITSP Acronyms List and an explanation of the conventions used to convey the full descriptions and usage of standards. If you are already familiar with this information, proceed to Section 3.0 Referenced Standards.

2.1 OVERVIEW

This HITSP Transaction Package supports the sharing of patient records in the form of source attested objects called documents. A healthcare document is a composite of structured and coded health information, both narrative and tabular, that describes acts, observations and services for the purpose of exchange. No assumption is made by this construct in terms of the format and structure of the content of documents shared. Interoperability related to document content is addressed by HITSP in other constructs.

Documents may be shared within a community where a significant part of the document sharing for a consumer or patient may occur, as well as across communities. This construct addresses both the Intra-Community and the Cross-Community sharing of documents. In Cross-Community interoperability, communities interconnecting their edge systems or enterprises in other ways than defined by this construct are also supported, as shown in Figure 2.1-1.

Figure 2.1-1 Intra and Cross-Community Document Sharing



To support “Manage Sharing of Documents”, HITSP has selected the Cross-Enterprise Document Sharing (XDS) and the Cross-Community Access (XCA) Integrating the Healthcare Enterprise (IHE) Integration Profiles, which facilitate the registration, distribution and access of patient electronic health records across healthcare enterprises and across communities of such enterprises. Cross-Enterprise Document Sharing is focused on providing a standards-based specification for managing the sharing of

documents between healthcare enterprises, ranging from a private physician office to a clinic to an acute care inpatient facility and other healthcare IT systems. Cross-Community Access is focused on creating a "network of networks" or communities by providing the means for a community to access consumer's health records managed by other communities. Additional source material from the IHE IT Infrastructure (ITI) Technical Framework (TF) Cross-Enterprise Document Sharing (XDS) Integration Profile and the Cross-Community Access Integration Profile is quoted in this document to further clarify the actions and interactions.

This construct supports the choice of one or more of the following options:

- XDS.a Option: Management of Document Sharing within a Community according to IHE XDS.a
  - (See Change History §7.6 – Note 1)
- XDS.b Option: Management of Document Sharing within a Community according to IHE XDS.b
  - This is an evolution of XDS which is functionally equivalent to XDS.a but which supports the most recent web services standards, thus enabling the support of Entity Identity Assertion on all transactions, simplifies implementation and is consistent with Cross-Community Access (XCA) (See Change History §7.6 – Note 2)
- XCA Option: Management of Cross-Community Access according to IHE XCA
  - This addresses the requirement for federating two or more communities using IHE XDS.b internally or other non-HITSP legacy means of communication (See Change History §7.6 – Note 2)

Note: Support of both XDS.a and XDS.b as options within this version preserves full compatibility with previous versions of HITSP/TP13, while allowing new implementations to take advantage of XDS.b. As XDS.a and XDS.b are functionally identical, transition from one to the other is facilitated. It is the intention of HITSP to select the XDS.b option for Intra-Community interoperability in new Interoperability Specifications and in current IS documents as they are revised; support of XDS.a will be phased out over time. Migration strategies are discussed in the IHE IT Infrastructure Technical Framework XDS.b Supplement (Section 10.7).

Related to this Transaction Package are the HITSP constructs described in Table 2.1-1.

Table 2.1-1 Related Documents

Related Documents	Document Description
HITSP/T29	HITSP Notification of Document Availability Transaction
HITSP/TP22	HITSP Patient ID Cross-Referencing Transaction Package
HITSP/T23	HITSP Patient Demographics Query Transaction
HITSP/T15	HITSP Collect and Communicate Security Audit Trail Transaction
HITSP/T16	HITSP Consistent Time Transaction
HITSP/T17	HITSP Secured Communication Channel Transaction
HITSP/TP20	HITSP Access Control Transaction Package

Related Documents	Document Description
HITSP/TP30	HITSP Manage Consent Directives Transaction Package
HITSP/C19	HITSP Entity Identity Assertion Component

2.2 TECHNICAL ASSUMPTIONS AND SCOPE

This Interoperability Specification focuses on a set of constrained standards for information interchange that address the core requirements of the Use Case described above. It may not define all functions, constructs and standards necessary to implement a conforming system in a real world environment. The following paragraphs provide the HITSP principles with regard to several critical topics to ensure consistent interpretation of the Interoperability Specifications.

2.2.1 INTEROPERABILITY SPECIFICATIONS NOT FUNCTIONAL SPECIFICATIONS

The HITSP Interoperability Specification defines how two or more systems exchange standard data content in a standardized manner. Interoperability Specifications define the necessary business and technical actors, the transactions between them including the message, content and terminology standards for the actual information exchange. Interoperability Specifications do not specify the functional requirements or behaviors of the systems or applications.

2.2.2 ARCHITECTURAL NEUTRALITY

HITSP Interoperability Specifications, unless otherwise noted, are not intended to define or prescribe any system architecture or implementation. At the most basic level, the Interoperability Specifications define specific information exchange standards that are to be used by any two systems. Information exchange must be placed within the context of a transaction between defined technical actors which fulfill higher level business requirements derived from the Use Case. In some cases the necessary technical actors may require some architectural structure or make some assumptions involving synchronous or asynchronous data exchanges, or require specific type of exchange, such as a message or document. These requirements may constrain to some degree the total range of choices regarding system architectures. When constraints are necessary to meet the Use Case requirements, the Interoperability Specification will note this and will retain as much architectural neutrality as possible. When appropriate, the Interoperability Specifications may provide architectural examples and discuss considerations of such examples.

2.2.3 THE USE OF MESSAGES AND DOCUMENTS AS APPROPRIATE

Within healthcare information there is an ongoing debate concerning the proper role of messages and documents as methods of exchanging data. Messages are typically non-persistent encapsulations of highly structured data that require external context. Documents are persistent encapsulations of both data and context which may be authenticated to insure Nonrepudiation. Persistence as defined by Health Level Seven (HL7) means that a clinical document continues to exist in an unaltered state for a time

period defined by local and regulatory requirements. Nonrepudiation, as defined by ISO adapted from ASTM E31, means a service that provides proof of the integrity and origin of data, which can be verified by any party. HITSP recognizes that requirements for both messages and documents exist and where consistent with harmonization will support both. For example, depending on specific phases of the workflow, a laboratory result might be exchanged as a message, as a document, or both. Business requirements may define which format is more effective.

2.2.4 SECURITY AND PRIVACY

The Health Insurance Portability and Accountability Act (HIPAA) and its Administrative Simplification sections establish the minimum federal requirements for security and privacy of individually identifiable health information (IIHI). HIPAA requires that “covered entities” establish and maintain secure systems that protect IIHI from unauthorized disclosures while ensuring its availability for authorized uses. Most providers, health plans and intermediaries, and by contract their business associates, are covered by HIPAA regulation. However, HIPAA does not cover personal health records unless they are held by a covered entity or business associate, nor an individual’s use of their own health information.

Currently, HITSP is charged by ONC to harmonize standards based on Use Cases derived from AHIC requirements and priorities. The Use Cases generally require a secure infrastructure and certain security or privacy functions; refer to the IS that uses this construct for specific Security and Privacy requirements.

