ACC, HIMSS and RSNA

Integrating the Healthcare Enterprise

IT Infrastructure Technical Framework

Volume 1 (ITI TF-1) Integration Profiles

Revision 2.0 – Final Text

August 15, 2005

Contents

1 Introduction

Integrating the Healthcare Enterprise (IHE) is an initiative designed to stimulate the integration of the information systems that support modern healthcare institutions. Its fundamental objective is to ensure that in the care of patients all required information for medical decisions is both correct and available to healthcare professionals. The IHE initiative is both a process and a forum for encouraging integration efforts. It defines a technical framework for the implementation of established messaging standards to achieve specific clinical goals. It includes a rigorous testing process for the implementation of this framework. And it organizes educational sessions and exhibits at major meetings of medical professionals to demonstrate the benefits of this framework and encourage its adoption by industry and users.

The approach employed in the IHE initiative is to support the use of existing standards, e.g HL7, ASTM, DICOM, ISO, IETF, OASIS and others as appropriate, rather than to define new standards. IHE profiles further constrain configuration choices where necessary in these standards to ensure that they can be used in their respective domains in an integrated manner between different actors. When clarifications or extensions to existing standards are necessary, IHE refers recommendations to the relevant standards bodies.

This initiative has numerous sponsors and supporting organizations in different medical specialty domains and geographical regions. In North America the primary sponsors are the American College of Cardiology (ACC), the Healthcare Information and Management Systems Society (HIMSS) and the Radiological Society of North America (RSNA). IHE Canada has also been formed. IHE Europe (IHE-EUR) is supported by a large coalition of organizations including the European Association of Radiology (EAR) and European Congress of Radiologists (ECR), the Coordination Committee of the Radiological and Electromedical Industries (COCIR), Deutsche Röntgengesellschaft (DRG), the EuroPACS Association, Groupement pour la Modernisation du Système d'Information Hospitalier (GMSIH), Société Francaise de Radiologie (SFR), Società Italiana di Radiologia Medica (SIRM), and the European Institute for health Records (EuroRec). In Japan IHE-J is sponsored by the Ministry of Economy, Trade, and Industry (METI); the Ministry of Health, Labor, and Welfare; and MEDIS-DC; cooperating organizations include the Japan Industries Association of Radiological Systems (JIRA), the Japan Association of Healthcare Information Systems Industry (JAHIS), Japan Radiological Society (JRS), Japan Society of Radiological Technology (JSRT), and the Japan Association of Medical Informatics (JAMI). Other organizations representing healthcare professionals are invited to join in the expansion of the IHE process across disciplinary and geographic boundaries.

1.1 Overview of the Technical Framework

This document, the IHE IT Infrastructure Technical Framework (ITI TF), defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of medical information to support optimal patient care. It is expanded annually, after a period of public review, and maintained regularly through the identification and correction of

errata. The current version, rev. 2.0 for Final Text, specifies the IHE transactions defined and implemented as of August 2005. The latest version of the document is always available via the Internet at http://www.ihe.net/Technical_Framework .

The IHE IT Infrastructure Technical Framework identifies a subset of the functional components of the healthcare enterprise, called IHE actors, and specifies their interactions in terms of a set of coordinated, standards-based transactions. It describes this body of transactions in progressively greater depth. The present volume (ITI TF-1) provides a high-level view of IHE functionality, showing the transactions organized into functional units called integration profiles that highlight their capacity to address specific IT Infrastructure requirements.

Volume 2 of the IT Infrastructure Technical Framework (ITI TF-2) provides detailed technical descriptions of each IHE transaction used in the IT Infrastructure Integration Profiles. These two volumes are consistent and can be used in conjunction with the Integration Profiles of other IHE domains.

The other domains within the IHE initiative also produce Technical Frameworks within their respective areas that together form the IHE Technical Framework. Currently, the following IHE Technical Framework(s) are available:

- IHE IT Infrastructure Technical Framework
- IHE Cardiology Technical Framework
- IHE Laboratory Technical Framework
- IHE Patient Care Coordination Technical Framework
- IHE Radiology Technical Framework

Where applicable, references are made to other technical frameworks. For the conventions on referencing other frameworks, see Section 1.6.3 within this volume.

1.2 Overview of the IT Infrastructure Volume I

The remainder of Section 1 further describes the general nature, purpose and function of the Technical Framework. Section 2 introduces the concept of IHE Integration Profiles that make up the Technical Framework.

Section 3 and the subsequent sections of this volume provide detailed documentation on each integration profile, including the IT Infrastructure problem it is intended to address and the IHE actors and transactions it comprises.

The appendices following the main body of the document provide a summary list of the actors and transactions, detailed discussion of specific issues related to the integration profiles and a glossary of terms and acronyms used.

1.3 Audience

The intended audience of this document is:

- IT departments of healthcare institutions

- Technical staff of vendors participating in the IHE initiative
- Experts involved in standards development
- Those interested in integrating healthcare information systems and workflows

1.4 Relationship to Standards

The IHE Technical Framework identifies functional components of a distributed healthcare environment (referred to as IHE actors), solely from the point of view of their interactions in the healthcare enterprise. At its current level of development, it defines a coordinated set of transactions based on ASTM, DICOM, HL7, IETF, ISO, OASIS and W3C standards. As the scope of the IHE initiative expands, transactions based on other standards may be included as required.

In some cases, IHE recommends selection of specific options supported by these standards; however, IHE does not introduce technical choices that contradict conformance to these standards. If errors in or extensions to existing standards are identified, IHE's policy is to report them to the appropriate standards bodies for resolution within their conformance and standards evolution strategy.

IHE is therefore an implementation framework, not a standard. Conformance claims for products must still be made in direct reference to specific standards. In addition, vendors who have implemented IHE integration capabilities in their products may publish IHE Integration Statements to communicate their products' capabilities. Vendors publishing IHE Integration Statements accept full responsibility for their content. By comparing the IHE Integration Statements from different products, a user familiar with the IHE concepts of actors and integration profiles can determine the level of integration between them. See Appendix C for the format of IHE Integration Statements.

1.5 Relationship to Real-world Architectures

The IHE actors and transactions described in the IHE Technical Framework are abstractions of the real-world healthcare information system environment. While some of the transactions are traditionally performed by specific product categories (e.g. HIS, Clinical Data Repository, Radiology Information Systems, Clinical Information Systems or Cardiology Information Systems), the IHE Technical Framework intentionally avoids associating functions or actors with such product categories. For each actor, the IHE Technical Framework defines only those functions associated with integrating information systems. The IHE definition of an actor should therefore not be taken as the complete definition of any product that might implement it, nor should the framework itself be taken to comprehensively describe the architecture of a healthcare information system.

The reason for defining actors and transactions is to provide a basis for defining the interactions among functional components of the healthcare information system environment. In situations where a single physical product implements multiple functions, only the interfaces between the product and external functions in the environment are considered to be significant by the IHE initiative. Therefore, the IHE initiative takes no position as to the relative merits of an integrated

environment based on a single, all-encompassing information system versus one based on multiple systems that together achieve the same end. IHE demonstrations emphasize the integration of multiple vendors' systems based on the IHE Technical Framework.

1.6 Conventions

This document has adopted the following conventions for representing the framework concepts and specifying how the standards upon which the IHE Technical Framework is based should be applied.

1.6.1 IHE Actor and Transaction Diagrams and Tables

Each integration profile is a representation of a real-world capability that is supported by a set of actors that interact through transactions. Actors are information systems or components of information systems that produce, manage, or act on categories of information required by operational activities in the enterprise. Transactions are interactions between actors that communicate the required information through standards-based messages.

The diagrams and tables of actors and transactions in subsequent sections indicate which transactions each actor in a given profile must support.

The transactions shown on the diagrams are identified both by their name and the transaction number as defined in ITI TF-2. The transaction numbers are shown on the diagrams as bracketed numbers prefixed with the specific Technical Framework domain.

In some cases, a profile is dependent on a prerequisite profile in order to function properly and be useful. For example, Enterprise User Authentication depends on Consistent Time. These dependencies can be found by locating the desired profile in Table 2-1 to determine which profile(s) are listed as prerequisites. An actor must implement all required transactions in the prerequisite profiles in addition to those in the desired profile.

1.6.2 Process Flow Diagrams

The descriptions of integration profiles that follow include process flow diagrams that illustrate how the profile functions as a sequence of transactions between relevant actors.

These diagrams are intended to provide an overview so the transactions can be seen in the context of an institution's workflow. Certain transactions and activities not defined in detail by IHE are shown in these diagrams in *italics* to provide additional context on where the relevant IHE transactions fit into the broader scheme of healthcare information systems.

These diagrams are not intended to present the only possible scenario. Often other actor groupings are possible, and transactions from other profiles may be interspersed.

In some cases the sequence of transactions may be flexible. Where this is the case there will generally be a note pointing out the possibility of variations. Transactions are shown as arrows oriented according to the flow of the primary information handled by the transaction and not necessarily the initiator.

1.6.3 Technical Framework Cross-references

When references are made to another section within a Technical Framework volume, a section number is used by itself. When references are made to other volumes or to a Technical Framework in another domain, the following format is used:

<domain designator> TF-<volume number>: <section number>, where

<domain designator> is a short designator for the IHE domain (ITI = IT Infrastructure, RAD = Radiology)

<volume number> is the applicable volume within the given Technical Framework (e.g., 1, 2, 3), and

<section number> is the applicable section number.

For example: ITI TF-1: 3.1 refers to Section 3.1 in volume 1 of the IHE IT Infrastructure Technical Framework. RAD TF-3: 4.33 refers to Section 4.33 in volume 3 of the IHE Radiology Technical Framework. ITI TF-2: Appendix B refers to Appendix B in volume 2 of the IHE IT Infrastructure Technical Framework.

When references are made to Transaction numbers in the Technical Framework, the following format is used:

[<domain designator>-<transaction number>], where

<transaction number> is the transaction number within the specified domain.

For example: [ITI-1] refers to Transaction 1 from the IHE IT Infrastructure Technical Framework.

1.7 Scope of Changes Introduced in the Current Year

The IHE Technical Framework is updated annually to reflect new profiles, corrections and new transactions (refer to ITI TF-2) used in those profiles.

This document expands the V1.0 IT Infrastructure Technical Framework and includes integration profiles developed in the 2003-2004 as well as the new profiles finalized in the 4-200-2005 cycle of the IHE IT Infrastructure initiative. It will be the basis for the 2006 connectathon testing and exhibition process associated in particular with the HIMSS 2006 annual meeting.

The V1.0 IHE IT Infrastructure Technical Framework included five Integration Profiles to which this V2.0 applies a small set of Change Proposals (CP) for clarifications or corrections as a result from implementers feedback.

Retrieve Information for Display (RID) – a simple and rapid read-only access to patient information necessary for provision of better care. It supports access to existing persistent documents in well-known presentation formats such as CDA, PDF, JPEG, etc. It also supports access to specific key patient-centric information such as allergies, current medications, summary of reports, etc. for presentation to a clinician.

Enterprise User Authentication (EUA) – a means to establish one name per user that can then be used on all of the devices and software that participate in this integration profile, greatly facilitating centralized user authentication management and providing users with the convenience and speed of a single sign-on. This profile leverages Kerberos (RFC 1510) and the HL7 CCOW standard (user subject).

Patient Identifier Cross-referencing (PIX) – provides cross-referencing of patient identifiers from multiple Patient Identifier Domains. These patient identifiers can then be used by identity consumer systems to correlate information about a single patient from sources that know the patient by different identifiers.

Patient Synchronized Applications (PSA) – a means for viewing data for a single patient using independent and unlinked applications on a user's workstation, reducing the repetitive tasks of selecting the same patient in multiple applications. Data can be viewed from different Identifier Domains when used with the Patient Identifier Cross-referencing Integration Profile to resolve multiple identifications for the same patient. This profile leverages the HL7 CCOW standard specifically for patient subject context management. .

Consistent Time (CT) – mechanisms to synchronize the time base between multiple actors and computers. Various infrastructure, security, and acquisition profiles require use of a consistent time base on multiple computers. The Consistent Time Profile provides a median synchronization error of less than 1 second.

This Version 2.0 IT Infrastructure Technical Framework finalizes four new Integration Profiles developed and tested in the 2004-2005 cycle:

Patient Demographics Query (PDQ) – 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.

Audit Trail and Node Authentication (ATNA) – establishes the characteristics of a Basic Secure Node:

1. 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.
2. It defines basic auditing requirements for the node
3. It defines basic security requirements for the communications of the node using TLS or equivalent functionality.
4. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information.

This 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

Radiology Audit Trail option in the IHE Radiology Technical Framework is an example of such an extension.

Personnel White Pages (PWP) – provides access to basic human workforce user directory information. This information has broad use among many clinical and non-clinical applications across the healthcare enterprise.

Cross-Enterprise Document Sharing (XDS) – enables a number of healthcare delivery organizations belonging to a clinical affinity domain (e.g. a community of care) to cooperate in the care of a patient by sharing clinical records in the form of documents as they proceed with their patients' care delivery activities. This profile is based upon ebXML Registry standards, SOAP, HTTP and SMTP. It describes the configuration of an ebXML Registry in sufficient detail to support Cross Enterprise Document Sharing.

1.8 Security Implications

IHE transactions often contain information that must be protected in conformance with privacy laws and regulations, such as HIPAA or similar requirements in other regions. IHE includes a few security and privacy-focused profiles listed below. Other IHE Profiles generally do not have specific privacy protections, but rather expect a proper grouping with one or more of the security profiles:

- The Audit Trail and Node Authentication (ATNA) profile specifies a means to ensure that nodes in a network are authenticated.
- The ATNA profile specifies an audit message for reporting security- and privacy-relevant events.
- The Enterprise User Authentication (EUA) profile specifies a means to authenticate system users and to share knowledge of the authenticated users among applications.
- The Personnel White Pages (PWP) profile provides a repository that may be used to hold system users' identification data.

Implementers may follow these IHE profiles to fulfill some of their security needs. It is understood that institutions must implement policy and workflow steps to satisfy enterprise needs and to comply with regulatory requirements.

1.9 Comments

HIMSS and RSNA welcome comments on this document and the IHE initiative. They should be directed to the discussion server at http://ihe.rsna.org/ihetf/ or to:

Chris Carr
Director of Informatics
820 Jorie Boulevard

Joyce Sensmeier
Director of Professional Services
230 East Ohio St., Suite 500

Oak Brook, IL 60523
Email: ihe@rsna.org

Chicago, IL 60611
Email: ihe@himss.org

1.10 Copyright Permission

1.11 IHE Technical Framework Development and Maintenance Process

The IHE IT Infrastructure Technical Framework is continuously maintained and expanded on an annual basis by the IHE IT Infrastructure Technical Committee. The development and maintenance process of the Framework follows a number of principles to ensure stability of the specification so that both vendors and users may use it reliably in specifying, developing and acquiring systems with IHE integration capabilities.

The first of these principles is that any extensions, clarifications and corrections to the Technical Framework must maintain backward compatibility with previous versions of the framework in order to maintain interoperability with systems that have implemented IHE Actors and Integration Profiles defined there.

The IHE IT Infrastructure Technical Framework is developed and re-published annually following a three-step process:

1. The IT Infrastructure Technical Committee develops supplements to the current stable version of the Technical Framework to support new functionality identified by the IHE Strategic and Planning Committees and issues them for public comment.

2. The Committee addresses all comments received during the public comment period and publishes an updated version of the Technical Framework for “Trial Implementation.” This version contains both the stable body of the Technical Framework from the preceding cycle and the newly developed supplements. It is the version of the Technical Framework used by vendors in developing trial implementation software for the annual IT Infrastructure Connectathon.

3. The Committee regularly considers change proposals to the Trial Implementation version of the Technical Framework, including those from implementers who participate in the Connectathon. After resolution of all change proposals received within 60 days of the Connectathon, the Technical Framework version is published as “Final Text”.

2 IT Infrastructure Integration Profiles

IHE IT Infrastructure Integration Profiles (Figure 2-1), offer a common language that healthcare professionals and vendors can use to discuss integration needs of healthcare enterprises and the integration capabilities of information systems in precise terms. Integration Profiles specify implementations of standards that are designed to meet identified clinical needs. They enable users and vendors to state which IHE capabilities they require or provide, by reference to the detailed specifications of the IHE IT Infrastructure Technical Framework.

Integration profiles are defined in terms of IHE Actors and transactions. Actors (see ITI TF-1, Appendix A) are information systems or components of information systems that produce, manage, or act on information associated with clinical and operational activities in the enterprise. Transactions (see ITI TF-1, Appendix B) are interactions between actors that communicate the required information through standards-based messages.

Vendor products support an Integration Profile by implementing the appropriate actor(s) and transactions. A given product may implement more than one actor and more than one integration profile.

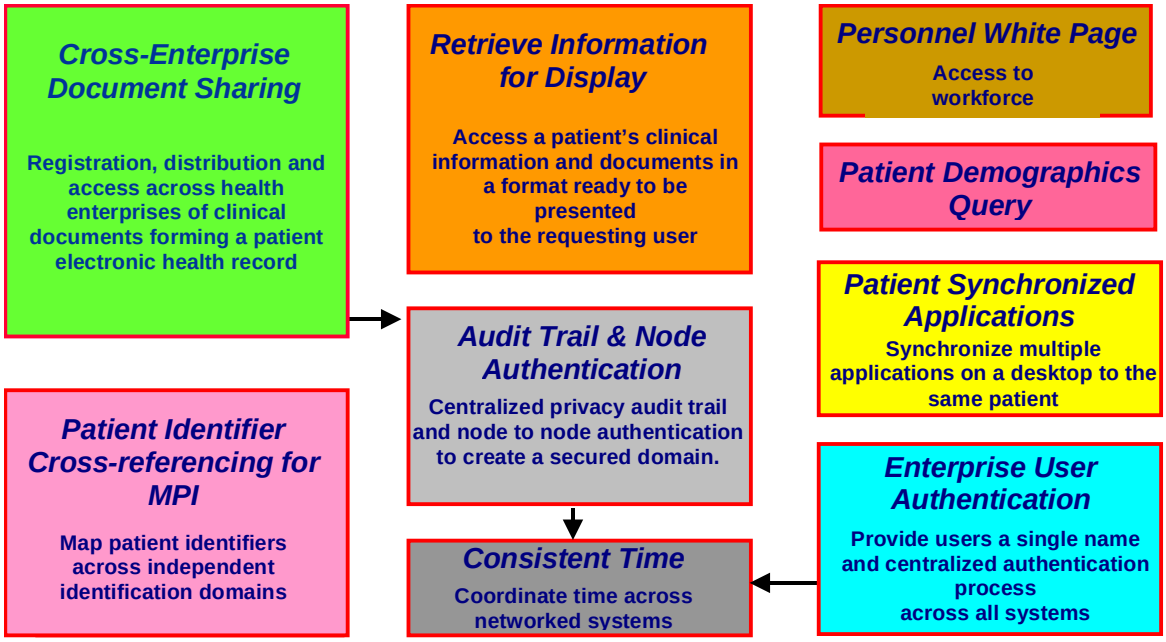


Figure 2-1 IHE IT Infrastructure Integration Profiles

2.1 Dependencies among Integration Profiles

Dependencies among IHE Integration Profiles exist when implementation of one integration profile is a prerequisite for achieving the functionality defined in another integration profile. Figure 2-1 provides a graphical view of the dependencies among IHE IT Infrastructure

Integration Profiles. The arrows in the figure point from a given integration profile to the integration profile(s) upon which it depends. Table 2-1 defines these dependencies in tabular form.

Some dependencies require that an actor supporting one profile be grouped with one or more actors supporting other integration profiles. For example, Enterprise User Authentication (EUA) requires that different participating actors be grouped with the Time Client Actor that participates in the Consistent Time (CT) Integration Profile. The dependency exists because EUA actors must refer to consistent time in order to function properly.

Table 2-1 Integration Profiles Dependencies

Integration Profile	Depends on	Dependency Type	Purpose
Retrieve Information for Display Integration	*None*	None	-
Enterprise User Authentication	Consistent Time	Each actor implementing EUA shall be grouped with the Time Client Actor	- Required to manage expirations of authentication tickets
Patient Identifier Cross-referencing	Consistent Time	Each actor implementing PIX shall be grouped with the Time Client Actor	Required to manage and resolve conflicts in multiple updates.
Patient Synchronized Applications	*None*	*None*	-
Consistent Time	*None*	*None*	-
Patient Demographics Query	*None*	*None*	-
Personnel White Pages	*None*	*None*	-
Audit trail and Node Authentication	Consistent Time	Each actor implementing ATNA shall be grouped with the Time Client Actor	- Required for consistent time in audit logs.
Cross-Enterprise Document Sharing	Audit Trail and Node Authentication	Each XDS Actor must be grouped with the Secure Node Actor.	- Required to manage audit trail of exported PHI, node authentication and transport encryption.

To support a dependent profile, an actor must implement all required transactions in the prerequisite profiles in addition to those in the dependent profile. In some cases, the prerequisite is that the actor selects any one of a given set of profiles.

2.2 Integration Profiles Overview

In this document, each IHE Integration Profile is defined by:

- The IHE actors involved
- The specific set of IHE transactions exchanged by each IHE actor.

These requirements are presented in the form of a table of transactions required for each actor supporting the Integration Profile. Actors supporting multiple Integration Profiles are required to support all the required transactions of each Integration Profile supported. When an Integration

Profile depends upon another Integration Profile, the transactions required for the dependent Integration Profile have not been included in the table.

Note that IHE Integration Profiles are not statements of conformance to standards, and IHE is not a certifying body. Users should continue to request that vendors provide statements of their conformance to standards issued by relevant standards bodies, such as HL7 and DICOM. Standards conformance is a prerequisite for vendors adopting IHE Integration Profiles.

Also note that there are critical requirements for any successful integration project that IHE cannot address. Successfully integrating systems still requires a project plan that minimizes disruptions and describes fail-safe strategies, specific and mutually understood performance expectations, well-defined user interface requirements, clearly identified systems limitations, detailed cost objectives, plans for maintenance and support, etc.

2.2.1 Retrieve Information for Display (RID)

Retrieve Information for Display enables simple and rapid access to patient information for better care. It supports access to existing persistent documents in well-known presentation formats such as CDA, PDF, JPEG, etc. It also supports access to specific key patient-centric information such as allergies, current medications, summary of reports, etc. for presentation to a clinician. It complements workflows from within the users' on-screen workspace or application. By linking it with two other IHE profiles - Enterprise User Authentication and Patient Identifier Cross-referencing, this profile's reach can extend across organization boundaries within an enterprise. This IHE Integration Profile leverages HTTP, Web Services, IT presentation formats and HL7 CDA Level 1.

2.2.2 Enterprise User Authentication (EUA)

Enterprise User Authentication (EUA) – Defines a means to establish one name per user that can then be used on all of the devices and software that participate in this integration profile. It greatly facilitates centralized user authentication management and provides users with the convenience and speed of a single sign-on. This profile leverages Kerberos (RFC 1510) and the HL7 CCOW standard (user subject). User authentication is a necessary step for most application and data access operations and streamlines workflow for users. Future profiles will deal with other security issues, such as authorization management.

2.2.3 Patient Identifier Cross-referencing (PIX)

The PIX profile supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains. These cross-referenced patient identifiers can then be used by "identity consumer" systems to correlate information about a single patient from sources that "know" the patient by different identifiers. This allows a clinician to have more complete view of the patient information.

2.2.4 Patient Synchronized Applications (PSA)

Patient Synchronized Applications supports viewing data for a single patient among otherwise independent and unlinked applications on a user's workstation. Its implementation reduces the repetitive tasks of selecting the same patient in multiple applications. It also improves patient safety by reducing the chance of medical errors caused by viewing the wrong patient's data. Its ability to work with the Patient Identifier Cross-referencing provides a seamless environment for clinicians and IT staff. This profile leverages the HL7 CCOW standard specifically for patient subject context management.

2.2.5 Consistent Time (CT)

Consistent Time Profile defines mechanisms to synchronize the time base between multiple actors and computers. Various infrastructure, security, and acquisition profiles require use of a consistent time base on multiple computers. The Consistent Time Profile provides median synchronization error of less than 1 second. Configuration options can provide better synchronization. The Consistent Time profile specifies the use of the Network Time Protocol (NTP) defined in RFC 1305.

2.2.6 Patient Demographics Query (PDQ)

Patient Demographics Query 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.

2.2.7 Audit Trail and Node Authentication (ATNA)

Audit Trail and Node Authentication establishes the characteristics of a Basic Secure Node:

1. 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.
2. It defines basic auditing requirements for the node
3. It defines basic security requirements for the communications of the node using TLS or equivalent functionality.
4. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information.

This 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 Radiology Audit Trail option in the IHE Radiology Technical Framework is an example of such an extension.

2.2.8 Personnel White Pages (PWP)

Personnel White Pages Profile (PWP) provides access to basic human workforce user directory information. This information has broad use among many clinical and non-clinical applications across the healthcare enterprise. The information can be used to enhance the clinical workflow (contact information), enhance the user interface (user friendly names and titles), and ensure identity (digital certificates). This Personnel White Pages directory will be related to the User Identity provided by the Enterprise User Authentication (EUA) Integration Profile previously defined by IHE.

2.2.9 Cross-Enterprise Document Sharing (XDS)

Cross-Enterprise Document Sharing enables a number of healthcare delivery organizations belonging to a clinical affinity domain (e.g. a community of care) to cooperate in the care of a patient by sharing clinical records in the form of documents as they proceed with their patients' care delivery activities. Federated document repositories and a document registry create a longitudinal record of information about a patient within a given clinical affinity domain. This profile is based upon ebXML Registry standards, SOAP, HTTP and SMTP. It describes the configuration of an ebXML Registry in sufficient detail to support Cross Enterprise Document Sharing.

2.3 Product Implementations

Developers have a number of options in implementing IHE actors and transactions in product implementations. The decisions cover three classes of optionality:

- For a system, select which actors it will incorporate (multiple actors per system are acceptable).
- For each actor, select the integration profiles in which it will participate.
- For each actor and profile, select which options will be implemented.

All required transactions must be implemented for the profile to be supported (refer to the transaction descriptions in ITI TF-2).

Implementers should provide a statement describing which IHE actors, IHE integration profiles and options are incorporated in a given product. The recommended form for such a statement is defined in ITI TF-1, Appendix C.

In general, a product implementation may incorporate any single actor or combination of actors. When two or more actors are grouped together, internal communication between actors is assumed to be sufficient to allow the necessary information flow to support their functionality; for example, the Context Manager uses the Patient Identifier Cross-reference Consumer Actor to obtain the necessary patient identifier mapping information from the Patient Identifier Cross-reference Manager. The exact mechanisms of such internal communication are outside the scope of the IHE Technical Framework.

When multiple actors are grouped in a single product implementation, all transactions originating or terminating with each of the supported actors shall be supported (i.e., the IHE transactions shall be offered on an external product interface).

The following examples describe which actors typical systems might be expected to support. This is not intended to be a requirement, but rather to provide illustrative examples.

A departmental system, such as a laboratory information system or a radiology picture archiving and communication system might include an Information Source Actor as well as a Kerberized Server Actor.

A clinical repository might include an Information Source Actor as well as a Kerberized Server Actor and a Patient Identifier Cross-reference Consumer Actor.

A context management server might include a Context Management Actor as well as a Patient Identifier Cross-reference Consumer Actor.

3 Retrieve Information for Display (RID)

The ***Retrieve Information for Display Integration Profile (RID)*** provides simple and rapid read-only access to patient-centric clinical information that is located outside the user's current application but is important for better patient care (for example, access to lab reports from radiology department). It supports access to existing persistent documents in well-known presentation formats such as CDA (Level 1), PDF, JPEG, etc. It also supports access to specific key patient-centric information such as allergies, current medications, summary of reports, etc. for presentation to a clinician. It complements workflows with access from within the users' on-screen workspace or application to a broad range of information.

In this profile, the Information Source is solely responsible to turn the healthcare specific semantics into what this IHE Integration Profile calls a "presentation" format. As a consequence the Display actor may process and render this "presentation" format with only generic healthcare semantics knowledge. Different formats have specific characteristics in terms of (1) server imposed limitations and (2) flexibility of display on the client side to render within its display constraints (e.g. a generic CDA level 1 style sheet).

The Information Source is entirely responsible for the information returned for display and its clinical accuracy.

This profile offers the capability to leverage industry standards that address both the structure and content of documents that may be returned by information sources. Where this profile references HL7 Clinical Documentation Architecture (CDA), it limits itself to the approved CDA Level 1. Furthermore, it only uses a subset of CDA Level 1 that facilitates making information available for display.

Future extensions to the IHE IT Infrastructure TF will more fully leverage CDA Release 2 and other industry standards, and will incorporate vocabularies such as SNOMED and Clinical LOINC as well as clinical templates.

This profile does not provide specific requirements on the means of assuring access control or security of information in transit. Such measures shall be implemented through appropriate security-related integration profiles, such as Enterprise User Authentication (see Section 4). Appendix E describes the process flows for usage of the Retrieve Information for Display Integration Profile in conjunction with the Enterprise User Authentication and Patient Identifier Cross-referencing Integration Profiles.

3.1 Actors/ Transactions

Figure 3.1-1 shows the actors directly involved in the Retrieve Information for Display Integration Profile and the relevant transactions between them. Other actors that may be

indirectly involved due to their participation in User Authentication and Patient Identifier Cross-referencing are not shown.

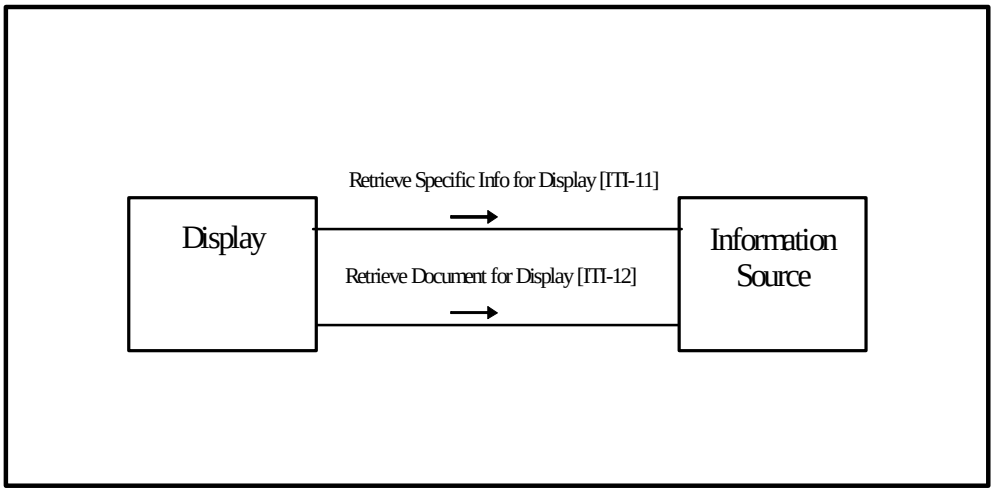


Figure 3.1-1. Retrieve Information for Display Actor Diagram

Table 3.1-1 lists the transactions for each actor directly involved in the Retrieve Information for Display Integration Profile. In order to claim support of this Integration Profile, an implementation must perform the required transactions (labeled "R"). A complete list of options defined by this Integration Profile and that implementations may choose to support is listed in ITI TF-1: 3.2.

Table 3.1-1 Retrieve Information for Display Integration Profile - Actors and Transactions

Actors	Transactions	Optionality	Section in Vol. 2
Display	Retrieve Specific Info for Display[ITI-11]	R	ITI TF-2: 3.11
	Retrieve Document for Display[ITI-12]	R	ITI TF-2: 3.12
Information Source	Retrieve Specific Info for Display[ITI-11]	R (see below)	ITI TF-2: 3.11
	Retrieve Document for Display[ITI-12]	R (see below)	ITI TF-2: 3.12

Transaction ITI-11 is required if one of the following Options is selected by the Information Source Actor (See Section 3.2):

Summary of All Reports
Summary of Laboratory Reports
Summary of Radiology Reports
Summary of Cardiology Reports
Summary of Surgery Reports
Summary of Intensive Care Reports
Summary of Emergency Reports
Summary of Discharge Reports
Summary of Prescriptions
List of Allergies and Adverse Reactions
List of Medications

Transaction [ITI-12] is required if the Persistent Document Option is selected by the Information Source Actor (See Section 3.2).

The means for a Display Actor to obtain documents' unique identifiers in order to retrieve them via Transaction [ITI-11] may be either via Transaction [ITI-12] or by other means that are outside the scope of the RID Integration Profile.

3.2 Retrieve Information for Display Integration Profile Options

Options that may be selected for this Integration Profile are listed in the Table 3.2-1 along with the IHE actors to which they apply.

Table 3.2-1 Retrieve Information for Display - Actors and Options

Actor	Options	Vol & Section
Display	*None*	- -
Information Source	Persistent Document	ITI TF-2: 3.12
	Summary of All Reports (note2)	ITI TF-2: 3.11
	Summary of Laboratory Reports (note2)	ITI TF-2: 3.11
	Summary of Radiology Reports (note2)	ITI TF-2: 3.11
	Summary of Cardiology Reports (note2)	ITI TF-2: 3.11
	Summary of Surgery Reports (note2)	ITI TF-2: 3.11
	Summary of Intensive Care Reports (note2)	ITI TF-2: 3.11
	Summary of Emergency Reports (note2)	ITI TF-2: 3.11
	Summary of Discharge Reports (note2)	ITI TF-2: 3.11
	Summary of Prescriptions (note2)	ITI TF-2: 3.11
	List of Allergies and Adverse Reactions	ITI TF-2: 3.11
	List of Medications (note1)	ITI TF-2: 3.11

Note1: List of Medications includes the list of medications currently known to be administered to the patient. It differs from the Summary of Prescriptions, in that the latter reflects what has been prescribed to the patient, but are not necessarily any longer administered.

Note2: In all the above options, "summary of reports" means that a general patient context (patient name, etc.) is provided along with a list of entries, where an entry includes key attributes such as date, specialty, and additional information sufficient to allow the viewer to select an entry. An entry may reference a persistent document for RID or other application defined RID summaries. Beyond these general guidelines, the specific content may likely be influenced by the context of use and customer desires. Such summaries are non-persistent in that they are likely to be updated in the course of patient care.

3.3 Retrieve Information for Display Process Flow

This section describes the process and information flow when displayable patient information is retrieved from an information source. Three cases are distinguished.

- **Case 1**-Retrieve *Specific* Information for Display: The first case describes use cases when the display actor and the person associated are requesting some information related to a patient. A somewhat specific request for information is issued (e.g. Retrieve a summary of laboratory reports) for a specific Patient ID to an Information Source Actor. The patient ID is assumed to be unambiguous as fully qualified with the assigning authority. A number of additional filtering keys may be used (last N reports, date range, etc.) depending on the specific type of request issued. The Information Source Actor responds with presentation-ready information that it considers relevant to the request. This Integration Profile leaves entire flexibility to the Information Source Actor to organize the content and presentation of the information returned. The Display Actor simply displays the information to the person that triggered the request. The Information Source Actor shall respond with an error message when it does not support the specific type of request or does not hold any records for the requested patient ID.

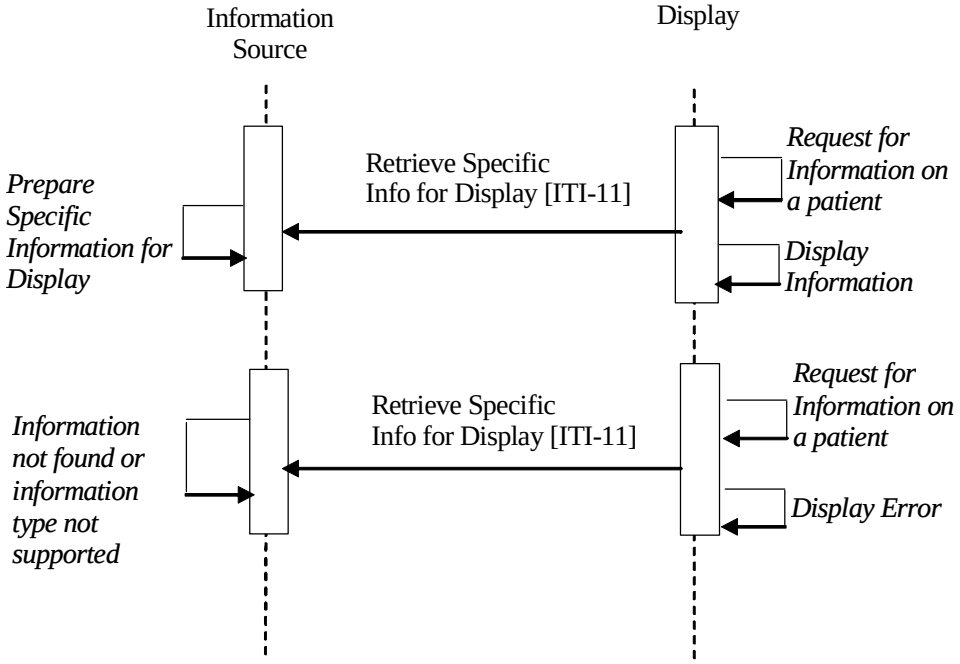


Figure 3.3-1 Case 1: Retrieve Specific Information for Display Process Flow

- **Case 2** - Retrieve a Document: The second case describes use cases when the Display Actor and the person associated are requesting a uniquely identified document such as a report, an

image, an ECG strip, etc. The Information Source Actor responds to the request by using one of the proposed formats to provide the presentation-ready content of the object it manages. The detailed presentation and the clinical integrity of the content of the document are under the control of the Information Source Actor. The Display Actor simply displays the presentation-ready document content to the person that triggered the request. The Information Source Actor shall respond with an error message when the requested document is unknown or when none of the formats acceptable to the Display Actor is suitable to present the requested document.