The use of this Transaction Package does not, by itself, provide any level of security for the transmission of documents; however it does allow the optional activity as described in Section 4.1.3.1 Document Integrity (Optional) to validate Document Integrity. Please refer to that section for further information.

All Documents that are registered shall include an XDS Affinity Domain defined confidentiality code(s) as discussed in IHE XDS. This confidentiality code(s) has a relationship to the security constructs for HITSP/TP30 - Manage Consent Directives and HITSP/TP20 - Access Control. This relationship is described in HITSP/TN900 - Security and Privacy, and may be further scoped by the Interoperability Specification.

All documents managed by this construct shall be used only in compliance with the XDS Affinity Domain policies and according to the confidentiality Code(s) indicated in the XDS metadata for that document. This compliance is assured using the HITSP/TP20 - Access Control security construct in relationship to HITSP/TP30 - Manage Consent Directives.

The sharing of documents across communities managed by this construct shall be used only in compliance with the Cross-Community policies established among the sharing communities (XDS Affinity Domains or other). Negotiation and matching of Security and Privacy polices among communicating communities requires the use of appropriate Security and Privacy constructs as specified by HITSP in the Interoperability Specifications that reference this construct.

All the Transactions described in this construct shall result in both Actors recording a security audit event as described in HITSP/T15 - Collect and Communicate Security Audit Trail, with clarifications found in IHE XDS.a, XDS.b and XCA.

2.3 COPYRIGHT PERMISSIONS

2.4 ACRONYMS

The acronyms used in this document are contained in the HITSP Acronyms List.

2.5 CONVENTIONS

Conventions are used to convey the full descriptions and usage of standards in the Interoperability Specification and are contained in the HITSP Conventions List.

2.6 REFERENCE DOCUMENTS

This section contains links to key reference documents and background material.

The HITSP Glossary provides definitions for relevant terms used by HITSP documents.

3.0 REFERENCED STANDARDS

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

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

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

3.1 LIST OF STANDARDS

It is important to understand that the standards selected here are within the context of the specific Use Case requirements and do not necessarily reflect selection in other contexts. The following standards are used to implement this Interoperability Specification:

Table 3.1-1 List of Standards

Composite Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles, offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. 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 - Registry Stored Query Transaction for XDS Profile 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 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 Intergation profile. This supplement is available at www.ihe.net.
International Organization for Standardization (ISO) Electronic business eXtensible Markup Language (ebXML), Technical Specification # 15000 -- Part 4: Registry services specification (ebRS), May, 2004	Describes eXtensible Markup Language (XML) and its usage characteristics. Consists of 4 parts: ebCPP, ebMS, ebRIM, and ebRS. Part 4 ebRS defines the interface between the registry and the registry clients, as well as the interaction protocols, message definitions and XML schema. Visit www.iso.org for more information.

Note: The specific references to the underlying web services standards (e.g. SOAP, WSDL, MTOM, etc.) upon which the above listed profiles and standards rely may be found in those documents.

3.2 LIST OF TRANSACTIONS

The following section specifies the list of transactions and their definitions used by this Transaction Package specification for the XDS.a, XDS.b and XCA option respectively.

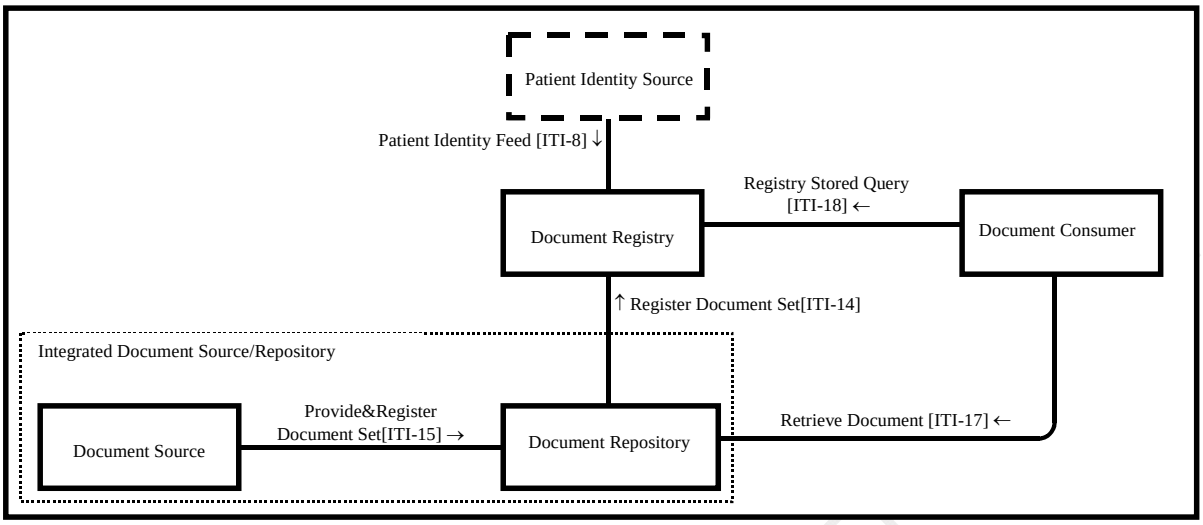
3.2.1 LIST OF TRANSACTIONS FOR XDS.a OPTION

Table 3.2.1-1 List of Transactions for XDS.a

Actor Name	Transaction Name	Description	Document Name	Required = R Optional = O Conditional = C
Document Source	ITI-15: Provide & Register Document Set	Provide and Register Document Set is used to provide a set of documents to a repository, and to request that the repository store these documents and then register them with a registry	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), Volume 2	R
Document Repository	ITI-15: Provide & Register Document Set	Provide and Register Document Set is used to provide a set of documents to a repository, and to request that the repository store these documents and then register them with a registry	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), Volume 2	R
	ITI-17: Retrieve Document	Retrieve Document is used by a Document Consumer to retrieve a document from a repository	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), Volume 2	R
	ITI-14: Register Document Set	Register Document Set transaction passes a Submission Request for documents from a repository to a registry	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Volume 2	R
Document Registry	ITI-14: Register Document Set	Register Document Set transaction passes a Submission Request for documents from a repository to a registry	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Volume 2	R
	ITI-18: Registry Stored Query	Registry Stored Query is used by a Document Consumer to query a registry for information about documents indexed in the registry (see Note)	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), XDS Stored Query Supplement	R
Document Consumer	ITI-17: Retrieve Document	Retrieve Document is used by a Document Consumer to retrieve a document from a repository	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), Volume 2	R
	ITI-18: Registry Stored Query	Registry Stored Query is used by a Document Consumer to query a registry for information about documents indexed in the registry (see Note)	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), XDS Stored Query Supplement	R

Note: The IHE ITI Technical framework 4.0 includes a Query Registry Transaction (ITI-16) which has been made optional and replaced by the ITI-18 Registry Stored Query introduced by the XDS Stored Query Supplement.