The main difference between the Retrieve *Specific* Information and the Retrieve *Document* transactions is that the latter applies to a uniquely identifiable persistent object (i.e. retrieving the same document instance at a different point in time will provide the same semantics for its presented content). For the Retrieve Specific Information transaction, this information is always related to a well-identified patient (Patient ID), but its content, although of a specific type (lab summary, or radiology summary, list of allergies) is generally dynamic (i.e. retrieving the same type of specific information at a different point in time is likely to result in different content; for example, a list of allergies may have been updated between two requests).

Note: This Integration profile is not intended for highly dynamic information such as that used for patient monitoring.

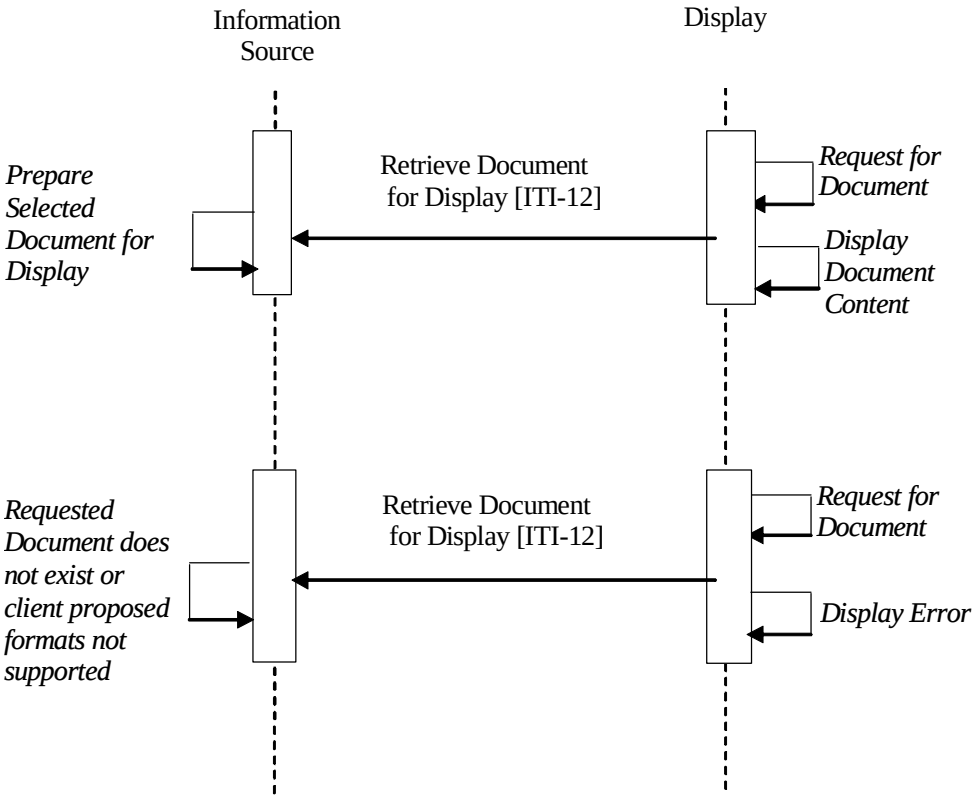


Figure 3.3-2 Case 2: Retrieve a Document Process Flow

- **Case 3** - Retrieve Specific Information for Display *and* Retrieve several Documents Process Flow: The third case combines the two cases above with the capability to associate in sequence the Retrieve Specific Information and the Retrieve Document for Display transactions. This allows for links to persistent documents within the returned specific information or for having persistent documents reference other persistent documents. For example, the user requests a summary of recent discharge reports, and then selects a specific document referenced in that summary list. From the discharge report displayed to the user, the user selects a specific surgery report. This surgery report is retrieved and displayed.

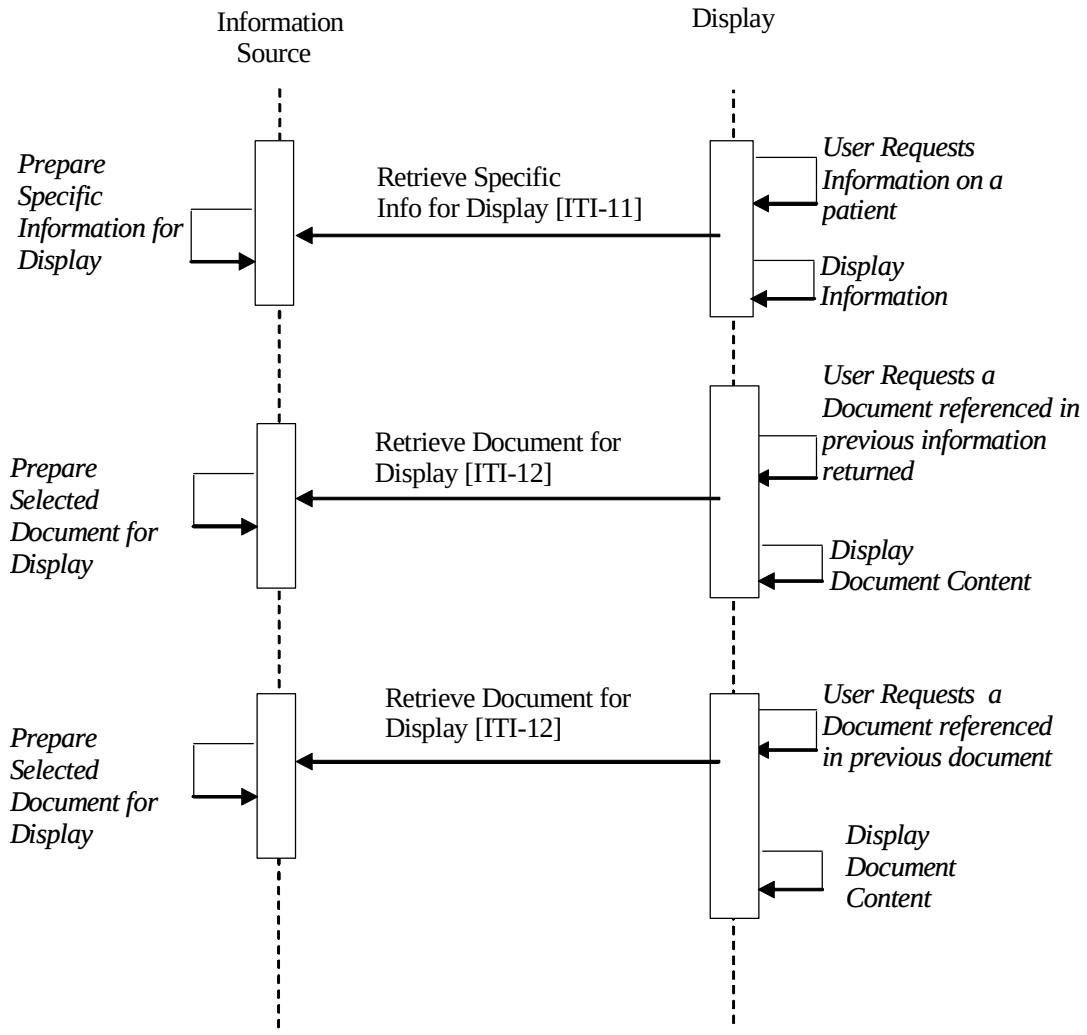


Figure 3.3-3 Case 3: Retrieve Summary Information for Display and Retrieve several Documents Process Flow

The same Display Actor may involve more than one Information Source Actor by sequentially issuing different transactions. This Integration Profile assumes that the Display Actors may be configured *a priori* with one or more remote Information Source Actors along with the type of retrieve transactions/type of requests/specific keys suitable for the application context from

which this Retrieve Information for Display requests are issued. Future Integration Profiles may facilitate such site-specific configuration tasks.

4 Enterprise User Authentication (EUA)

Enterprise User Authentication Profile (EUA) **–** This defines a means to establish one name per user that can then be used on all of the devices and software that participate in this integration profile. It greatly facilitates centralized user authentication management and provides users with the convenience and speed of a single sign-on. This profile leverages Kerberos (RFC 1510) and the HL7 CCOW standard (user subject). User authentication is a necessary step for most application and data access operations and it is a workflow improvement for the users. The IHE EUA Profile adds value to the CCOW specification for the user subject by specifying the user subject and CCOW user subject suffix. This profile does not address security features such as audit trails, access control, authorization management and PKI. Future profiles will be developed to address these security features in a manner complementary to this EUA profile.

The environment is assumed to be a single enterprise, governed by a single security policy and having a common network domain. Unsecured domains -- in particular, Internet access -- are of interest, but not in the scope of this profile. Considerations for applications such as telemedicine and patient remote access to healthcare data are therefore also not in its scope. See Appendix G.

Node and machine authentication is specified in the IHE Basic Security Profile as specified in the IHE Radiology Technical Framework and is not part of this profile.

4.1 Actors/ Transactions

A number of transactions used in this profile conform to the Kerberos v5 standard, defined in RFC 1510. This standard has been stable since 1993, is widely implemented on current operating system platforms, has successfully withstood attacks in its 10-year history, and is fully interoperable among platforms. For example, Sun Solaris, Linux, AIX, HPUX, IBM-z/OS, IBM-OS400, Novell, MAC OS X, and Microsoft Windows 2000/XP all implement Kerberos in an interoperable manner. This is not a complete list; many other vendors also support Kerberos.

For additional detailed information on Kerberos, beyond what is specified in this profile, we suggest these references:

- RFC 1510 - http://www.ietf.org/rfc/rfc1510.txt
- MIT's Kerberos home page - http://web.mit.edu/kerberos/www/
- The Moron's Guide to Kerberos - http://www.isi.edu/~brian/security/kerberos.html
- Microsoft Kerberos information http://www.microsoft.com/TechNet/prodtechnol/windows2000serv/deploy/kerberos.asp

Kerberos implementations are widely available worldwide. Kerberos does include cryptography that may have restricted use laws in some countries. The US export regulations can be found at http://www.bxa.doc.gov/Encryption.

Figure 4.1-1 shows the actors directly involved in the Enterprise User Authentication Profile and the relevant transactions between them. The box labeled "Other IHE Actor" represents actors from other integration profiles that are meant to be grouped with the nearby actor from within

this profile. Other actors that may be indirectly involved due to their use of authentication, etc. are not shown.

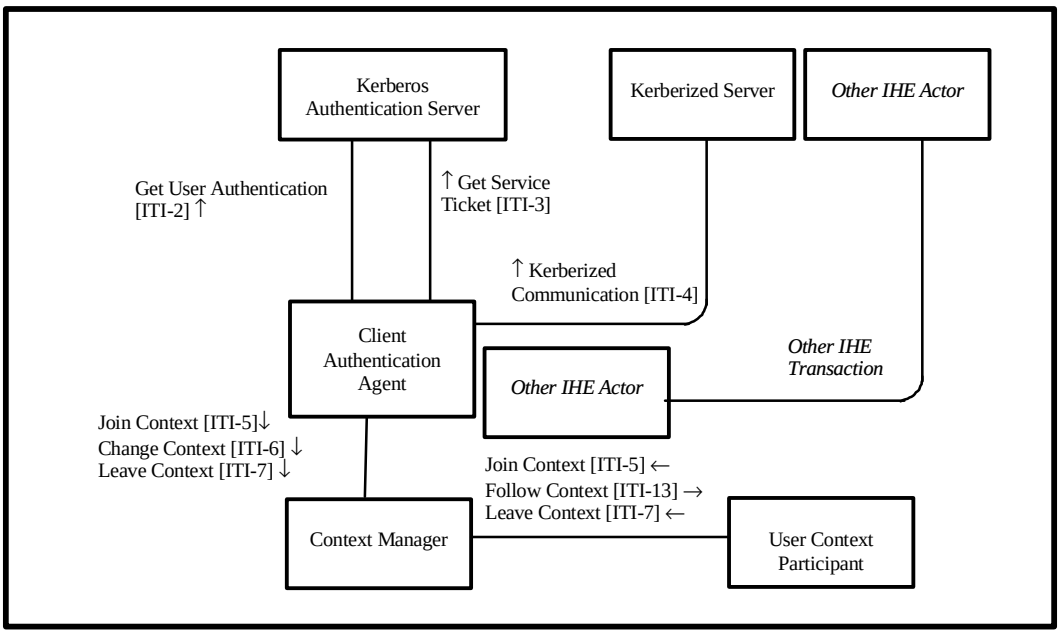


Figure 4.1-1 Enterprise Authentication Actor Diagram

Table 4.1-1 lists the transactions for each actor directly involved in the Enterprise User Authentication Profile. In order to claim support of this Integration Profile, an implementation must perform the required transactions (labeled “R”). Transactions labeled "O" are optional. A complete list of options defined in this Integration Profile and that implementations may choose to support is listed in ITI TF-1: 4.2.

Table 4.1-1 Enterprise User Authentication Profile - Actors and Transactions

Actors	Transactions	Optionality	Section in Vol. 2
Kerberos Authentication Server	Get User Authentication [ITI-2]	R	ITI TF-2: 3.2
	Get Service Ticket [ITI-3]	R	ITI TF-2: 3.3
Client Authentication Agent	Get User Authentication [ITI-2]	R	ITI TF-2: 3.2
	Get Service Ticket [ITI-3]	R	ITI TF-2: 3.3
	Kerberized Communication [ITI-4]	R	ITI TF-2: 3.4
	Join Context [ITI-5]	O [Note1]	ITI TF-2: 3.5
	Change Context [ITI-6]	O [Note1]	ITI TF-2: 3.6
	Leave Context [ITI-7]	O [Note1]	ITI TF-2: 3.7
Kerberized Server	Kerberized Communication [ITI-4]	R	ITI TF-2: 3.4
User Context Participant	Join Context [ITI-5]	R	ITI TF-2: 3.5
	Follow Context [ITI-13]	R	ITI TF-2: 3.13
	Leave Context [ITI-7]	R	ITI TF-2: 3.7
Context Manager	Join Context [ITI-5]	R	ITI TF-2: 3.5
	Follow Context [ITI-13]	R	ITI TF-2: 3.13
	Leave Context [ITI-7]	R	ITI TF-2: 3.7
	Change Context [ITI-6]	R	ITI TF-2: 3.6

Note 1: When the Authentication for User Context Option is supported, then the transaction is required.

CCOW facilitates the sharing of the identity of a EUA authentication user but does not provide for the authentication of users. In order for the Context Manager and User Context Participant to participate in the EUA profile it is required that the Client Authentication Agent supports the Authentication for User option. This design provides the User Context Participant with a consistent and enterprise recognized user identity, but does not define access to the Kerberos credentials. Future IHE profiles may address this limitation. Note that the Client Authentication Agent is the key actor when PSA and EUA are combined. See the use case outlined in Section 4.3.2. Applications that implement both the Client Authentication Agent Actor and the User Context Participant Actor shall support configurations where either Actor is disabled.

In any single user environment there shall be only one Client Authentication Agent for one user. In a multi-user environment there shall not be more than one Client Authentication Agent per user.

4.2 Enterprise User Authentication Integration Profile Options

Options that may be selected for this Integration Profile are listed in Table 4.2-1 along with the Actors to which they apply. Dependencies between options when applicable are specified in notes.

Table 4.2-1 Enterprise User Authentication - Actors and Options

Actor	Options	Vol & Section

Actor	Options	Vol & Section
Kerberos Authentication Server	*No options defined*	- -
Client Authentication Agent	*Authentication for User Context*	ITI TF-2: 3.6
Kerberized Server	*No options defined*	- -
Context Manager	*No options defined*	- -
User Context Participant	*No options defined*	- -

4.3 Enterprise User Authentication Profile Process Flow

4.3.1 Basic User Authentication Process Flow

The following diagram describes the sequence of events in the use of Enterprise User Authentication:

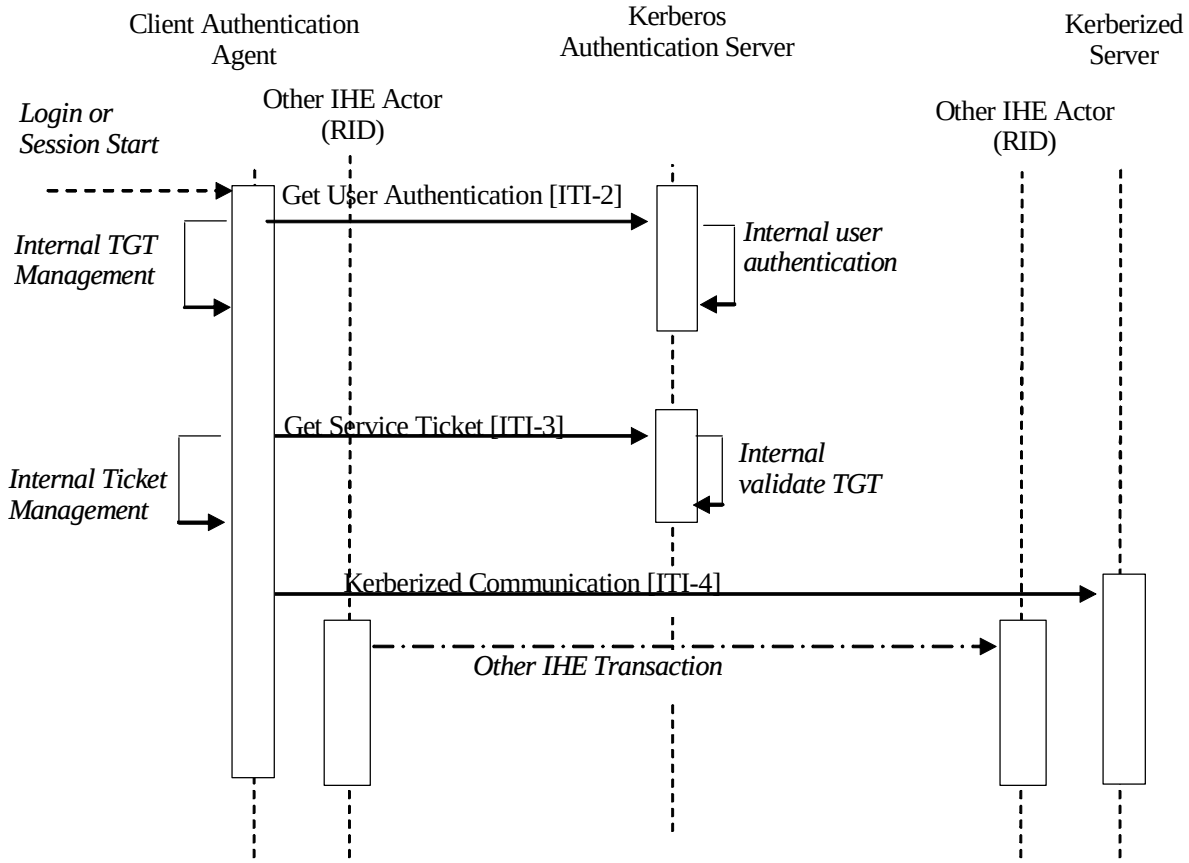


Figure 4.3.1-1. Basic Process Flow in Enterprise User Authentication Profile

The sequence of events in the use of Enterprise User Authentication is:

- The user begins the session. This initiates a local username/password authentication that is converted into the challenge/response system used by Kerberos to avoid transmitting the password over the network. This information is used as part of the Get User Authentication Transaction to get a "Ticket Granting Ticket" (TGT).
- The TGT is saved and managed internally by the Client Authentication Agent Actor. The TGT acts as confirmation that the user has been authenticated.
- For each service that has been Kerberized, the Client Authentication Agent Actor uses the Get Service Ticket Transaction to obtain a service ticket. The service ticket is then used as part of the Kerberized Communication Transaction.