Figure 3.2.1-1 Cross-Enterprise Document Sharing – XDS.a Diagram



3.2.2 LIST OF TRANSACTIONS FOR XDS.B OPTION

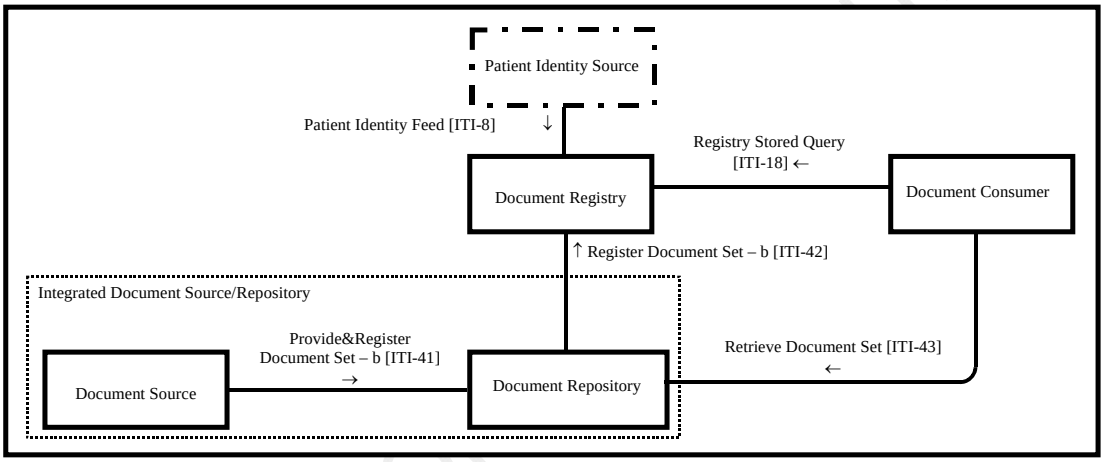
Table 3.2.2-1 List of Transactions for XDS.b

Actor Name	Transaction Name	Description	Document Name	Required = R Optional = O Conditional = C
Document Source	ITI-41: Provide & Register Document Set-b	Provide and Register Document Set is used to provide a set of documents to a repository, and to request that the repository store these documents and then register them with a registry	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), XDS.b Supplement	R
Document Repository	ITI-41: Provide & Register Document Set-b	Provide and Register Document Set is used to provide a set of documents to a repository, and to request that the repository store these documents and then register them with a registry	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), XDS.b Supplement	R
	ITI-42: Register Document Set-b	Register Document Set transaction passes a Submission Request for documents from a repository to a registry	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) XDS.b Supplement	R
	ITI-43: Retrieve Document Set	Retrieve Document Set is used by a Document Consumer to retrieve one or more documents from a repository	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) XDS.b Supplement	R
Document Registry	ITI-42: Register Document Set-b	Register Document Set transaction passes a Submission Request for documents from a repository to a registry	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) XDS.b Supplement	R
	ITI-18: Registry Stored Query	Query Registry is used by a document consumer to query a registry for information about documents indexed in the registry (see Note)	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), XDS Stored Query Supplement	R

Actor Name	Transaction Name	Description	Document Name	Required = R Optional = O Conditional = C
Document Consumer	ITI-43: Retrieve Document Set	Retrieve Document Set is used by a Document Consumer to retrieve one or more documents from a repository	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) XDS.b Supplement	R
	ITI-18: Registry Stored Query	Query Registry is used by a Document Consumer to query a registry for information about documents indexed in the registry (see Note)	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), XDS Stored Query Supplement	R

Note: The IHE ITI Technical framework 4.0 includes a Query Registry Transaction (ITI-16) which has been made optional and replaced by the ITI-18 Registry Stored Query introduced by the XDS Stored Query Supplement.

Figure 3.2.2-1 Cross-Enterprise Document Sharing – XDS.b Diagram



3.2.3 LIST OF TRANSACTIONS FOR XCA OPTION

Table 3.2.3-1 List of Transactions for XCA

Actor Name	Transaction Name	Description	Document Name	Required = R Optional = O Conditional = C
Initiating Gateway	ITI-38: Cross Gateway Query	Cross-Community Query is used by a community to query another community in order to identify what healthcare information satisfying specific criteria may be available in the target community	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), Cross-Community Access (XCA) Supplement	R
	ITI-39: Cross Gateway Retrieve	Cross Gateway Retrieve requests the retrieval of a specific set of healthcare information (a document or documents) from a remote location.	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), Cross-Community Access (XCA) Supplement	R
Responding Gateway	ITI-38: Cross Gateway Query	Cross-Community Query is used by a community to query another community in order to identify what healthcare information satisfying specific criteria may be available in the target community	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), Cross-Community Access (XCA) Supplement	R
	ITI-39: Cross Gateway Retrieve	Cross Gateway Retrieve requests the retrieval of a specific set of healthcare information (a document or documents) from a remote location.	Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF), Cross-Community Access (XCA) Supplement	R

3.3 DEPENDENCIES

The following table shows a list of Transactions with their existing Dependencies. Dependencies usually exist when there are some additional pre-requisites for a specific Transaction specification.

Table 3.3-1 Dependencies

Transaction Name	Depends On (Name of Transaction that it depends on)	Dependency Type (Pre-condition, Post-condition, general)	Purpose (Reason for this dependency)
Register Document Set on Document Registry Actor (XDS.a Option)	TP22-Patient Identity Cross-Referencing	Pre-condition	Confirm patient exists before registering one or more documents in a submission set.
Register Document Set-b on Document Registry Actor (XDS.b Option)	TP22-Patient Identity Cross-Referencing	Pre-condition	Confirm patient exists before registering one or more documents in a submission set.

3.4 CONSTRAINTS

No applicable constraints.

4.0 TRANSACTION PACKAGE

4.1 CONTEXT OVERVIEW

This specification includes by reference the Transactions from the IHE Cross-Enterprise Document Sharing (XDS) and the Cross-Community Access (XCA) Integration Profiles. Source material is from the IHE IT Infrastructure (ITI) Technical Framework (TF), Volume 2 (ITI TF-2) and associated supplements on Registry Stored Query, XDS.b, and XCA. The IHE XDS and XCA specifications are published by Integrating the Healthcare Enterprise (IHE). The IHE XDS and XCA Integration Profile, which is reproduced in part in this specification, with specific written permission from IHE, provide sample scenarios depicting how specific technical actors should comply with the proposed standards for interoperability. Key concepts from the IHE XDS and XCA Integration Profiles are introduced in this document to help the reader understand the context of the Profile. The entire IHE XDS and XCA Integration Profiles are available at www.ihe.net

4.1.1 OVERVIEW OF IHE XDS INTEGRATION PROFILE

This section provides an overview of the IHE XDS Integration Profile. Its intent is to provide the reader with an introductory context to the XDS Profile. XDS provides the ability to register, store, and query/retrieve documents containing consumer or patient-centric health information. For more detailed explanations, examples and the complete specification see the actual the IHE XDS Integration Profile at www.ihe.net

Text extracted from the IHE XDS Integration Profile begins here:

> Cross-Enterprise Document Sharing (XDS) is focused on providing a standards-based specification for managing the sharing of patient electronic health records or documents between any healthcare entity, ranging from a private physician office to a clinic to an acute care in-patient facility or other health information system.
>
> The XDS IHE Integration Profile assumes that these enterprises belong to one or more XDS Affinity Domains. An XDS Affinity Domain is a group of healthcare enterprises that have agreed to share health information together using a common set of policies and share a common infrastructure.
>
> Examples of XDS Affinity Domains include:
>
> - Community of Care supported by a Regional Health Information Organization in order to serve all patients in a given region
> - Nationwide EHR
> - Specialized or Disease-Oriented Care