A Kerberized Communication is a Kerberos data exchange that is integrated into another protocol, such as HL7 or DICOM, which is used in another IHE transaction. The details of Kerberization vary and are described separately for the protocols that have been Kerberized. The Kerberization enables the other IHE Actors involved in the other transaction to use the identity of the authenticated user for purposes such as user authorization or audit messages.

The Client Authentication Agent Actor also maintains an internal cache of credentials such as the TGT and service tickets. It renews the tickets as necessary to deal with ticket expirations, re-uses tickets while they are still valid, and removes credentials from the cache when the user session ends. The Client Authentication Agent shall make the Kerberos credentials available using the local operating system mechanisms. Other IHE Actors that need the Kerberos credentials are strongly encouraged to obtain them using the local operating system mechanisms. Operating system support for ticket management has been implemented and has been defined for various operating systems.

4.3.2 User Authentication with User Synchronized Applications Process Flow

In this use case an application supporting user authentication on the same desktop as another application is synchronized to the same user identity, thus giving the user a single-sign-on experience.

The following diagram describes the sequence of events in the use of User Authentication with User Synchronized Applications:

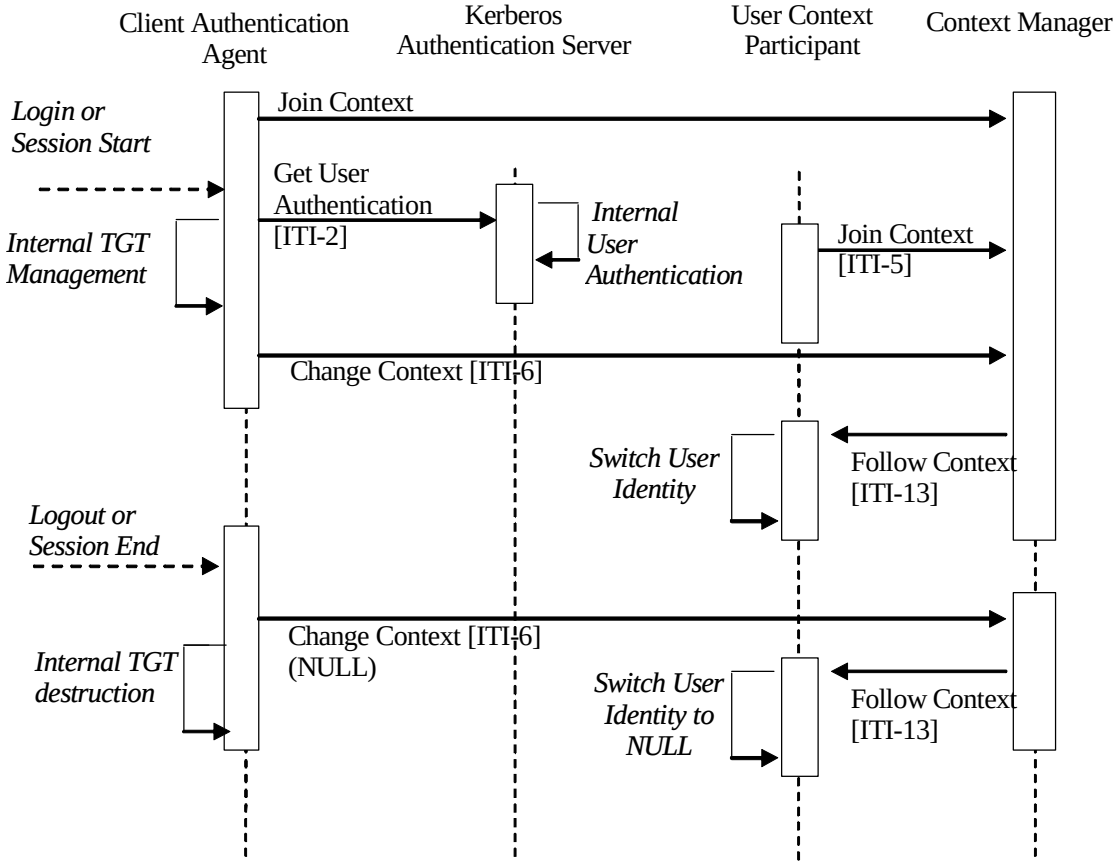


Figure 4.3.2-1 Process Flow with User Synchronized Applications

The sequence of events of the User Authentication with User Synchronized Applications is:

- The user initiates a login by starting the Client Authentication Agent.
- The Client Authentication Agent joins the CCOW user context by sending a Join Context Transaction to the Context Manager Actor. At this point there is no user identity in the context.
- The user provides their username and password to the Client Authentication Agent. This authentication information is converted into the challenge/response system used by Kerberos to avoid transmitting the password over the network. This information is used as part of the Get User Authentication Transaction to get a "Ticket Granting Ticket" (TGT).
- The TGT is saved and managed internally by the Client Authentication Agent Actor. The TGT acts as confirmation that the user has been authenticated.
- A Change Context Transaction is sent to the Context Manager Actor with the users fully qualified user name.
- The user is now logged in to the User Context Participant.
- When the user ends the session, a Change Context Transaction is sent to the Context Manager Actor with a NULL user name.

- The user is logged out of the User Context Participant.

4.3.3 Fast User Switching with Multiple Applications Process Flow

The use model in the clinical environment can be characterized as multiple clinicians using the same workstation for short intervals of time many times a day. In this shared workstation environment the user requires quick access to the patient data contained in the applications. Traditional methods of logging in and out of the workstation at the operating system or network level can take too long and typically force the applications to terminate. This means that the application clients will potentially need to initialize and establish new database connections, introducing further delay to the Clinician access to patient data. The CCOW standard and more specifically the “user” subject provides a means in combination with the Enterprise Authenticator to allow the user to authenticate at the application level and have all of the other applications tune to the new user.

The following diagram describes the sequence of events in the case of Fast User Switching with Multiple Applications:

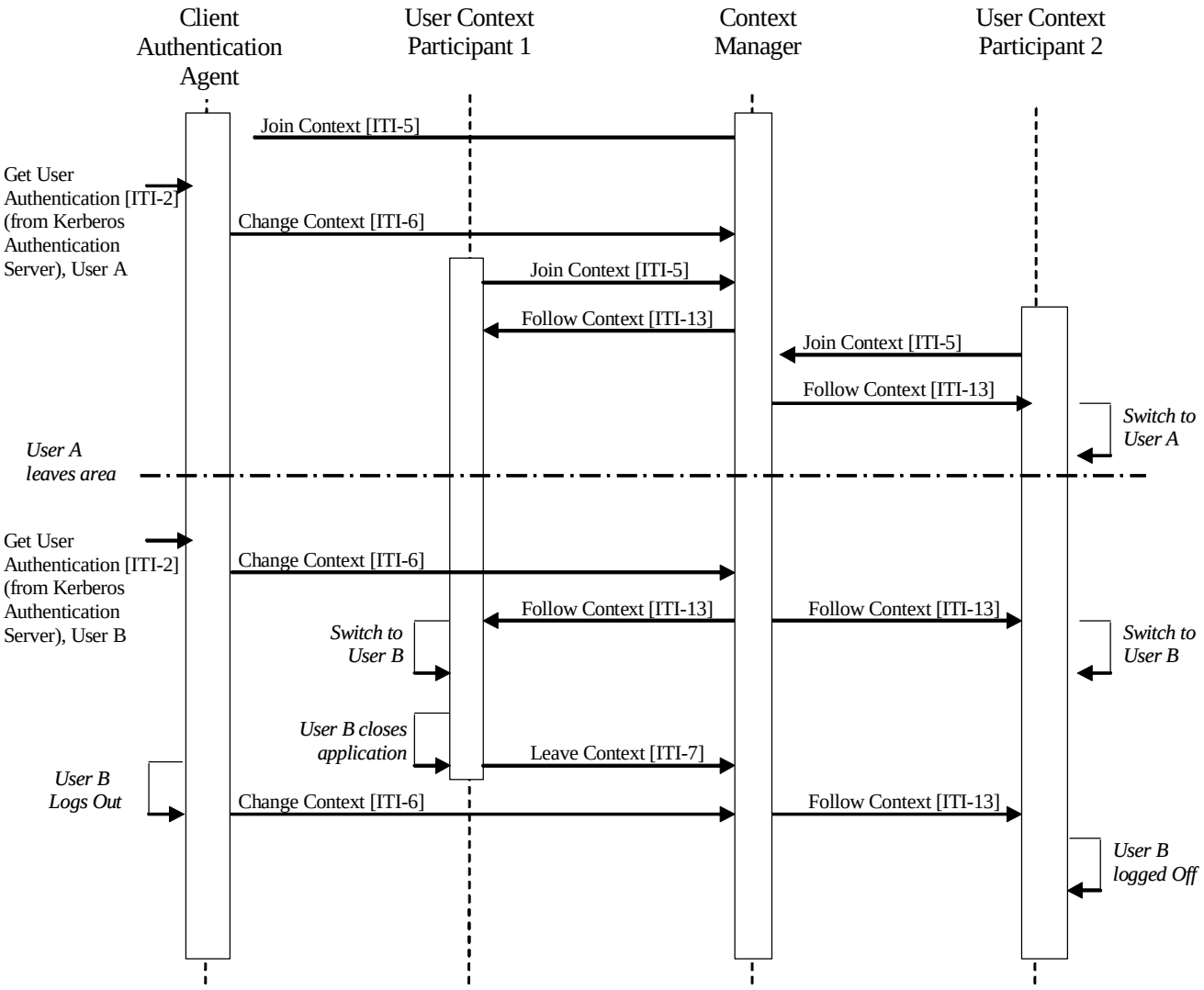


Figure 4.3.3-1. Fast User Switching when using Multiple Applications

The process flow would be similar to the following:

Clinician A launches and authenticates via an application containing the Client Authentication Agent (refer to Figure 4.3.3-1 for details). This actor joins the context session and performs a context change to set Clinician A as the user in context.

Clinician A launches the clinical data repository application, containing a User Context Participant Actor, depicted as User Context Participant 1. The actor joins the context session, gets the current user from the Context Manager, and logs clinician A into the application.

Clinician A launches a cardiology application, containing a User Context Participant Actor, depicted as User Context Participant 2. The actor joins the context session, gets the current user from the Context Manager, and logs clinician A into the application.

Clinician A does his job and then gets called away and leaves the workstation.

Clinician B approaches the workstation and authenticates using the Client Authentication Agent. This results in a context change from Clinician A to Clinician B being set in context without the delay typically associated with a logout and login at the operating system level. The clinical data repository and the cardiology application are notified of the context change by the Context Manager resulting in Clinician A being logged out of both applications and Clinician B being logged into both applications.

Clinician B does his job and then closes the clinical data repository application, which leaves the context prior to terminating the application.

Clinician B is finished reviewing patient data within the cardiology application and logs out using the Client Authentication Agent. This forces a context change to remove the current user from the context, which results in the user being logged out of the cardiology application.

5 Patient Identifier Cross-referencing (PIX)

The ***Patient Identifier Cross-referencing Integration Profile (PIX)*** is targeted at healthcare enterprises of a broad range of sizes (hospital, a clinic, a physician office, etc.). It supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains via the following interactions:

- The transmission of patient identity information from an identity source to the Patient Identifier Cross-reference Manager.
- 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.

The following diagram shows the intended scope of this profile (as described above).

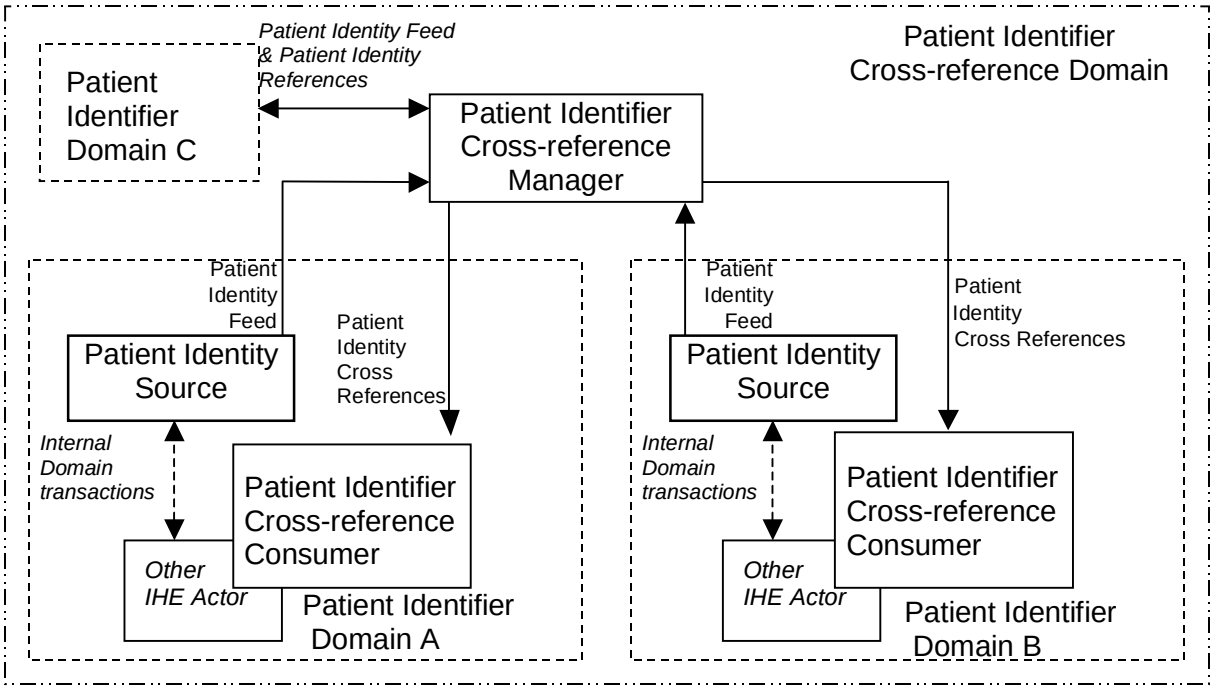


Figure 5-1 Process Flow with Patient Identifier Cross-referencing

The diagram illustrates two types of Identifier Domains: a Patient Identifier Domain and a Patient Identifier Cross-reference Domain.

A Patient Identifier Domain is defined as a single system or a set of interconnected systems that all share a common identification scheme (an identifier and an assignment process to a patient) and issuing authority for patient identifiers. Additionally, a Patient Identifier Domain has the following properties:

- A set of policies that describe how identities will be defined and managed according to the specific requirements of the domain.
- An administration authority for administering identity related policies within the domain.
- A **single** system, known as a patient identity source system, that assigns a unique identifier to each instance of a patient-related object as well as maintaining a collection of identity traits.
- Ideally, only one identifier is uniquely associated with a single patient within a given Patient Identifier Domain, though a single Patient Identity Source Actor may assign multiple identifiers to the same patient and communicate this fact to the Patient Identifier Cross-reference Manager. For a description of how the Patient Identifier Cross-reference Manager Actor responds to requests for a list of cross-referenced identifiers that include these "duplicates" see ITI TF-2: 3.9.4.2.2.6).
- An "Identifier Domain Identifier" (known as assigning authority) that is unique within a Patient Identifier Cross-reference Domain.
- Other systems in the Patient Identifier Domain rely upon the identifiers assigned by the patient identity source system of the domain to which they belong.

A Patient Identifier Cross-reference Domain consists of a set of Patient Identifier Domains known and managed by a Patient Identifier Cross-reference Manager Actor. The Patient Identifier Cross-reference Manager Actor is responsible for creating, maintaining and providing lists of identifiers that are aliases of one another across different Patient Identifier Domains.

The Patient Identifier Cross-reference Domain embodies the following assumptions about agreement within the group of individual Identifier Domains:

- They have agreed to a set of policies that describe how patient identities will be cross-referenced across participating domains;
- They have agreed to a set of processes for administering these policies;
- They have agreed to an administration authority for managing these processes and policies.

All these assumptions are critical to the successful implementation of this profile. This integration profile imposes minimal constraints on the participating Patient Identifier Domains and centralizes most of the operational constraints for the overall Patient Identification Cross-reference Domain in the Patient Identifier Cross-reference Manager Actor. If the individual Identifier Domains cannot agree to the items outlined above, implementation of this profile may not provide the expected results.

The Patient Identifier Cross-reference Manager Actor is not responsible for improving the quality of identification information provided to it by the Identity Source Actors. It is assumed that the Identity Source actors are responsible for providing high quality data to the Patient

Identifier Cross-reference Manager. For example, the Patient Identifier Cross-reference Manager Actor is NOT responsible to provide a single reference for patient demographics. The intent is to leave the responsibility for the quality and management of its patient demographics information and the integrity of the identifiers it uses within each Patient Identity Domain (Source actors). When receiving reports and displays from multiple PIX domains, it is inevitable that some of those reports and displays will have inconsistent names.

The Patient Identifier Cross-reference Consumer may use either a query for sets of cross-reference patient identifiers or use both a notification about cross-reference changes and a query transaction. In the case of using a notification, the Patient Identifier Cross-reference Consumer may also use the PIX Query Transaction to address situations where the Patient Identifier Cross-reference Consumer may be out of synch with the Patient Identifier Cross-reference Manager. This Integration Profile does not specify the consumer policies in using the PIX Query Transaction (ITI TF-2: 3.9).

For a discussion of the relationship between this Integration Profile and an enterprise master patient index (eMPI) see Section 5.4.

5.1 Actors/ Transactions

Figure 5.1-1 shows the actors directly involved in the Patient Identifier Cross-referencing Integration Profile and the relevant transactions between them. Other actors that may be indirectly involved due to their participation in other related profiles are not shown.