    - Cardiology Specialists and an Acute Cardiology Center
    - Oncology Network
    - Diabetes Network
- Federation of Enterprises
    - A regional federation made up of several local hospitals and healthcare providers
- Government Sponsored Facilities (e.g., VA or Military)
- Insurance Provider Supported Communities

Within an XDS Affinity Domain, certain common policies and business rules must be defined. They include how patients are identified, consent is obtained, and access is controlled, as well as the format, content, structure, organization and representation of health information. This Integration Profile does not define specific policies and business rules; however it has been designed to accommodate a wide range of such policies to facilitate the deployment of standards-based infrastructures for sharing patient health documents. This is managed through federated document repositories and a Document Registry to create a longitudinal record of information about a patient within a given XDS Affinity Domain. These are distinct entities with separate responsibilities:

- A Document Repository is responsible for storing documents in a transparent, secure, reliable and persistent manner and responding to document retrieval requests

- A Document Registry is responsible for storing information about those documents so that the documents of interest for the care of a patient may be easily found, selected and retrieved irrespective of the repository where they are actually stored

The concept of a document in XDS is not limited to textual information. As XDS is document content neutral, any type of health information without regard to content and representation is supported. This makes the XDS IHE Integration Profile equally able to handle documents containing simple text, formatted text (*e.g.,* HL7 CDA Release 1), images (*e.g.*, DICOM) or structured and vocabulary coded clinical information (*e.g.*, CDA Release 2, DICOM SR). In order to ensure the necessary interoperability between the Document Sources and the Document Consumers, the XDS Affinity Domain must adopt policies concerning document format, structure and content.

Text from the IHE XDS Integration Profile ends here.

4.1.2 OVERVIEW OF THE IHE XCA INTEGRATION PROFILE

This section provides an overview of the IHE XCA Integration Profile. Its intent is to provide the reader with an introductory context to the XCA Profile.

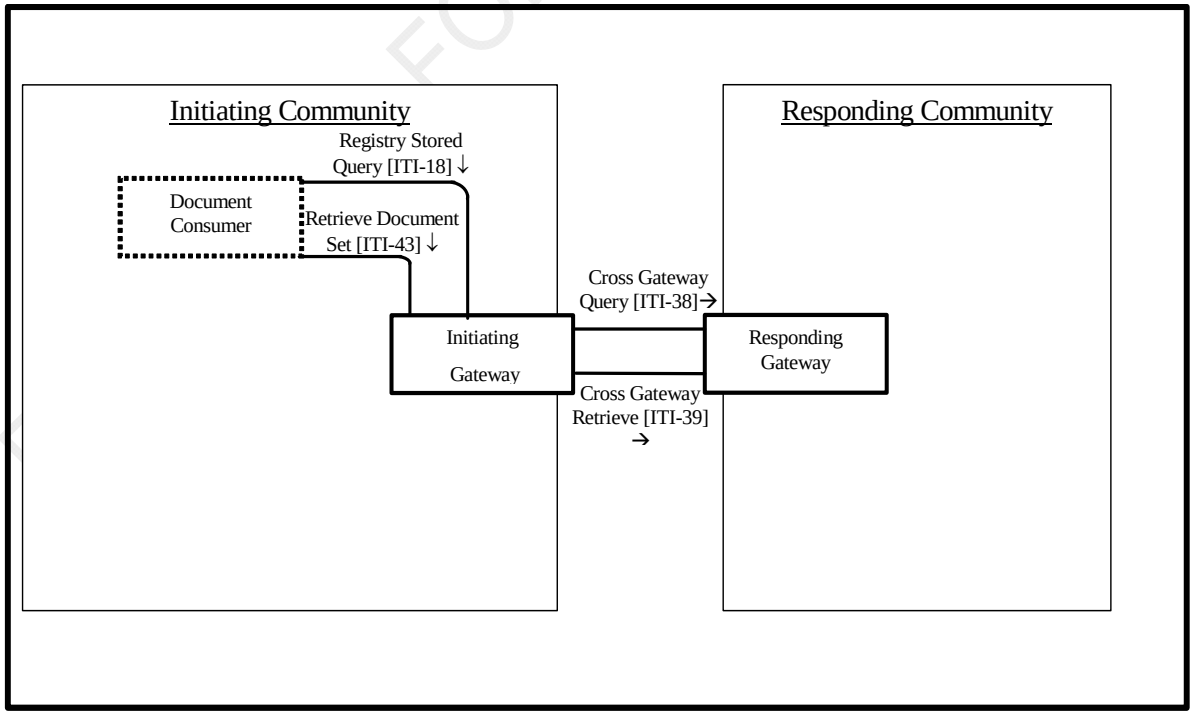
Text extracted from the IHE XCA Integration Profile begins here:

The Cross Community Access (XCA) profile supports the means to query and retrieve patient relevant medical data held by other communities. A community is defined as a coupling of facilities/enterprises that have agreed to work together using a common set of policies for the purpose of sharing clinical information via an established mechanism. Facilities/enterprises may host any type of healthcare application such as EHR, PHR, etc. A community is identifiable by a globally unique ID called the homeCommunityId. Membership of a facility/enterprise in one community does not preclude it from being a member in another community. Such communities may be XDS Affinity Domains which define document sharing using the XDS Profile or any other communities, no matter what their internal sharing structure.

Assume within a given domain, such as the State of California, we have several healthcare communities (or XDS Affinity Domains or RHIOs/HIEs). One in Los Angeles is based on IHE-XDS. One in Sacramento is based on another form of healthcare sharing infrastructure. One in San Francisco is also based on IHE-XDS. A patient X, who travels frequently, has received healthcare in each of these communities. Patient X is admitted to a hospital in LA. The attending physician uses his hospital information system to query across multiple domains for healthcare information about this patient. Once found, references to patient data outside the local domain are cached locally for easy future reference.

Figure 18.1-1 shows the actors directly involved in the XCA Integration Profile and the relevant transactions between them.

Figure 18.1-1 – XCA Actor Diagram

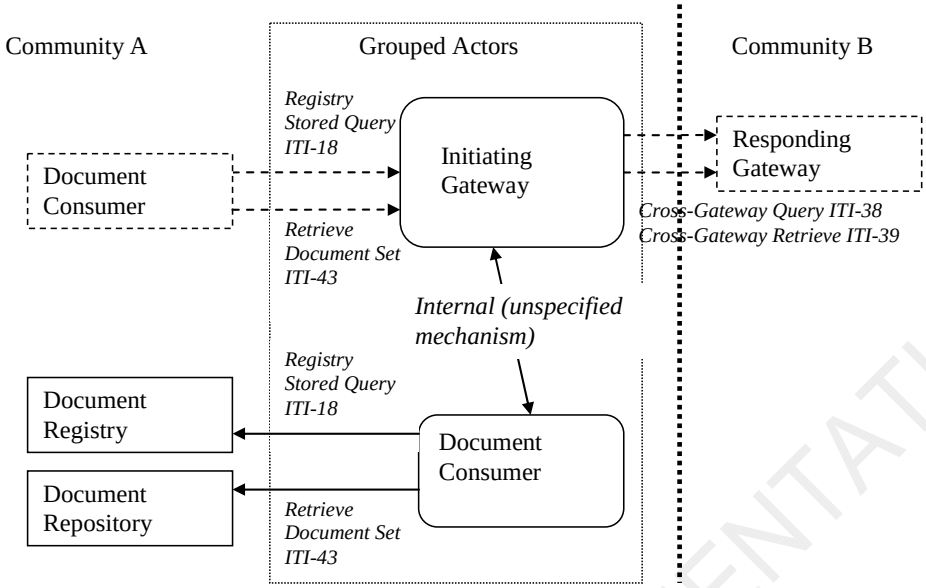


The Document Consumer Actor is shown in Figure 18.1-1 to clarify the responsibility of the XDS Affinity Domain Option. Initiating Gateways, which support the XDS Affinity Domain Option, interact with Document Consumers within the XDS Affinity Domain served by the Initiating Gateway. Initiating Gateway actors which support this option:

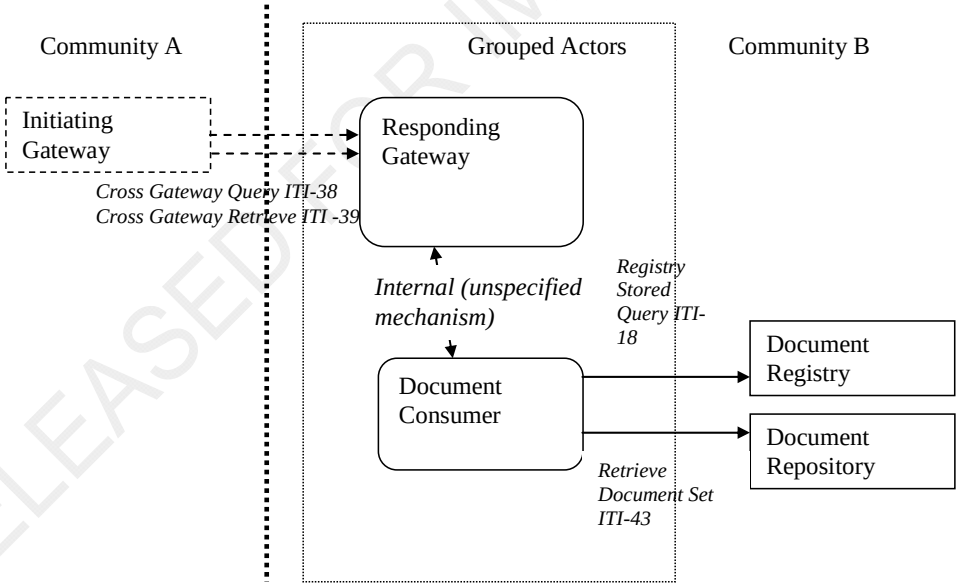
- shall **receive** Registry Stored Query [ITI-18] transactions from a local Document Consumer actor and act on those requests on behalf of the Document Consumer. When receiving a Registry Stored Query from a local Document Consumer, shall require the homeCommunityId as an input parameter on relevant queries, and shall specify the homeCommunityId attribute within its Registry Stored Query responses. See IHE XCA Section 18.3.2 for description of homeCommunityId
- shall **receive** Retrieve Document Set [ITI-43] transactions from a local Document Consumer actor and act on those requests on behalf of the Document Consumer. When receiving a Retrieve Document Set from a local Document Consumer, shall require the homeCommunityId as an input parameter

When an Initiating Gateway does not support the XDS Affinity Domain option it is expected to be using non-IHE specified interactions to communicate remote community data to systems within its local community. These proprietary interactions are not further described within any IHE Profile. The use of XCA for the Integration of XDS and non-XDS communities is discussed further in the IHE ITI Technical Framework XCA Supplement, Appendix E section E.6.

When an Initiating Gateway is supporting an XDS Affinity Domain, it can choose to query and retrieve from local actors in addition to remote communities. This is accomplished by grouping the Initiating Gateway Actor with a Document Consumer Actor. This grouping allows Document Consumers such as EHR/PHR/etc systems to query the Initiating Gateway to retrieve document information and content from both the local XDS Affinity Domain as well as remote communities. For details see IHE XCA Section 18.2.2.1. An Initiating Gateway Actor that is not grouped with a Document Consumer Actor is only able to return results from remote communities, so local EHR/PHR/etc systems (Document Consumer Actors) must direct separate query and document retrieve transactions internally and externally.



When a Responding Gateway is supporting an XDS Affinity Domain, it may resolve Cross Gateway Query and Cross Gateway Retrieve Transactions by grouping with a Document Consumer Actor and using the Registry Stored Query and Retrieve Document Set transactions. For details see 18.2.2.2



Text from the IHE XCA Integration Profile ends here.

4.1.3 CONTEXTUAL CONSTRAINTS

4.1.3.1 DOCUMENT INTEGRITY (OPTIONAL)

The following is the requirement derived from existing AHIC Use Cases for Document Integrity:

- Data needs to be protected so that they are not altered in violation of any existing policies

The use of HITSP/T17 - Secured Communication Channel provides strong protections of authenticity, integrity and confidentiality of the transactions but does not cover changes that might have occurred while the document was stored for long periods of time in the Document Repository.

Document Integrity requires Document Consumers to validate the SHA-1 hash, which is an attribute maintained in the Document Registry for all documents maintained in Document Repositories. When a document is provided and registered, as per this specification, the SHA-1 hash attribute should be filled in by the Document Source. If it is not then the Document Repository fills in the hash before registering the document. Under either scenario, the hash is required to exist in the Document Registry.

It is important to note that once a document is forwarded outside the scope of the HITSP Interoperability Specifications (for example, a lab result document forwarded to a business actor not included in the Interoperability Specification), Document Integrity is not persisted and is no longer asserted. This Document Integrity option when combined with access controls, and audit controls can provide a low or medium level of Nonrepudiation (See HITSP/C26 - Nonrepudiation of Origin for further discussion of Nonrepudiation and for a high assurance solution). Note that a Document Source that is in possession of a previously registered document may validate the SHA-1 hash at any time using this method.