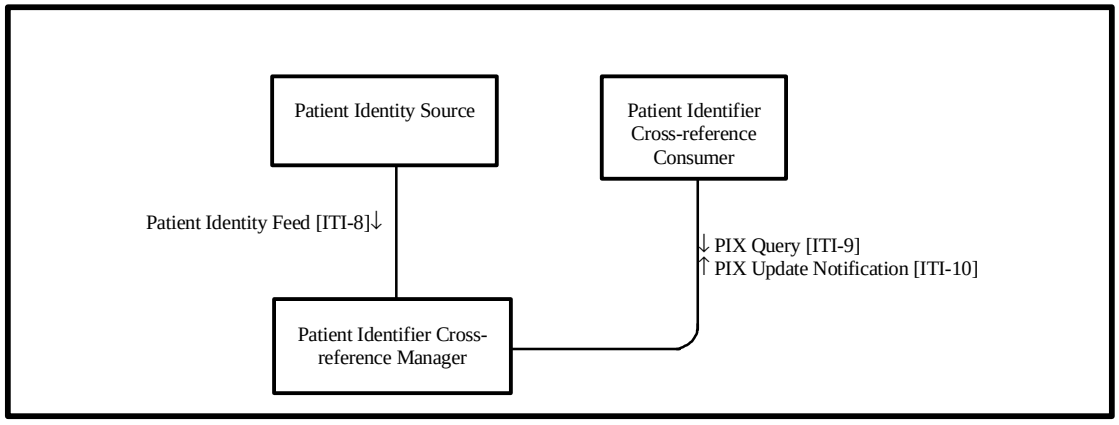


Figure 5.1-1 Patient Identifier Cross-referencing Actor Diagram

Table 5.1-1 lists the transactions for each actor directly involved in the Patient Identifier Cross-referencing Profile. In order to claim support of this Integration Profile, an implementation must perform the required transactions (labeled “R”). Transactions labeled “O” are optional. A complete list of options defined by this Integration Profile and that implementations may choose to support is listed in the ITI TF-1: 5.2.

Table 5.1-1 Patient Identifier Cross-referencing Integration for MPI Profile - Actors and Transactions

Actors	Transactions	Optionality	Section in Volume 2
Patient Identity Source	Patient Identity Feed[ITI-8]	R	ITI TF-2: 3.8
Patient Identifier Cross-reference Consumer	PIX Query[ITI-9]	R	ITI TF-2: 3.9
	PIX Update Notification[ITI-10]	O	ITI TF-2: 3.10
Patient Identifier Cross-reference Manager	Patient Identity Feed[ITI-8]	R	ITI TF-2: 3.8
	PIX Query[ITI-9]	R	ITI TF-2: 3.9
	PIX Update Notification[ITI-10]	R	ITI TF-2: 3.10

5.2 Patient Identifier Cross-referencing Integration Profile Options

Options that may be selected for this Integration Profile are listed in the Table 5.2-1 along with the Actors to which they apply. Dependencies between options when applicable are specified in notes.

Table 5.2-1 Patient Identifier Cross-referencing - Actors and Options

Actor	Options	Vol & Section
Patient Identity Source	No options defined	- -
Patient Identifier Cross-reference Manager	No options defined	- -
Patient Identifier Cross-reference Consumer	PIX Update Notification	ITI TF-2: 3.10

5.3 Patient Identifier Cross-referencing Profile Process Flows

The following sections describe use cases that this profile addresses.

5.3.1 Use Case: Multiple Identifier Domains within a Single Facility/ Enterprise

A clinician in the Intensive Care Unit at General Hospital is reviewing a patient chart on the Intensive Care information system and wishes to review or monitor the patient's glucose level, which is included in a laboratory report stored in the hospital's main laboratory system. The Intensive Care system needs to map its own patient ID, which it generates internally, to the patient's medical record number (MRN), which is generated from the hospital's main ADT system and is used as the patient identity by the lab system. In this case the Intensive Care system is essentially in a different identifier domain than the rest of the hospital since it has its own notion of patient identity.

In this scenario, the hospital's main ADT system (acting as a Patient Identity Source) would provide a Patient Identity Feed (using the patient's MRN as the identifier) to the Patient Identifier Cross-reference Manager. Similarly, the Intensive Care system would also provide a Patient Identity Feed to the Patient Identifier Cross-reference Manager using the internally generated patient ID as the patient identifier and providing its own unique identifier domain identifier.

Once the Patient Identifier Cross-reference Manager receives the Patient Identity Feed transactions, it performs its internal logic to determine which, if any, patient identifiers can be "linked together" as being the same patient based on the corroborating information included in the Feed transactions it has received. The cross-referencing process (algorithm, human decisions, etc.) is performed within the Patient Identifier Cross-reference Manager and is outside the scope of IHE. (See ITI TF-2: 3.9.4.2.2.6 for a more complete description of the scope of the cross-referencing logic boundary).

The Intensive Care system wants to get lab information associated with a patient that the Intensive Care system knows as patient ID = 'MC-123'. It requests the lab report from the lab system using its own patient ID (MC-123) including the domain identifier/ assigning authority. Upon receipt of the request, the lab system determines that the request is for a patient outside of its own identifier domain (ADT Domain). It requests a list of patient ID aliases corresponding to patient ID = 'MC-123' (within the "Intensive Care domain") from the Patient Identifier Cross-reference Manager. Having linked this patient with a patient known by medical record number = '007' in the 'ADT Domain', the Patient Identifier Cross-reference Manger returns this list to the lab system so that it may retrieve the lab report for the desired patient and return it to the Intensive Care system. Figure 5.3-1 illustrates this process flow.

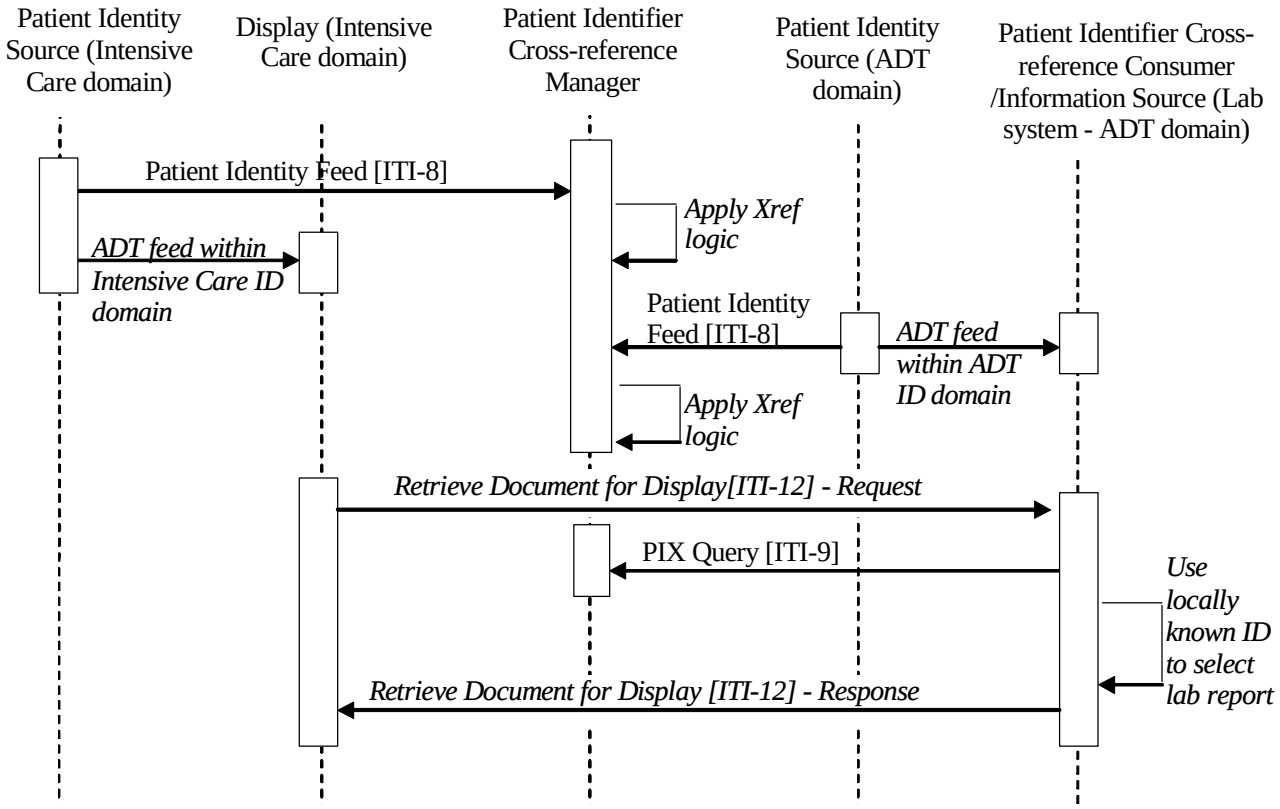


Figure 5.3-1. Multiple ID Domains in a Single Facility Process Flow in PIX Profile

Note: Request and Response portions of the Retrieve Document for Display transaction are not part of this profile and included for illustration purposes only.

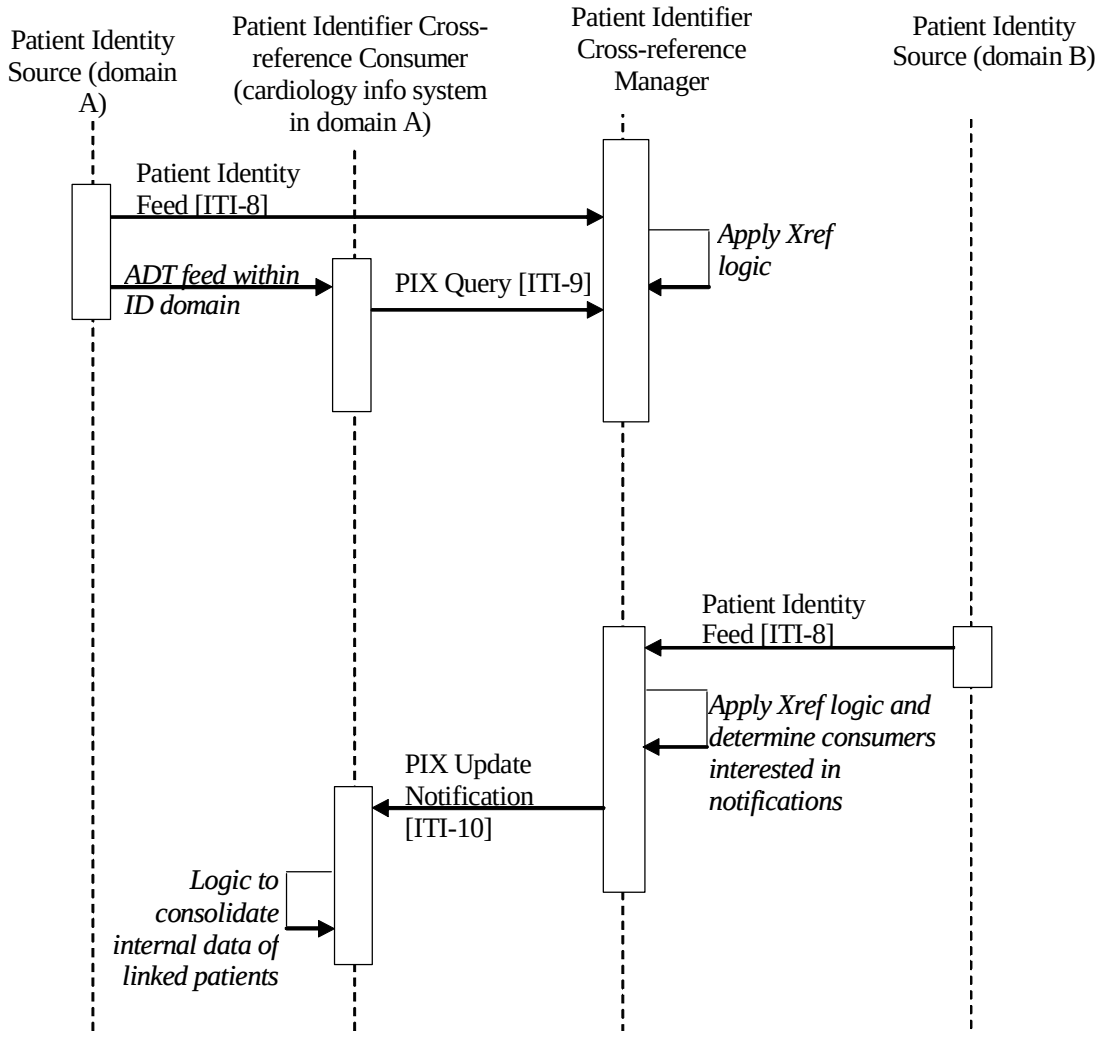
5.3.2 Use Case: Multiple ID Domains Across Cooperating Enterprises

A healthcare enterprise is established by the consolidation of two hospitals, each having its own separate patient registration process run by different hospital information systems. When a patient is treated in one hospital, the access to its electronic records managed by the other hospital is necessary. The following use case illustrates this scenario.

Hospitals A and B have been consolidated and have a single Patient Identifier Cross-reference Manager that maintains the ID links between the two hospitals. Each hospital has a different HIS that is responsible for registering patients, but they have consolidated their cardiology information systems. The cardiology system has been configured with a Patient Identifier Cross-reference Consumer to receive patient identity notifications when cross-referencing activity occurs.

A patient is registered and then has some diagnostic stress tests done at hospital A. The cardiology information system queries the Patient Identifier Cross-reference Manager to get a list of possible ID aliases for the patient to see if any past cardiology reports may be available. No patient ID aliases are found. Some time later the same patient goes to hospital B to have a second diagnostic stress test done. The patient is registered via the HIS in hospital B which then sends that identity information to the Patient Identifier Cross-reference Manager. The Patient Identifier Cross-reference Manager determines this is in fact the same patient as was registered previously at hospital A. The cardiology information system was previously configured with the Patient Identifier Cross-reference Manager to receive notifications, thus a notification is sent to the cardiology system to inform it of the patient identifier aliases. This notification is done to allow systems that are aware of multiple identifier domains to maintain synchronization with patient identifier changes that occur in any of the identifier domains that they are aware of.

Figure 5.3-2 illustrates the process flow for this use case.



995 **Figure 5.3-2 Multiple ID Domains Across Cooperating Enterprises Process Flow in PIX Profile**

Note: PIX Update Notifications are not sent for the first Patient Identity Feed for a patient, since no cross-referencing activity occurred after this first Patient Identity Feed Transaction.

.

1000 5.4 Relationship between the PIX Integration Profile and eMPI

The PIX Integration Profile achieves the integration of disparate Patient Identifier Domains by using a cross-referencing approach between Patient Identifiers associated with the same patient. This section discusses how this approach is compatible with environments that wish to establish master patient identifiers (MPI), or enterprise MPI (eMPI) systems. An eMPI may be considered 1005 a particular variation in implementation of the PIX Integration Profile.

The concept of an MPI is a rather broad concept, yet it is most often associated with the creation of a master patient identifier domain. Such a master domain is considered more broadly

applicable or more "enterprise-level" than the other patient identifier domains it includes. Such a hierarchical inclusion of patient identification domains into a "master patient identification domain" can be considered a particular case of patient cross-reference, where the patient identifiers in the various domains are cross-referenced to the patient identifiers of the master domain. Two possible configurations are depicted by Figure 5.4-1.

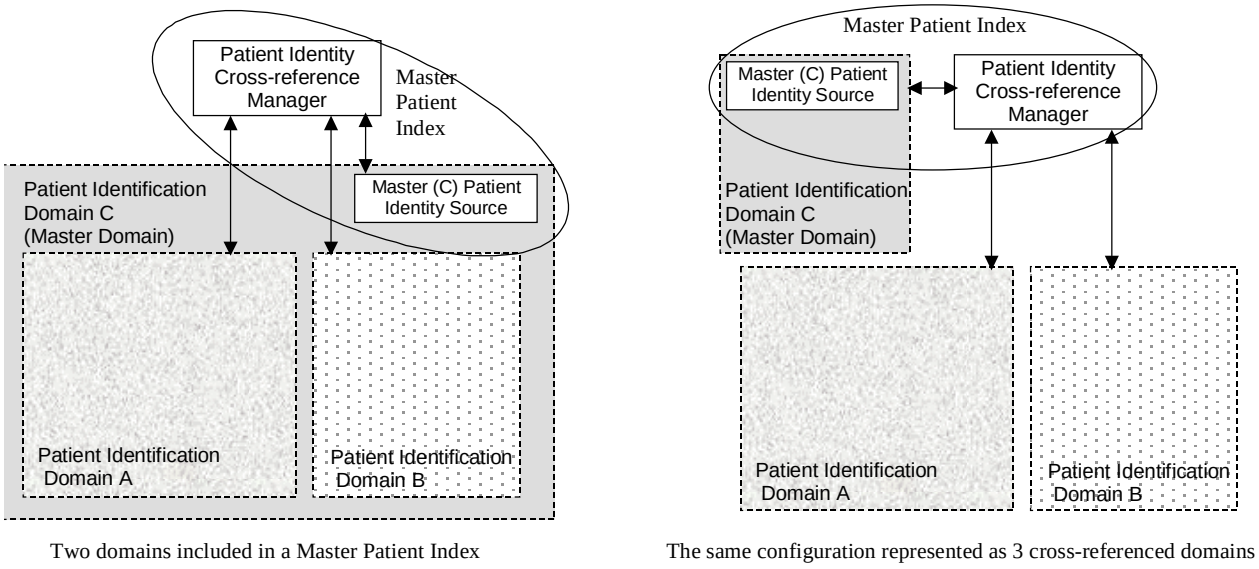


Figure 5.4-1 PIX Profile Relationship to eMPI

Figure 5.4-1 above shows how the Master Patient Identifier Domain (Domain C), in a typical MPI approach, is simply another patient Identification Domain when considered in a Cross-referencing approach. The decision to place enterprise-wide systems such as Clinical Data Repositories into the so-called master domain is simply a configuration choice. In addition, such a configuration sometimes assumes that any system in Patient Domain A not only manages the patient Identifiers of Domain A but is also aware of those of Domain C. In the Patient Identifier Cross-reference Integration Profile, this is a configuration choice where certain systems have been designed and configured to operate across multiple domains. Thus the entity often called an MPI (shown by the oval) is actually the combination of a Patient Identity Source Actor (ADT) along with a Patient Identifier Cross-reference Manager.

The PIX Integration Profile can coexist with environments that have chosen to deploy a distinct MPI, and provides a more scalable approach. Many other configurations can also be deployed, in particular those where the creation of a master domain "including" the other domains is not necessary (i.e., a simple federation of domains where none is actually the master).

6 Patient Synchronized Applications (PSA)

The ***Patient Synchronized Applications Profile (PSA)*** enables single patient selection for the user working in multiple applications on a workstation desktop. With this Integration Profile patient selection in any of the applications causes all other applications to tune to that same patient. This allows a clinician to use the application they are most familiar with to select the patient and have that selection reflected in the other applications they are using follow along.

This profile leverages the HL7 CCOW standard, specifically for patient subject context management. The scope of this profile is for sharing of the CCOW Patient subject only. The IHE PSA profile adds value to the CCOW specification for the patient subject by further constraining the patient identifier to ensure consistency across applications supporting PSA, providing guidance for consistent behavior across applications supporting PSA and ensuring consistent interaction with the Patient Identifier Cross-reference Consumer Actor across the enterprise.

For applications that require user authentication, IHE recommends implementation of the Enterprise User Authentication Profile, as opposed to other means, such as a CCOW Authentication Repository. ITI TF-1: 4 describe the Enterprise User Authentication Profile and the use of the CCOW user subject.