Table 4.1.3.1-1 Data Mapping

Data Element	Description	Limit/Range of values	Data Source	Destination	Requirements/Pre-conditions
SHA-1	HITSP/TP13 - Manage Sharing of Documents - XDS metadata	The Document Consumer must validate the SHA-1 hash once they have received a document	XDS		Without this constraint, Document Integrity cannot be verified

Text from the IHE XDS Integration Profile begins here:

> The XDS Integration Profile is not intended to address all cross-enterprise EHR communication needs. Some scenarios may require the combined use of other IHE Integration Profiles, such as Patient Identifier Cross-Referencing, Audit Trail and Node Authentication, and Cross-Enterprise User Assertion. Other scenarios may be only partially supported, while still others may require future IHE Integration profiles, which will be defined by IHE as soon as the necessary base standards are available. Specifically:

- The access to information in targeted environments where it is dynamically managed, such as a current allergy lists, medication lists, problem lists, etc. is not addressed by XDS. Although, access to this information within a longitudinal patient record may be managed by XDS, only access to this information in published documents will be available. IHE has defined a separate Integration Profile called Query for Existing Data (QED) to obtain this information for a specific target system.
- The placing and tracking of orders (e.g., drug prescriptions, radiology orders, etc.) is not supported by XDS. This does not preclude the use of XDS to store and register orders and corresponding results when such artifacts need to be recorded in the patient's health record. However, XDS provides no facilities for tracking progress of an order through its workflow, and therefore is not intended for order management. A complementary approach to cross-enterprise order workflow (ePrescription, eReferral) may be expected as separate Integration Profiles in the future.
- The operation of any XDS Affinity Domain will require that a proper security model be put in place. It is expected that a range of security models should be possible. Although the XDS Integration Profile is not intended to include nor require any specific security model, it is expected that XDS implementers will group XDS Actors with actors from the IHE Audit Trail and Node Authentication Profile and will need an Access Control capability that operates in such a cross-enterprise environment. Specific IHE Integration Profiles complementary to XDS are available (e.g., Cross-Enterprise User Assertion, Document Digital Signature, Basic Patient Privacy Consent, etc.) and may be expected in the future.
- The establishment of independent but consistently XDS-based Affinity Domains will call for their federation, as patients expect their records to follow them as they move from region to region, or country to country. IHE foresees a need for accessing information from one XDS Affinity Domain to another, or to allow access from one XDS Affinity Domain to documents managed in non-XDS Affinity Domains. Cross-Community Access (XCA) addresses in part this need. As standards mature in this area, additional Profiles may be expected in the future.
- XDS does not address transactions for the management or configuration of an XDS Affinity Domain. For example, the configuration of network addresses or the definition of what type of clinical information is to be shared is specifically left up to the policies established by the XDS Affinity Domain.

Text from the IHE XDS Integration Profile ends here.

4.1.4 TECHNICAL ACTORS

Options that may be selected for this Construct are listed below:

- In IHE-ITI-TF-1, Section 10.2, table 10.2-1 (in the IHE XDS Integration Profile) along with the Actors to which they apply

- In IHE-ITI-XCA Supplement Section 18.2, table 18.2-1 (in the IHE XCA Integration Profile) along with the Actors to which they apply

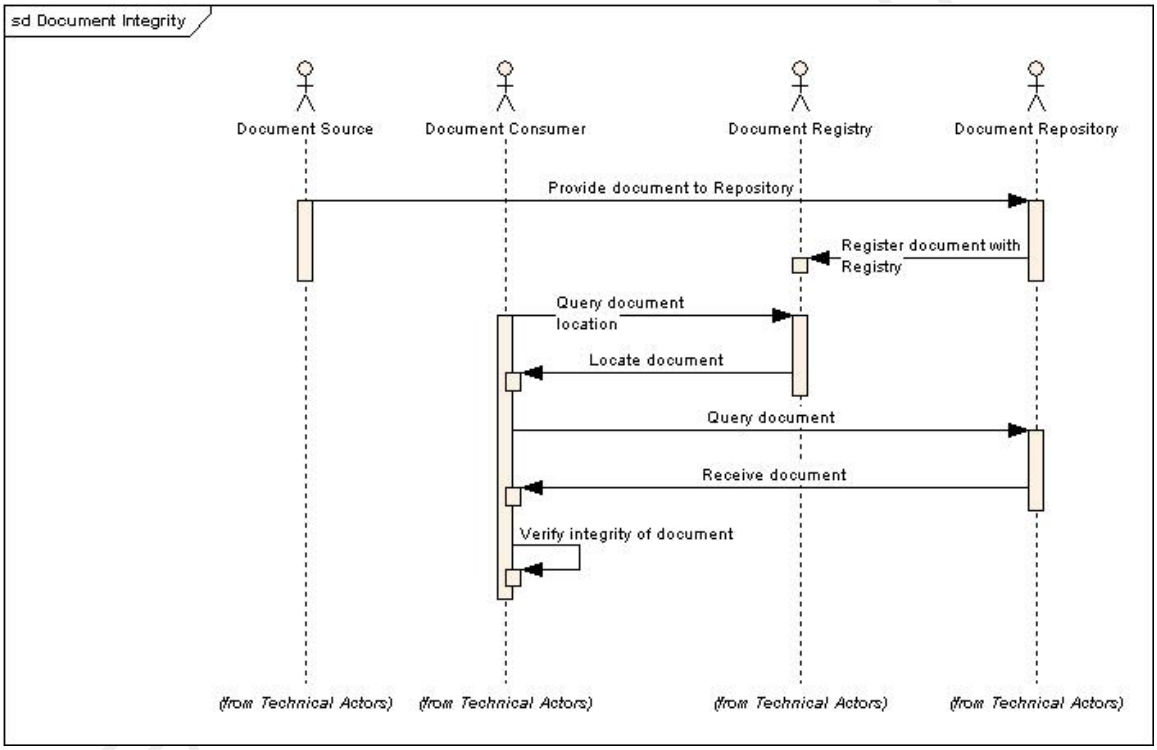
4.1.5 ACTOR INTERACTIONS

The relationship between the technical actors and the transactions of this Transaction Package are shown in IHE-ITI-TF-1, Section 10.1 (in the IHE Technical Framework, XDS Integration Profile Chapter).

4.1.5.1 DOCUMENT INTEGRITY OPTION

The following diagram further illustrates where the optional verification of Document Integrity is performed within an XDS Affinity Domain. This option applies both on the XDS.a and the XDS.b options.

Figure 4.1.5.1-1 Optional Document Integrity Sequence Diagram



The diagram above outlines several interactions that are integral to the establishment of Document Integrity. The storage and querying of documents, as occurs in the Provide Document to Repository transaction is the trigger by which the Document Integrity activity is invoked. Once a document is provided to the Document Repository by the Document Source, the document is also registered in a Registry, so that it can be located.

Once a document is stored into a Document Repository, it can be located through a registry query and then retrieved by the Document Consumer.

The “Verify Integrity of Document” interaction is a required activity that must occur in order to ensure that Document Integrity is validated. This represents the validation of the SHA-1 hash attribute by the Document Consumer.

4.2 PROCESS FLOWS

The process flows supported by this Transaction Package are shown in IHE-ITI-TF-1 Section 10.4.1 (in the IHE XDS Integration Profile).

4.2.1 PROCESS PRE-CONDITIONS WITHIN A COMMUNITY

The following Pre-conditions are assumed to be in place for the successful execution of the XDS.a and XDS.b options in this Transaction Package within a community supporting an XDS Affinity Domain:

1. The Patient Identity Feed Transaction conveys the patient identifier. It conveys the patient identifier and corroborating demographic data, captured when a patient’s identity is established, modified or merged or in cases where the key corroborating demographic data has been modified. Its purpose in the IHE XDS Integration Profile is to populate the registry with patient identifiers that have been registered for the domain
2. Organizations that share documents are part of the same XDS Affinity Domain. If they belong to different XDS Affinity Domains, these are hierarchically federated (e.g. sub-networks within one RHIO/HIE), or integrated by means not specified by HITSP (See Section 6.1.2 Cross-Affinity Domain Document Sharing)

4.2.1.1 PROCESS TRIGGERS

This section describes the triggers, including actors and/or processes, which are necessary for the XDS.a and XDS.b Options in this Transaction Package.