6.1 Actors/ Transactions

Figure 6.1-1 shows the actors directly involved in the Patient Synchronized Applications Integration Profile and the relevant transactions between them. Other actors that may be indirectly involved due to their participation in other profiles are not shown.

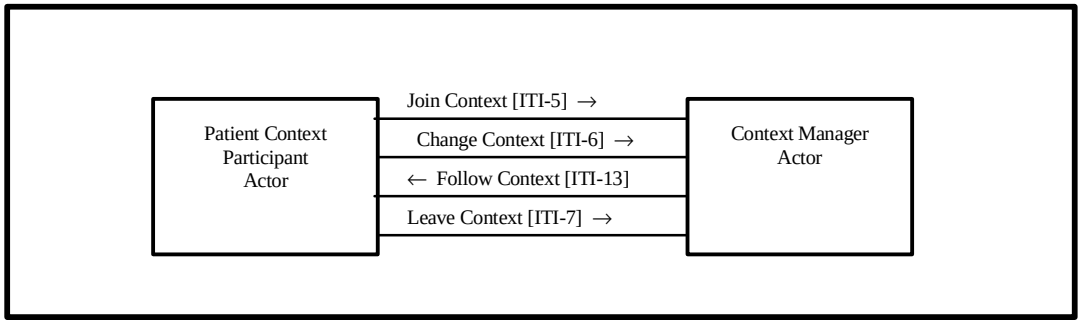


Figure 6.1-1 Patient Synchronized Applications Profile Actor Diagram

Table 6.1-1 lists the transactions for each actor directly involved in the PSA Profile. In order to claim support of this Integration Profile, an implementation must perform the required transactions (labeled “R”).

The Patient Context Participant Actor shall support all four transactions identified in Figure 6.1-1 as defined in ITI TF-2. The Patient Context Participant Actor shall respond to all patient context changes. This actor shall set the patient context provided the application has patient selection capability.

The IHE Context Manager Actor may encompass more than a CCOW context manager function. It may include a number of other components such as the context management registry and patient mapping agent.

The Context Manager Actor may be grouped with a Patient Identifier Cross-referencing (PIX) Consumer Actor of the Patient Identity Cross-referencing Profile; see ITI TF-2: Appendix D for a description of the additional responsibilities placed on the Context Manager Actor in this case.

Table 6.1-1 Patient Synchronized Applications Integration Profile - Actors and Transactions

Actors	Transactions	Optionality	Section
Patient Context Participant	Join Context [ITI-5]	R	ITI TF-2: 3.5
	Change Context [ITI-6]	R	ITI TF-2: 3.6
	Leave Context [ITI-7]	R	ITI TF-2: 3.7
	Follow Context [ITI-13]	R	ITI TF-2: 3.13
Context Manager	Join Context [ITI-5]	R	ITI TF-2: 3.5
	Change Context [ITI-6]	R	ITI TF-2: 3.6
	Leave Context [ITI-7]	R	ITI TF-2: 3.7
	Follow Context [ITI-13]	R	ITI TF-2: 3.13

6.2 Patient Synchronized Applications Integration Profile Options

Options that may be selected for this Integration Profile are listed in Table 6.2-1 along with the actors to which they apply. Dependencies between options, when applicable, are specified in notes.

Table 6.2-1 Patient Synchronized Applications - Actors and Options

Actor	Options	Vol & Section
Patient Context Participant	*No options defined*	- -
Context Manager	*No options defined*	- -

6.3 Patient Synchronized Applications Integration Profile Process Flows

The Patient Synchronized Applications Integration Profile provides maximum value when a user needs to use more than one application simultaneously. The process flow outlined in Section 6.3.1 depicts a use case where the applications only participate in the PSA profile. The process flow outlined in ITI TF-1: Appendix E illustrates when the PSA and Enterprise User Authentication (EUA) profiles are deployed together.

6.3.1 Use Case: Simple Patient Switching

When the PSA profile is not grouped with EUA profile only the patient identity is passed in context. This use case does not explicitly identify the method of user authentication, as it may

not be required by the application or may be accomplished by other means. In this use case both applications share the same patient identifier domain. The process flow for this use case is:

The clinician launches the clinical data repository application, depicted as Patient Context Participant Actor 1. The clinical data repository application joins the context session for the clinician desktop.

The clinician selects patient A in the clinical data repository application. The clinical data repository application sets the identifier for patient A in context.

The clinician launches a cardiology application, depicted as Patient Context Participant Actor 2. The Cardiology application joins the context session, gets the identifier for patient A from context, and tunes its display to patient A.

The clinician selects patient B in the cardiology application. This action results in the initiation of a Change Context transaction by the cardiology application (Patient Context Participant Actor 2). All non-instigating applications participate via the Follow Context transaction, which results in the selected patient being displayed in the clinical data repository application (Patient Context Participant Actor 1).

The clinician closes the clinical data repository application. The clinical data repository application leaves the context prior to terminating the application.

The clinician closes the cardiology application. The cardiology application leaves the context prior to terminating the application.

Figure 6.3-1 illustrates the process flow for this use case.

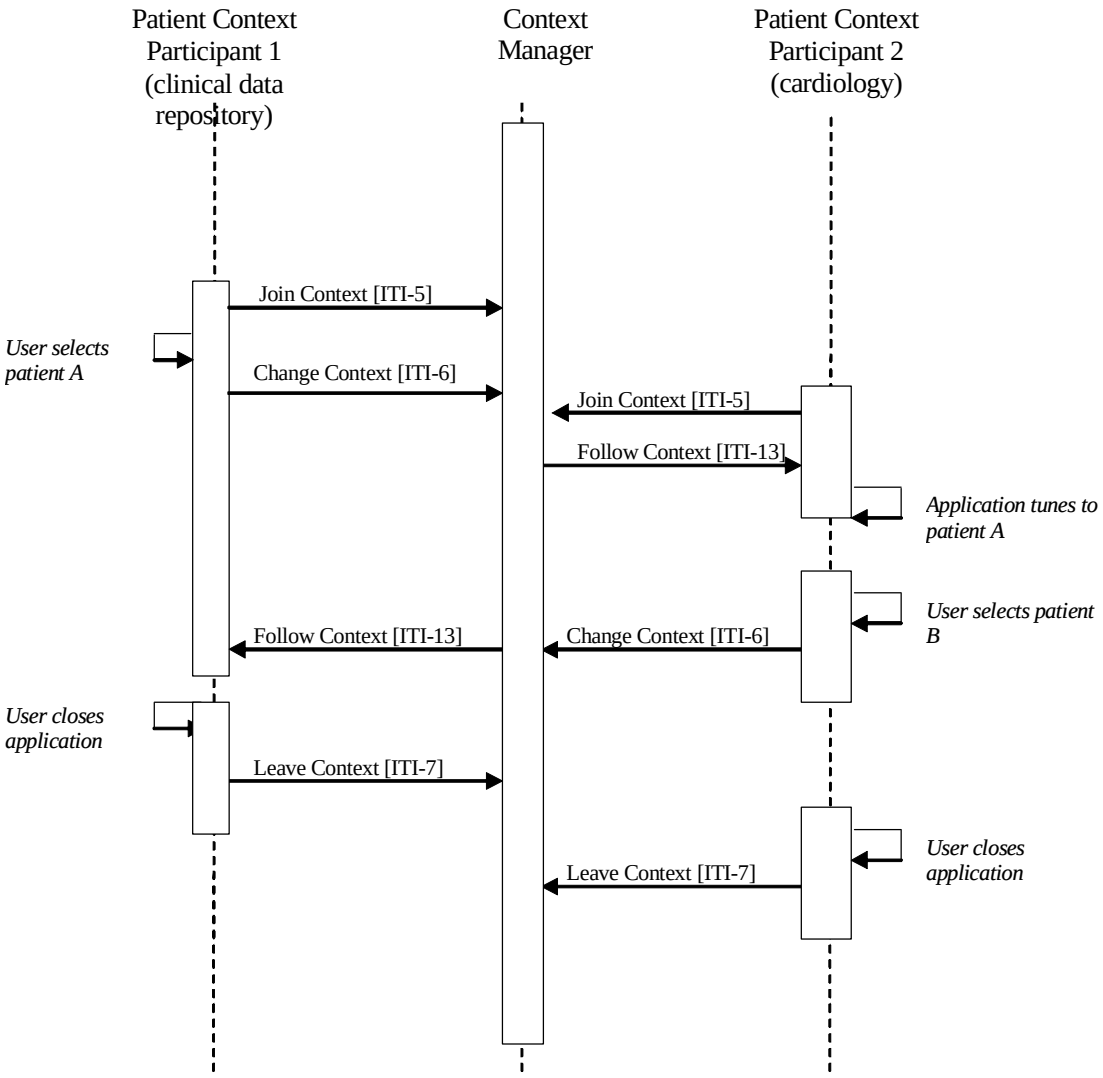


Figure 6.3-1. Simple Patient Switching Process Flow

7 Consistent Time (CT)

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 Consistent Time Integration Profile defines mechanisms to synchronize the time base between multiple actors and computers. Various infrastructure, security, and acquisition profiles require use of a consistent time base on multiple computers. The Consistent Time profile requires the use of the Network Time Protocol (NTP) defined in RFC 1305. When the Time Server is grouped with a Time Client to obtain time from a higher tier Time Server, the Time Client shall utilize NTP. For some Time Clients that are not grouped with a Time Server, SNTP may be usable.

This profile was previously a portion of the Radiology Basic Security Profile, but it has a variety of other infrastructure uses.

Note: This profile corresponds to a portion of the IHE Radiology Technical Framework, Basic Security Profile. It is required by more than just radiology systems. It is needed by several of the profiles in the IHE IT Infrastructure and will also be needed by Cardiology. It is therefore being re-located from IHE Radiology into IHE IT Infrastructure. There are no changes to the requirements, so actors that supported the Radiology Basic Secure Node or Time Server do not need modification. The Maintain Time [RAD TF-3: 4.33] transaction from Radiology and the Maintain Time [ITI TF-2: 3.1] transaction for IT Infrastructure are the same.

7.1 Actors/ Transactions

Figure 7.1-1 shows the actors directly involved in the Consistent Time Profile and the relevant transactions between them. Other actors that may be indirectly involved because of their participation in profiles that require consistent time are not shown.

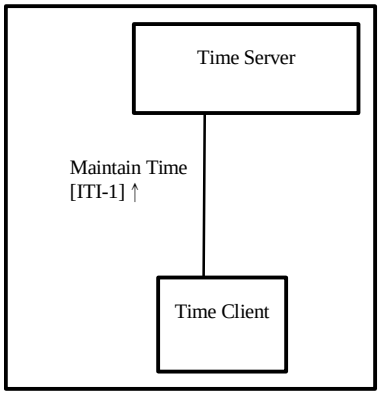


Figure 7.1-1: Consistent Time Profile Actor Diagram

Table 7.1-1 lists the transactions for each actor directly involved in the Consistent Time Integration Profile. In order to claim support of this integration profile, an implementation must perform the required transactions (labeled "R").

Table 7.1-1: Consistent Time - Actors and Transactions

Actors	Transactions	Optionality	Section in Vol. 2
Time Server	Maintain Time [ITI-1]	R	ITI TF-2: 7.1
Time Client	Maintain Time [ITI-1]	R	ITI TF-2: 7.1

7.2 Consistent Time Integration Options

Options that may be selected for this integration profile are listed in the Table 7.2-1 along with the actors to which they apply.

Table 7.2-1: Consistent Time - Actors and Options

Actor	Options	Vol & Section
Time Server	*Secured NTP*	ITI TF-2: 3.1.4-1
Time Client	*SNTP, Secured NTP*	ITI TF-2: 3.1.4-1

7.3 Consistent Time Process Flow

This section describes the typical flow related to the Consistent Time Profile. In the process flow diagram 7.3-1, the Time Client B and Time Server B have been grouped. When a Client and Server are grouped they utilize internal communications mechanisms to synchronize their time.

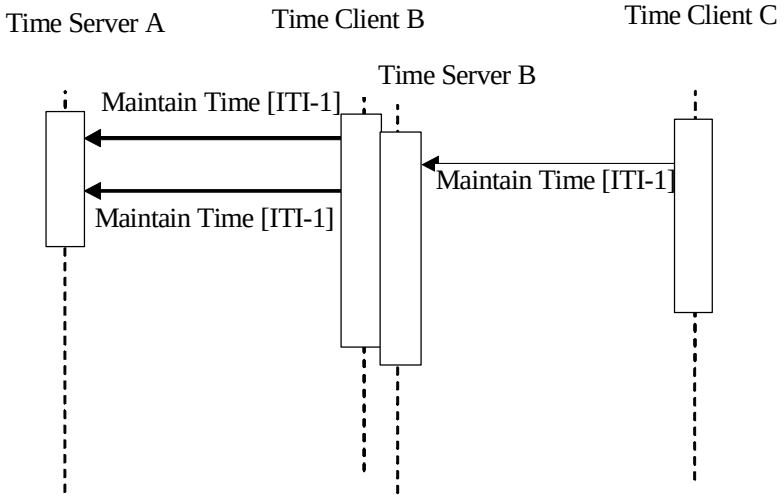


Figure 7.3-1 Basic Process Flow in Consistent Time Profile

The Time Client B maintains time synchronization with the Time Server A. The Time Server B is internally synchronized with Time Client B. The Time Client C maintains time synchronization with Time Server B.

The NTP protocol has been designed to provide network time services for synchronization with this kind of cascaded synchronization. The achievable accuracy is dependent on specific details of network hardware and topology, and on details of computer hardware and software implementation. The Time Server and Time Client are grouped to provide synchronization cascading and reduce network traffic.

8 Patient Demographics Query (PDQ)

8.1 Actors/ Transactions

Figure 8.1-1 shows the actors directly involved in the Patient Demographics Query Integration Profile and the relevant transactions between them. Other actors that may be indirectly involved due to their participation in Patient ID Cross-referencing, etc. are not necessarily shown.

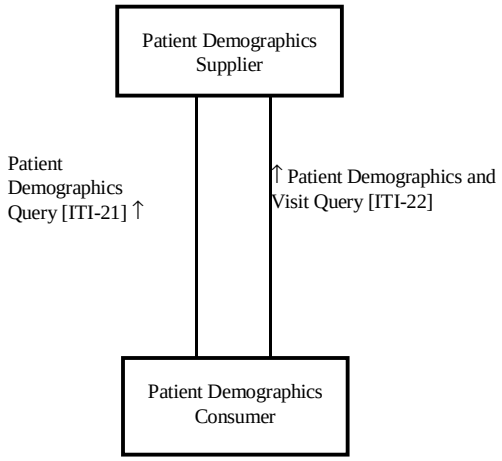


Figure 8.1-1. Patient Demographics Query Profile Actor Diagram

Table 8.1-1 lists the transactions for each actor directly involved in the Patient Demographics Query Profile. In order to claim support of this Integration Profile, an implementation must perform the required transactions (labeled "R"). Transactions labeled "O" are optional. A complete list of options defined by this Integration Profile and that implementations may choose to support is listed in Volume I, Section 8.2.

Table 8.1-1. Patient Demographics Query Integration Profile - Actors and Transactions

Actors	Transactions	Optionality	Section in Vol. 2
Patient Demographics Consumer	Patient Demographics Query	R	ITI TF-2: 3.21
	Patient Demographics and Visit Query	O	ITI TF-2: 3.22
Patient Demographics Supplier	Patient Demographics Query	R	ITI TF-2: 3.21
	Patient Demographics and Visit Query	O	ITI TF-2: 3.22

8.2 Patient Demographics Query Integration Profile Options

Options that may be selected for this Integration Profile are listed in the table 8.2-1 along with the actors to which they apply. Dependencies between options when applicable are specified in notes.

Table 8.2-1 Patient Demographics Query - Actors and Options

Actor	Options	Vol & Section
Patient Demographics Consumer	Patient Demographics and Visit Query	ITI TF-2: 3.22
Patient Demographics Supplier	Patient Demographics and Visit Query	ITI TF-2: 3.22

8.3 Patient Demographics Query Process Flow

The Patient Demographics Supplier performs the following functions.

- It receives patient registration and update messages from other systems in the enterprise (*e.g.,* ADT Patient Registration systems), which may or may not represent different Patient ID Domains. The method in which the Patient Demographics Supplier obtains the updated patient demographic information is not addressed by this profile.
- It responds to queries for information.

Specific methods for acquiring demographic information are beyond the scope of this Profile. It is a prerequisite that the Patient Demographics Supplier possess current demographic information. One method by which current demographic information may be obtained is for the Patient Demographic Supplier to be grouped with another IHE actor, such as Order Filler, that either maintains or receives such information.

In all cases, the Patient Demographics Supplier receives a Patient Demographics Query or Patient Demographics and Visit Query request from the Patient Demographics Consumer, and returns demographics (and, where appropriate, visit) information from the single domain that is associated with the application to which the query message is sent. Identifier information may be returned from multiple or single domains; see the "Using Patient Data Query (PDQ) in a Multi-Domain Environment" section (ITI TF-2: Appendix M) for a discussion of the architectural issues involved.

Use Case 1: Patient Information Entering at Bedside

An admitted patient is assigned to a bed. The patient may or may not be able to provide positive ID information. The nurse needs to enter patient identity information into some bedside equipment to establish the relationship of the assigned bed to the patient. The equipment issues a query for a patient pick list to a patient demographics supplier that provides data for a patient pick list. Search criteria entered by the nurse might include one or more of the following:

- Partial or complete patient name (printed on the patient record or told by the patient)

- Patient ID (this may be obtained from printed barcode, a bed-side chart, etc.)
- Partial ID entry or scan.
- Date of birth / age range
- Bed ID

The system returns a list of patients showing the MRN, full name, age, sex, room/bed, and admit date, and displays the list to the nurse. The nurse then selects the appropriate record to enter the patient identity information into the bedside equipment application.

Use Case 2: Patient Identity Information Entering in Physician Offices

A patient visits a physician office for the first time. The nurse needs to register the patient; in doing so, it is desired to record the patient's demographic data in the practice management information system (PMIS). The physician office is connected to a hospital enterprise's central patient registry. The nurse issues a patient query request to the central patient registry, with some basic patient demographics data as search criteria. In the returned patient list, she picks up an appropriate record for the patient, including the hospital's patient ID, to enter into the PMIS. (Note that the PMIS uses a different Patient ID domain than that of the central patient registry.)

The PMIS uses its own patient identifier, coordinating this identifier with the patient identifier returned in the pick list (sharing the hospital's Patient ID Domain) to retrieve information from the hospital's clinical repository.

Use Case 3: Patient Demographics Query in an Enterprise with Multiple Patient ID Domains

A lab technician enters some basic demographics data (*e.g.*, patient name) into a lab application to query a patient demographics supplier to identify a patient for his lab exams. As the application also needs the patient identifier in another Patient ID Domain in the enterprise for results delivery, the application is configured to receive patient IDs from other domains in the query response.

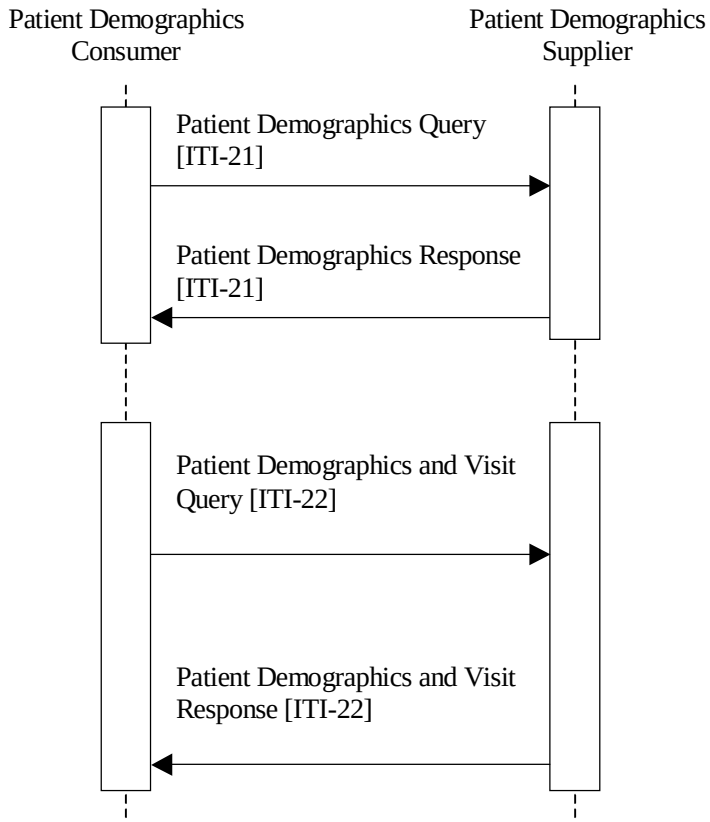


Figure 8.2-1. Basic Process Flow in Patient Demographics Query Profile

8.3.1 Combined Use of PDQ with Other IHE Workflow Profiles

1235 When the Patient Demographics Supplier Actor is grouped with actors in other IHE profiles that perform patient information reconciliation activities (*e.g.*, Radiology PIR), the PDQ Supplier Actor may use the updated information to respond to PDQ Queries. In addition, the Patient Demographics Query Profile may play an integral workflow role in conjunction with other IHE Profiles.

1240 8.3.2 Supplier Data Configuration

A Patient Demographics Supplier Actor that holds demographic information for a single Patient ID domain shall provide matches in that domain.

In the case where the Patient Demographics Supplier Actor holds demographic information for multiple Patient ID domains, the Patient Demographics Supplier Actor shall return information
1245 for the domain associated with *MSH-5-Receiving Application* and *MSH-6-Receiving Facility*. See the "Using Patient Data Query (PDQ) in a Multi-Domain Environment" section (ITI TF-2: Appendix M) for a further discussion of this case and an illustration of the supporting architecture.

1250

9 Audit Trail and Node Authentication (ATNA)

The Audit Trail and Node Authentication (ATNA) Integration Profile establishes security measures which, together with the Security Policy and Procedures of the enterprise, provide patient information confidentiality, data integrity and user accountability. The goals of the Audit Trail and Node Authentication Integration Profile are:

- User Accountability (Audit Trail).

  To allow a security officer in an institution to audit activities, to assess compliance with a secure domain's policies, to detect instances of non-compliant behavior, and to facilitate detection of improper creation, access, modification and deletion of Protected Health Information (PHI). PHI is considered to be the patient-identifiable information records (e.g. Registration, Order, Study/Procedure, Reports, Images, and Presentation States). It may be accessed by users or exchanged between the systems. This includes information exported to and imported from every secured node in the secure domain.

  The audit trail contains information so that questions can be answered such as:

  - For some user: which patients' PHI was accessed?
  - For some patient PHI: which users accessed it?
  - What user authentication failures were reported?
  - What node authentication failures were reported?

- Access Control

  ATNA contributes to access control by limiting network access between nodes and limiting access to each node to authorized users. Network communications between secure nodes in a secure domain are restricted to only other secure nodes in that domain. Secure nodes limit access to authorized users as specified by the local authentication and access control policy.

- Centralized Audit Record Repository

  Provides a central Audit Record repository as the simplest means to implement security requirements. An immediate transfer of Audit Records from all the IHE actors to the Audit Record Repository is required when possible, reducing the opportunities for tampering and making it easier to audit the department, but disconnected nodes may store audit data for transfer to the Audit Repository upon reconnection to the secure domain network.

- PHI Data Integrity

  To allow tracking of the life of PHI information (creation, modification, deletion and location) and its data integrity during this process.

Key Features of ATNA

The key features of the Audit Trail and Node Authentication Integration Profile are the following:

- Authentication of the user. For this profile the user authentication may utilize any technology. IHE does not restrict or describe the user authentication technology to be used for the ATNA profile.
- Audit record generation. This profile requires that events concerning PHI use are recorded and transmitted to a repository where they can be monitored to detect indications of inappropriate activity.
- Authentication of the node during communications. This profile requires that the nodes are authorized and authenticated nodes for all data communications transferring PHI. It does not convey user identification. By using the user authentication and access control selected for each node, user accountability can be assured.

ATNA Security Assumptions

The underlying assumptions are:

- All systems that are members of the secure domain implement a Secure Node Actor for the ATNA profile. The ATNA profile defines transactions between the secure nodes to create a secure domain that is under the management of a domain security officer.
- All applications on a secure node will comply with ATNA requirements, regardless of whether they are IHE Actors or not. They apply to all IT assisted activities that directly create, access, update, and delete PHI, not only those specified by IHE and performed by IHE actors.
- IHE addresses only those security requirements related to systems within the scope of IHE healthcare applications. It does not address other security requirements such as defending against network attacks, virus infection, etc. The principal objective of the Audit Trail mechanism is to track data access to PHI, not IHE transactions.
- IHE does not mandate the use of encryption during transmission. Most hospital networks provide adequate security through physical and procedural mechanisms. The additional performance penalty for encryption is generally not justified for these networks. This profile mandates the use of the TLS security negotiation mechanism for all communications between secure nodes as a means of ensuring that they only communicate with other authorized secure nodes. It permits the negotiation of encryption if both nodes are configured to request and support encryption. This allows installation of IHE secure nodes into environments where the network is not otherwise secured.
- The Audit Trail and Node Authentication Integration Profile requires only local user authentication. The profile allows each secure node to use the access control technology of its choice to authenticate users. The use of Enterprise User Authentication is one such choice, but it is not necessary to use this profile.

- Mobile equipment can participate in the Audit Trail and Node Authentication Integration Profile, but special issues related to mobile equipment are not explicitly addressed in this profile.
- The Audit Trail and Node Authentication Profile provides tools that are useful for enterprises attempting to become compliant with privacy and security regulations (HIPAA, European, Japanese, etc.), but the profile does not itself make the enterprise compliant.
- ATNA assumes that physical access control, personnel policies and other organizational security considerations necessary to make an enterprise compliant with security and privacy regulations are in place.

9.1 Connection Authentication

The Audit Trail and Node Authentication Integration Profile requires the use of bi-directional certificate-based node authentication for connections to and from each node. The DICOM, HL7, and HTML protocols all have certificate-based authentication mechanisms defined. These authenticate the nodes, rather than the user. Connections to these machines that are not bi-directionally node-authenticated shall either be prohibited, or be designed and verified to prevent access to PHI.

Note: Communications protocols that are not specified by IHE profiles, e.g. SQL Server, must be bi-directionally authenticated if they will be used for PHI. This profiles does not specify how that authentication is to be performed.

This requirement can also be met by ensuring complete physical network security with strict configuration management. This means that no untrusted machine can obtain physical access to any portion of the network. Making the connection authentication configurable enhances performance in physically secured networks. A Secure Node Actor shall be configurable to support both connection authentication and physically secured networks.

9.2 Audit Trails

9.2.1 Audit Messages

The use of auditing as part of a security and privacy process is appropriate for situations where the people involved are generally trustworthy and need a wide range of flexibility to respond rapidly to changing situations. This is the typical healthcare provider environment. Auditing tracks what takes place, and the people involved know that their actions are being audited. This means that the audit records must capture event descriptions for the entire process, not just for individual components that correspond to individual IHE actors.

The IHE audit trail is the first of several profiles that correspond to different forms of access control and authentication. Auditing is always needed independent of the access control and authentication method chosen.

The IHE-specified audit flow is illustrated in Figure 9.2-1.

1. Real world activities take place, and some of these activities involve the applications processing of a device that includes support for some IHE profiles. This product has components that may correspond to specific IHE Actors. The product may also have other capabilities that are independent of IHE recommendations.

2. A wide variety of events take place during this process. Some of these events are directly related to IHE Actor activities. Others may be indirectly related, and still others are not related to any IHE specification. The events are both extremely detailed minor events, such as keystrokes, and high level events such as analyzing a diagnostic study. Very few of these events are relevant to security and privacy auditing. Most are too low level to be useful or are otherwise irrelevant.

3. The "Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications" (RFC-3381) defines an XML schema for reporting events that are relevant to security and privacy auditing. It was defined in cooperation with the ASTM, HL7, and DICOM standards organizations and the NEMA/COCIR/JIRA Security and Privacy Committee. The IHE recommends the use of the RFC-3381 format, and recommends reporting only events that it can describe.

    a) DICOM has standardized some of the audit message vocabulary. The DICOM Audit Message Vocabulary extends the basic vocabulary provided with RFC-3381, and also further specifies some optional elements in RFC-3381. An example of vocabulary extension is the addition of a coded value to indicate that a field contains a DICOM Study Instance UID. An example of optional element specification is the requirement that the UserID field in RFC-3381 messages shall be the user ID used by the local device operating system, and that the AlternateID shall be the user ID used by the enterprise authentication system (if it is different).

    b) This profile defines other events that do not correspond to events defined in the DICOM vocabulary. These events are describable by RFC-3381, and this profile includes requirements for such descriptions.

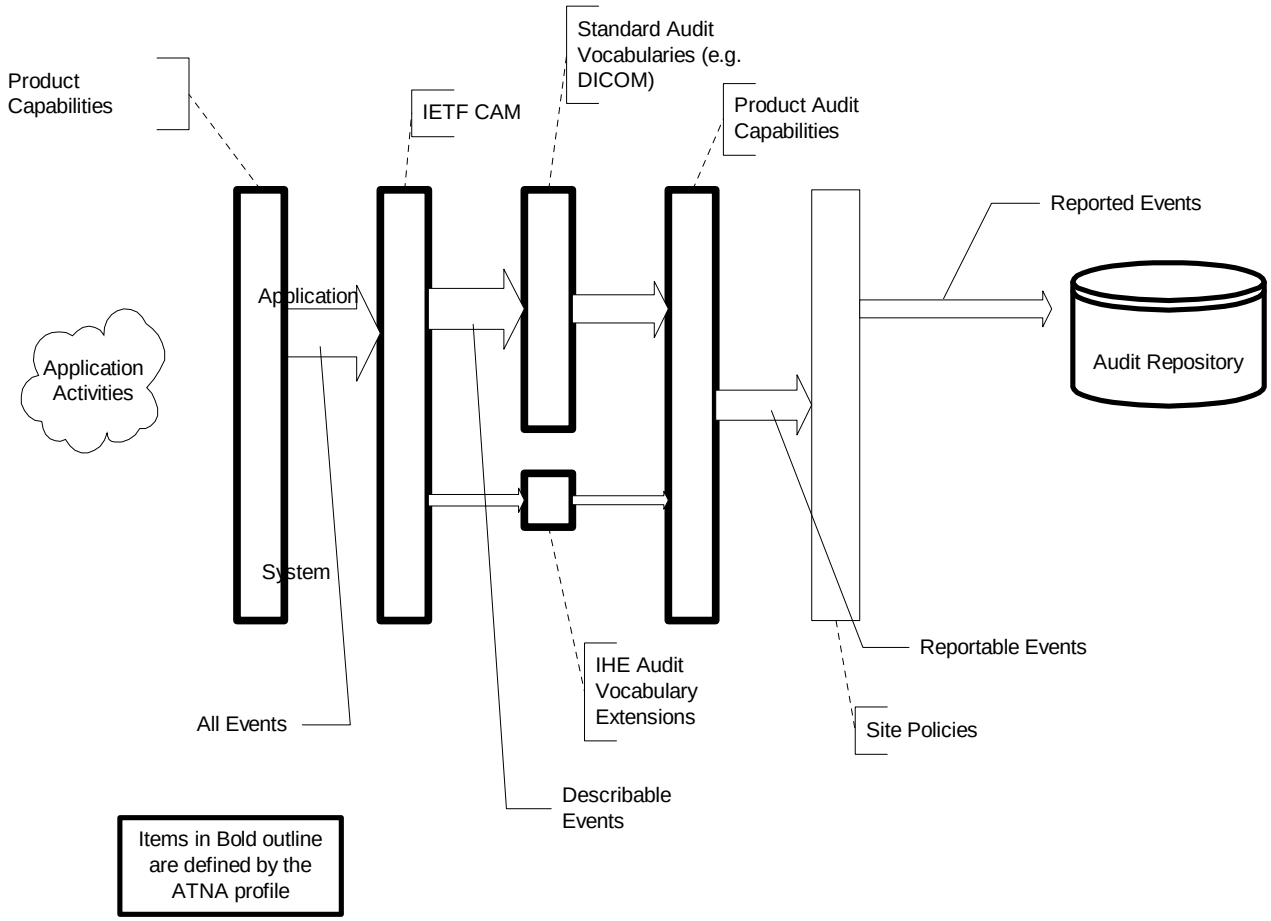
    IHE auditing specifies that when using the RFC-3381, events that can be described using the DICOM vocabulary they shall be reported using the DICOM vocabulary, even if the device is not otherwise a DICOM compliant device. Events that do not match the DICOM vocabulary shall be reported using RFC-3381 vocabulary or other extensions. Events that cannot be reported using RFC-3381 are not candidates for reporting.

4. The local site will then apply its own reporting policies. The IHE profile specifies the capabilities that should be present for audit reporting, and also that there should be controls present to allow the local site security administration to control

reporting detail. The IHE profile does not specify any audit reporting functions or formats.

5. IHE specifies events that must be reported in the audit trail. There are other events related to security, which may be reported in the audit trail or by other means. This profile does not describe them and does not require that they use this reporting format or mechanism. Examples of such events are network routing and firewall logs.

Figure 9.2-1 Flow of Events into Audit Messages



9.2.2 Backwards Compatibility

This profile also defines the continued use of messages that are formatted in accordance with the IHE Provisional Audit Message format from the deprecated Basic Security Profile in IHE Radiology TF 6.0. This older format describes events that are suitable for reporting in Radiology

and other diagnostic and treatment activities. These events are a subset of the kind of events that can be described using RFC-3381 and the DICOM vocabulary.

The IHE ATNA Profile also allows for the reporting of these events using the Provisional format over either of the IHE specified transport mechanisms. The intention is that products will gradually transition from the Provisional message format to RFC-3381 format, but it is recognized that this transition will take time and that there is a significant installed base.

The Provisional format is unlikely to be of interest to other healthcare applications, which should use the RFC-3381 format and DICOM Vocabulary where appropriate.

9.3 Audit Trail Transport

The Audit Trail and Node Authentication Integration Profile specifies the use of Reliable Syslog Cooked Profile (RFC-3195, Section 4) as the mechanism for logging audit record messages to the central audit record repository. It also permits the use of BSD Syslog (RFC-3164). There are, however, several known limitations of BSD Syslog:

- There is no confirmation to the sender that the audit record message was received at the destination
- There is no option to encrypt the audit record messages
- Authentication by means of certificates of the sending nodes and the central audit repository is not possible
- Messages may be truncated or lost.

The specification of Reliable Syslog Cooked Profile messages corrects these deficiencies.

9.4 Actors/Transactions

Table 9.4-1 lists the transactions for each actor directly involved in the Audit Trail and Node Authentication Integration Profile. In order to claim support of this Integration Profile, an implementation must perform the required transactions (labeled “R”). Transactions labeled “O” are optional. A complete list of options defined by this Integration Profile that implementations may choose to support is listed in ITI-TF 1: 9.4. Their relationship is shown in Figure 9.4-1.

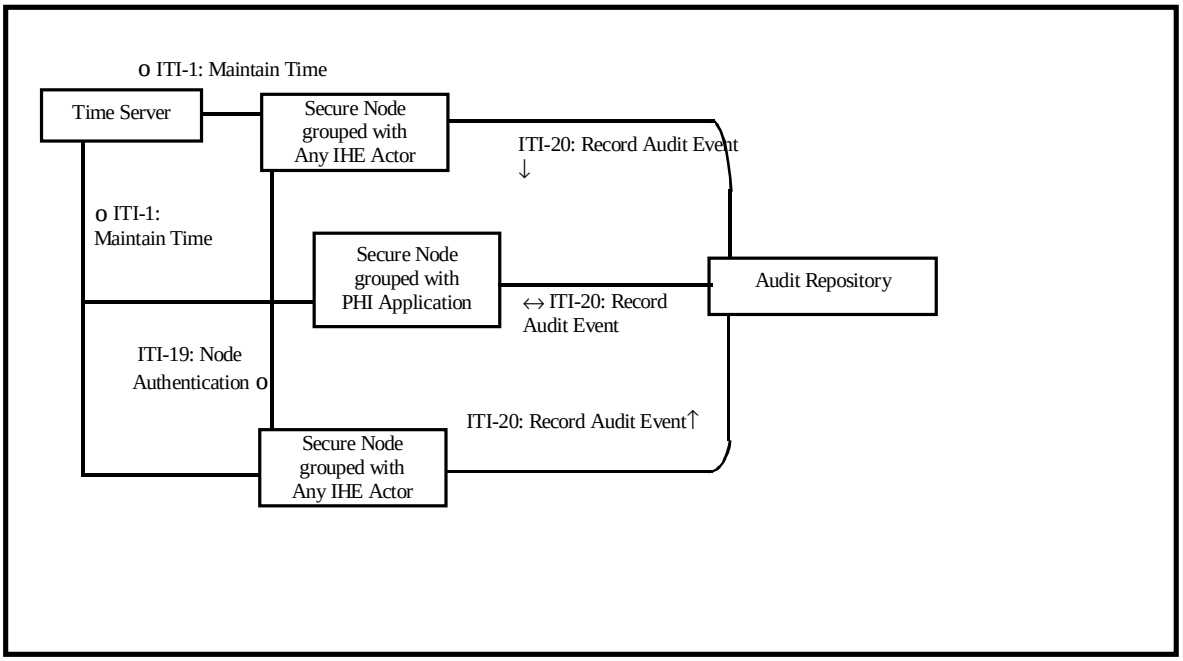


Figure 9.4-1. Audit Trail and Node Authentication Diagram

When an implementation chooses to support this Integration Profile for an actor, that actor shall be grouped with the Secure Node actor. It is required that all IHE actors and any other activities in this implementation support the Audit Trail and Node Authentication Integration Profile.