- The **Document Consumer Actor** queries a Document Registry Actor for documents meeting certain criteria, and retrieves selected documents from one or more Document Repository actors
- The **Document Source Actor** is the producer and publisher of documents. It is responsible for sending documents to a Document Repository Actor. It also supplies metadata to the Document Repository Actor for subsequent registration of the documents with the Document Registry Actor
- The **Document Registry Actor** maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumer Actors about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration
- The **Document Repository** is responsible for both the persistent storage of these documents as well as for their registration with the appropriate Document Registry. It assigns a Uniform Resource Identifier to documents for subsequent retrieval by a Document Consumer
- The **Patient Identity Source Actor** is a provider of a unique identifier for each patient and maintains a collection of identity traits. The Patient Identify Source facilitates the validation of patient identifiers by the Registry Actor in its interactions with other actors

4.2.2 PROCESS POST-CONDITIONS WITHIN A COMMUNITY

The desired Post-conditions for the XDS.a and XDS.b options in this Transaction Package are:

- The patient was successfully identified unambiguously
- Sources and consumers of document(s) were effectively identified
- The document was successfully retrieved by the requesting system (e.g., local or remote EHR system, authorized public health agencies)
- The authorized public health agencies have gained access to the document

If the optional Document Integrity constraint is applied, then the following post-conditions are also desired:

- Failed validation of the SHA-1 hash, the document shall be considered invalid by the supporting application
- Successful validation of the SHA-1 hash, the document shall be considered valid by the supporting application

4.2.2.1 PROCESS OUTPUTS

There were no identified outputs from the processes supported for the XDS.a and XDS.b options in this Transaction Package other than the integration of the documents into the clinician's EHR system and Biosurveillance database.

If the optional Document Integrity constraint applied, then the following outputs are identified:

- Require application to record an audit event to indicate a failed validation of the SHA-1 hash

4.2.3 PROCESS PRE-CONDITIONS ACROSS COMMUNITIES

The following Pre-conditions are assumed to be in place for the successful execution of the XCA Option in this Transaction Package across communities:

1. The communities providing access to each other need to have agreed to a patient identification cross-referencing process. This may be supported dynamically by using other HITSP Constructs such Patient ID Cross-Referencing (TP22) or Patient Demographics Query (T23) or other means agreed between pairs of communicating communities. Further development in this area may be expected in the future.
2. The communities providing access to each other need to have established a trust relationship, especially in terms of matching their respective security and privacy policies. This is likely to be achieved by peer-to-peer agreement without electronic transactions. Some of the existing HITSP security constructs are likely to be relevant. In the area of privacy and consent directive management, additional HITSP may be developed in the future. IHE has developed a white paper (See www.ihe.net) and continues work in this area along with NHIN projects and several Health Information Exchange projects.

4.2.3.1 PROCESS TRIGGERS

This section describes the triggers, including actors and/or processes, which are necessary for the XCA Option in this Transaction Package.

- The **Initiating Gateway Actor** supporting a Community queries one or more Responding Gateway Actor each serving one or more communities for documents meeting certain criteria, and retrieves selected documents from the respective Responding Gateway Actors
- The **Responding Gateway Actor** supporting one or more communities receives queries and documents or retrieve requests from remote Initiating Gateways and responds to these requests

4.2.4 PROCESS POST-CONDITIONS ACROSS COMMUNITIES

The desired Post-conditions for Cross-Community Access for the XCA Option in this Transaction Package are:

- The patient was successfully identified unambiguously
- Initiating and responding gateways were effectively identified
- The documents were successfully retrieved by the requesting community (e.g., an XDS Affinity Domain, an integrated delivery network, a health information exchange which does not support the intra-community interoperability from this Transaction Package)

4.3 DATA FLOWS

See IHE Infrastructure IT Technical Framework specifications for clinical examples.

5.0 TECHNICAL IMPLEMENTATION

5.1 CONFORMANCE

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

5.1.1 CONFORMANCE CRITERIA

In order to claim conformance to this construct specification, an implementation must satisfy all the requirements and mandatory statements listed in this specification, the associated HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards.

A conformant system must also be constrained as specified in this construct, and implement all of the required transactions associated with the actor to be supported from

Table 3.2.1-1 (XDS.a), Table 3.2.2-1 (XDS.b) or Table 3.2.3-1 (XCA), within the scope, subset or implementation option that is selected from the referencing Interoperability Specification.

Claims of conformance may only be made for an overall HITSP Interoperability Specification with which this construct is associated.

5.1.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

A HITSP Interoperability Specification must be implemented in its entirety for an implementation to claim conformance to the specification. HITSP may define the permissibility for actor scoping, subsetting or implementation options by which the specification may be implemented in a limited manner. Such scoping, subsetting and options may extend to associated constructs, such as this construct. This construct must implement all requirements within the selected scope, subset or options as defined in the associated Interoperability Specification to claim conformance.

This construct defines the following options that may be selected by the referencing HITSP Interoperability Specification.

5.1.2.1 INTRA-COMMUNITY SHARING OF DOCUMENTS (XDS.a OPTION)

Within the XDS.a option, a number of options may be selected depending on the technical actor implemented as defined by Table 5.1.2.1-1.

Table 5.1.2.1-1 XDS.a – Options by Actors

Actor	Options	Vol & Section
Document Source	Multiple Document Submission	ITI TF-1:10.2.1

Actor	Options	Vol & Section
	Document Life Cycle Management	ITI TF-1:10.2.2
	Folder Management	ITI TF-1:10.2.3
Document Repository	No options defined	
Document Registry	No options defined	
Document Source Actor Integrated with a Document Repository Actor	Multiple Document Submission	ITI TF-1:10.2.1
	Document Life Cycle Management	ITI TF-1:10.2.2
	Folder Management	ITI TF-1:10.2.3
Document Consumer	No options defined	

5.1.2.2 INTRA-COMMUNITY SHARING OF DOCUMENTS (XDS.b OPTION)

Within the XDS.b option, a number of options may be selected depending on the technical actor implemented as defined by Table 5.1.2.2-1.

Table 5.1.2.2-1 XDS.b – Options by Actors

Actor	Options	Vol & Section
Document Source	Multiple Document Submission	ITI TF-1:10.2.1
	Document Life Cycle Management	ITI TF-1:10.2.2
	Folder Management	ITI TF-1:10.2.3
Document Repository	No options defined	
Document Registry	No options defined	
Document Source Actor Integrated with a Document Repository Actor	Multiple Document Submission	ITI TF-1:10.2.1
	Document Life Cycle Management	ITI TF-1:10.2.2
	Folder Management	ITI TF-1:10.2.3
Document Consumer	No options defined	

5.1.2.3 CROSS-COMMUNITY SHARING OF DOCUMENTS (XCA OPTION)

Within the XCA option, a number of options may be selected depending on the technical actor implemented as defined by Table 5.1.2.3-1.

Table 5.1.2.3-1 XCA – Options by Actors

Actor	Options	Vol & Section
Initiating Gateway	XDS Affinity Domain Option	ITI TF-1:18.2.1
Responding Gateway	No options defined	- -

5.2 SUPPORTING DOCUMENTS

See Volume 1 and 2 of the IHE IT Infrastructure Technical Framework Release 4.0 specification and XCA Supplement.

6.0 APPENDIX

6.1 GAPS

6.1.1 TERMINOLOGY

“Document Registration Terminology” is a gap. This Component will include the set of vocabularies used in the XDS Document Registry to populate the metadata associated with each document. There is no “ready terminology” to reference, but we will leverage subsets of existing terminology structures such as those used by LOINC Document dimensions.

6.1.2 CROSS-AFFINITY DOMAIN DOCUMENT SHARING

The HITSP Manage Sharing of Documents Transaction Package is based on the IHE-XDS and the IHE XCA Integration Profile referenced by HITSP from the IHE IT Infrastructure Technical Framework. This section discusses the pre-conditions associated with document sharing environments across multiple independent domains.

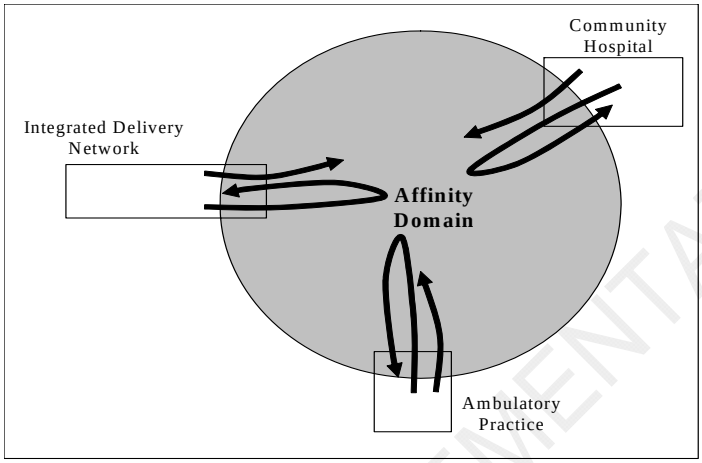
The Integrating the Healthcare Enterprise has defined an Integration Profile called Cross-Enterprise Document Sharing (XDS), which defines document sharing among a number of entities or organizations forming an XDS Affinity Domain using the IHE-XDS terminology. This construct also includes the means for Communities (XDS based or not) to access remote Communities (XDS based or not), leveraging the IHE Cross-Community Access (XCA).

For Cross-Community Access, a number of additional interoperability requirements need to be addressed beyond XCA. Some of those are addressed in specific environment by existing HITSP Constructs, others remain to be addressed:

1. Cross-Community patient identification linkage. In two common environments, this is addressed by use of the existing HITSP/TP22 (IHE-PIX) and HITSP/T23 (IHE-PDQ). This is discussed in detail in the IHE XCA supplement. Some specific issues may need further work for which HITSP should leverage lessons learned by the NHIN contractors, Connecting for Health, Federal Agencies, IHE and other implementation experiences.
2. Community Discovery. In this domain there are numerous strategies, some patient-centric such as use of a Patient Community Locator, Consumer carried smart tokens conveying community addresses, etc. This may be handled by manual configurations which may be the most practical especially when the Cross-Community consent sharing remains a complex issue.
3. Cross-Community policy matching. This area requires much work and analysis. In the short to mid-term this may be handled by manual configuration among peer communities that have performed a matching of their document sharing policies.

HITSP will contribute to and review the white paper being developed by IHE in 2008 along with other input such as lessons learned by the NHIN contractors, Connecting for Health, Federal Agencies, IHE and other implementation experiences.

Figure 6.1.2-1 XDS Affinity Domain



Within an XDS Affinity Domain, for the purpose of information exchange among the member organizations, certain common policies and business rules must be defined. Neither HITSP, nor IHE define these policies or what is the appropriate implementation of XDS Affinity Domains for the NHIN, RHIOs/HIEs, Sub-network Organizations or large enterprises such as Federal Agencies. HITSP does not rule on the number of organizations that partake. These choices are considered to be implementation, configuration or architecture decisions, not within the purview of HITSP.

Conclusion

The HITSP Manage Sharing of Documents Transaction Package addresses a number of environments while others are beyond its current scope:

1. *Single Organization – Stand-alone XDS Affinity Domain*: An organization/enterprise implements IHE-XDS internally and chooses to be a single XDS Affinity Domain, where its internal systems are Document Sources and Document Consumers. There is a Document Registry and one or more Document Repositories in the XDS Affinity Domain.
2. *Multi-Organization – Stand-alone Affinity Domain*: A number of independent organizations choose to share documents by joining in an XDS Affinity Domain. Each organization chooses to be a Document Source and /or Document Consumer. Each organization may also choose to be its own Document Repository or to use one or more shared Document Repository. There is a Document Registry in the XDS Affinity Domain (possibly hosted by one of the member organizations).
3. *Multi-Affinity Domains – Hierarchical Federation*: A number of XDS Affinity Domains, each independently managed, choose to establish a federation. With a federation level PIX Manager (e.g. an RLS as defined by Connecting for Health) and the use of Cross-Community Access (XCA) as defined by this construct, Cross-Affinity Domain access is possible.

4. *Multi-Affinity Domains – Lateral Cross-Community*: A number of XDS Affinity Domains, each independently managed, wish to establish peer-to-peer communication without establishing a federation. With the use of Cross-Community Access (XCA) as defined by this construct, Cross-Affinity Domain access is possible.

Approach 3 and 4 require further work in the area of community discovery, privacy and Cross-Community policy matching. The HITSP will leverage lessons learned by the NHIN contractors, Connecting for Health, Federal Agencies, IHE and other implementation activities as they become available.

7.0 CHANGE HISTORY

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

7.1 MAY 11, 2007

This document is now Released for Implementation.

7.2 JULY 20, 2007

Added optional constraints for assurance of Document Integrity.

7.3 SEPTEMBER 25, 2007

Added updates for relationship to Access Control and Consent Directives SPTC constructs.
Changes to this document also reflect the disposition of comments received during the public comment period of July 20 – August 16, 2007.

7.4 OCTOBER 5, 2007

The changes in this cycle address the following comments received during the Public Comment and Inspection Testing period (July 23, 2006 - August 17, 2007):

980, 981, 983, 1207, 1252, 1253, 1258

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

7.5 OCTOBER 15, 2007

Upon approval by the HITSP Panel on October 15, 2007, this document has been moved to Version 2.1. This document is now Released for Implementation.

7.6 NOVEMBER 6, 2007

The changes in this cycle introduce the optional use of XDS.b and the optional use of XCA. These changes reflect the response of IHE to address identified gaps in the previous versions. Minor updates to text throughout this document have been made where appropriate to indicate where optionality can be exercised, and what additional constraints apply when optionality is invoked.

7.6.1 VERSION COMPATIBILITY:

Note 1: This is identical to the interoperability supported by HITSP/TP13 Version 2.0
Note 2: Gap identified in XDS as defined by HITSP/TP13 Version 2.0, June 2006

7.7 DECEMBER 5, 2007

The changes in this cycle address the following comments:

2557

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

7.8 DECEMBER 13, 2007

Upon approval by the HITSP Panel on December 13, 2007, this document is now Released for Implementation.