A means must be provided to upload the required certificates to the implementation, e.g. via floppy disk or file transfer via network.

Non-IHE applications that process PHI shall detect and report auditable events, and protect access.

Table 9.4-1. Audit Trail and Node Authentication Integration Profile - Actors and Transactions

Actor	Transactions	Optionality	Vol II / III Section
<any PHI application grouped with a Secure Node Actor>	Record Audit Event	R	**IHE ITI-2: 3.20**
<any IHE actor grouped with a Secure Node actor>	Record Audit Event	R	**IHE ITI-2: 3.20**
Audit Record Repository	Record Audit Event	R	**IHE ITI-2: 3.20**
Secure Node	Authenticate Node	R	**IHE ITI-2: 3.19**
	Maintain Time	R	**IHE ITI-2: 3.7**

Table 9.4-2 ATNA Extensions in other domain Technical Frameworks

Profile Option	Vol & Section
Radiology Audit Trail Option	RAD TF-1: 2.2.1; TF-2: 5.1

The Secure Node Actor shall include:

1. The Authenticate Node transaction for all network connections that may expose private information. These transactions are defined for:
   a) DICOM, using TLS
   b) HL7, using TLS
   c) HTTP, using TLS
2. All local user activity (login, logout, etc.) protected to ensure only authorized users.
3. An audit transport mechanism, either:
   a) Reliable Syslog Cooked Profile format (RFC-3195, Section 4)
   b) BSD Syslog (RFC-3164), the baseline syslog mechanism.
4. Generation of audit messages for recommended events utilizing one of the defined alternatives for audit message formats. The audit messages formatted are:
   a) The IETF common audit message format, using the DICOM and IHE vocabularies.
   b) The Provisional IHE Audit Message format,

The Audit Repository shall support:

1. Both audit transport mechanisms.
2. Any IHE-specified audit message format, when sent over one of those transport mechanisms. Note that new applications domains may have their own extended vocabularies in addition to the DICOM and IHE vocabularies. This also means that an ATNA Audit Repository is also automatically a Radiology Basic Security profile Audit Repository because it must support the IHE Provisional Message format and it must support the BSD syslog protocol.
3. Self protections and user access controls.

This profile does not specify other functions for the Audit Repository, but it is expected that most repositories will perform screening, reporting, archival, etc.

9.5 Encryption Option

Secure Nodes may implement the ATNA Encryption Option. This option specifies the support of encryption to protect confidentiality.

9.6 Audit Trail and Node Authentication Process Flow

The security measures in the Audit Trail and Node Authentication Integration Profile are user authentication, node authentication, and generation of audit records. Node authentication and user authentication define a number of transactions that establish the concept of a Secure Node and a collection of connected Secure Nodes in a secure domain (see Volume ITI-III: Appendix A).

Generation of audit records requires a set of audit trigger events and a definition of the content of the audit records. This profile specifies two acceptable message formats:

1. Messages formatted in accordance with the IHE Audit Message format. This is a combination of the DICOM Audit Messages format and IHE extensions. The IHE extensions to RFC-3381 add event codes and information needed for uses that are not within the domain of the DICOM Standard.
2. The predecessor IHE Provisional Audit Message format. This format was defined as an interim format while the standards work to define the Common Audit Message format and vocabularies progressed through the standards organizations.

Based on the work done in ASTM (E2147-01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems) and HL7 (Framework for Audit Messages), IHE defined a detailed set of audit trigger events, a set of general audit messages with the content for the audit record, and a mapping for each event to a general audit message. The content of the audit record has been specified by means of an XML Schema (see Volume ITI-II: Appendix F).

In the following paragraphs three typical process flows are described for situations in which authorized users, unauthorized users, and unauthorized nodes attempt to gain access to protected health information (PHI).

9.6.1 Normal Node Process Flow

The following scenario shows how the IHE security measures operate for authorized access to PHI from an authorized node in the network:

1. Time synchronization occurs independently. These transactions may take place at any time. Correct time is needed to generate Audit Records with a correct timestamp.
2. A user logs on to Image Display/Secure Node actor.
   The user enters valid credentials and is authorized to access the node.
3. The node generates audit records.
4. The user wants to query/retrieve and view some images.
   Before image transactions can take place, an authentication process between the Image

Display/Secure Node actor and the Image Manager/Image Archive/Secure Node actor takes place.

5. Following node authentication, the node initiates the query/retrieve transactions.
6. The node generates audit records.

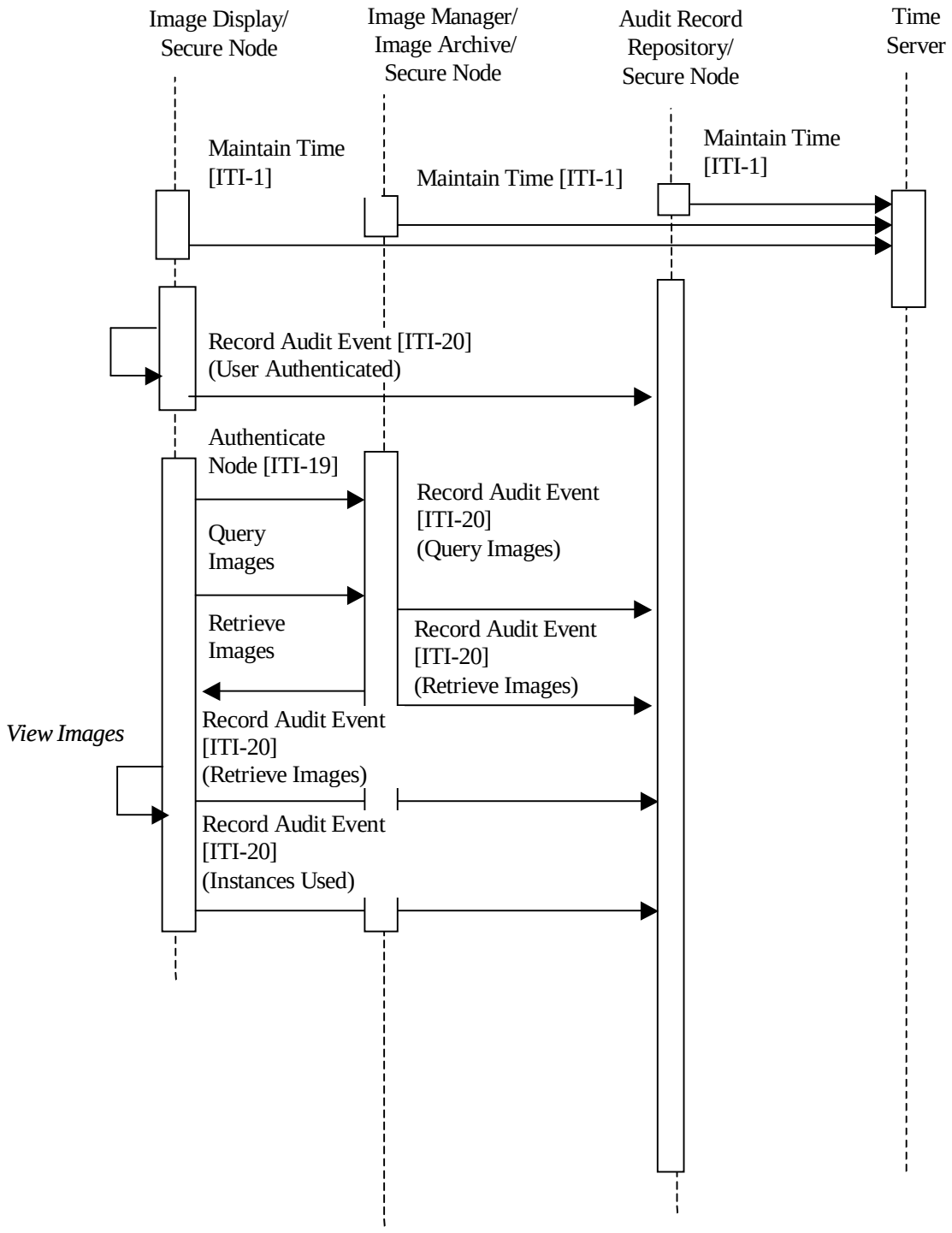


Figure 9.6-1. Authorized Node Process Flow

9.6.2 Unauthorized Node Process Flow

The following scenario shows how the IHE security measures help to prevent unauthorized access to PHI from an unauthorized node in the network:

1. An unauthorized node tries to query the Lab Automation Manager/Secure Node actor for information. This fails because no authentication has taken place, and an audit record is generated.

2. The unauthorized node tries an authentication process with the Lab Automation Manager/Secure Node. This fails because the Lab Automation Manager/Secure Node will not trust the certificate presented by the Malicious Node, and an audit record is generated.

Note that the sequencing of the transactions is just one example; transactions from an unauthorized node are totally unpredictable and may happen in any order.

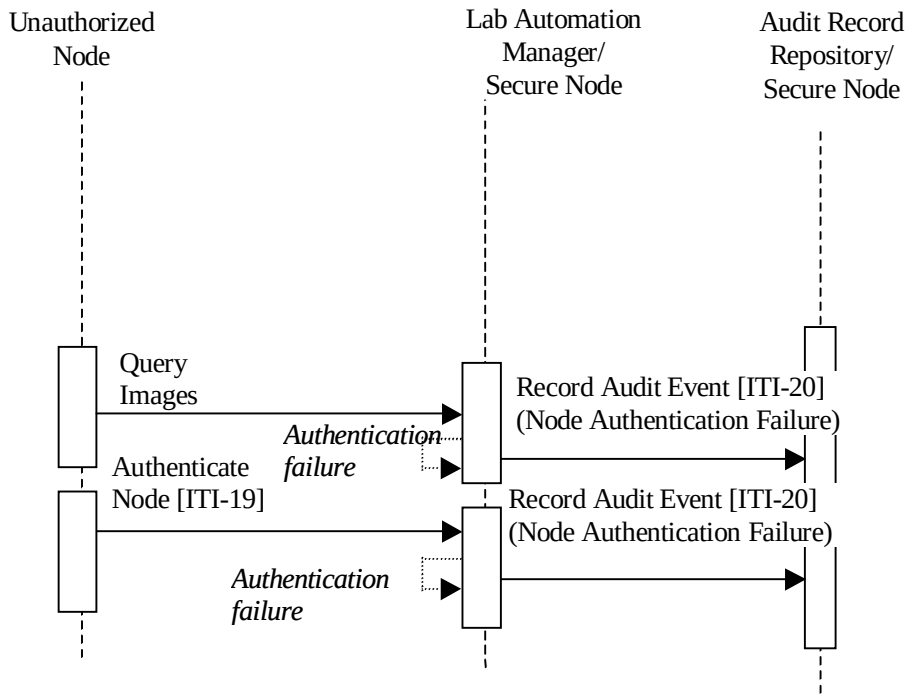


Figure 9.6-2. Unauthorized Node Process Flow

9.6.3 Unauthorized User Process Flow

The following scenario shows how the IHE security measures help to prevent unauthorized access to PHI from an unauthorized user in the healthcare enterprise:

1. An unauthorized user tries an authentication process with the ECG Display/Secure Node actor. This fails because the ECG Display/Secure Node actor detects that the user name and credentials presented are not valid at this secure node, and an audit record is generated.

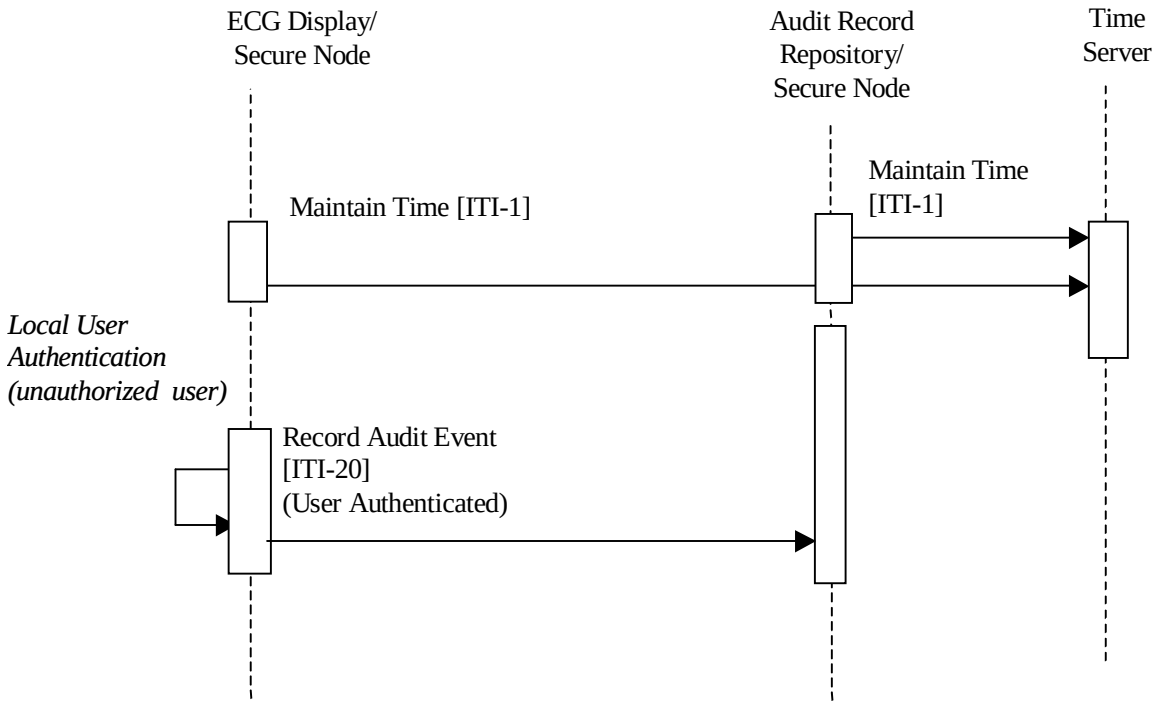


Figure 9.6-3. Unauthorized User Process Flow

10 Cross-Enterprise Document Sharing (XDS)

The ***Cross-Enterprise Document Sharing*** IHE Integration Profile facilitates the registration, distribution and access across health enterprises of patient electronic health records. Cross-Enterprise Document Sharing (XDS) is focused on providing a standards-based specification for managing the sharing of documents between any healthcare enterprise, ranging from a private physician office to a clinic to an acute care in-patient facility.

The XDS IHE Integration Profile assumes that these enterprises belong to one or more clinical affinity domains. A clinical affinity domain is a group of healthcare enterprises that have agreed to work together using a common set of policies and share a common infrastructure.

Examples of affinity domains include:

- Community of Care supported by a regional health information organizations 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 a clinical 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 clinical 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 clinical 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 clinical 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 clinical 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, CCR, CEN ENV 13606, DICOM SR). In order to ensure the necessary interoperability between the document sources and the document consumers, the Clinical Affinity Domain must adopt policies concerning document format, structure and content.

The XDS Integration Profile is not intended to address all cross-enterprise EHR communication needs. Some scenarios may require the use of other IHE Integration profiles, such as Patient Identifier Cross-Referencing, Audit Trail and Node Authentication, Cross-Enterprise User Authentication, and Retrieve Information for Display. 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:

1. The management of dynamic information such as allergy lists, medication lists, problem lists, etc is not addressed by XDS. However, the Retrieve Information for Display Integration Profile does provide some transactions (e.g., LIST-ALLERGIES, LIST-MEDS) that may be used to provide an elementary support of such capabilities. A complementary approach to managing updates and structured application access to such dynamic clinical information may be expected as a separate Integration Profile in the future.
2. 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.
3. The operation of any XDS Clinical 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 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 Authentication, Document Digital Signature, etc).
4. 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 transferring information from one Clinical Affinity Domain to another, or to allow access from one Affinity Domain to documents managed in other Affinity Domains. XDS has been designed with this extension in mind. An XDS Domains Federation Integration Profile that complements XDS may be anticipated in the future.

5. XDS does not address transactions for the management or configuration of a clinical 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 clinical affinity domain.

10.1 Actors/Transactions

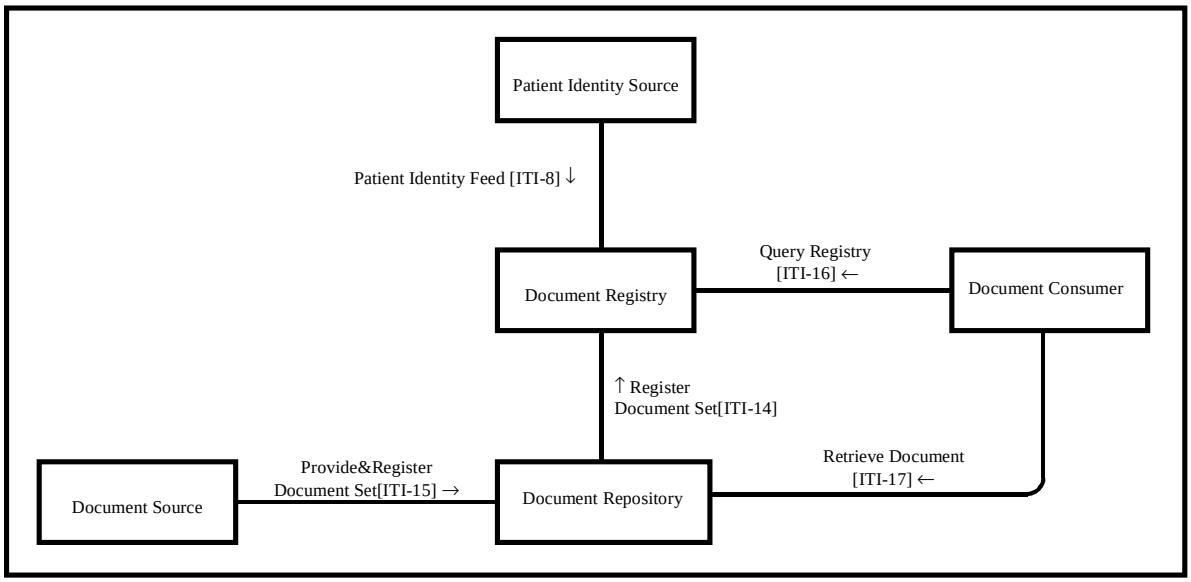


Figure 10.1-1 Cross-Enterprise Document Sharing Diagram

Table 10.1-1 XDS - Actors and Transactions

Actors	Transactions	Optionality	Section in Vol. 2
Document Consumer	Query Registry	R	ITI TF-2:3.16
	Retrieve Document	R	ITI TF-2:3.17
Document Source	Provide and Register Document Set	R (Note 1)	ITI TF-2:3.15
	Off-Line Transaction mode	O	ITI TF-1:10.4.7.1
	Multiple Documents Submission	O	ITI TF-2:3.15.5
	Document Life Cycle Management	O	ITI TF-2:3.15.5
	Folder Management	O	ITI TF-2:3.15.5
Document Repository	Provide and Register Document Set	R (Note 1)	ITI TF-2:3.15
	Register Document Set	R (Note 2)	ITI TF-2:3.14
	Retrieve Document	R	ITI TF-2:3.17
	Off-Line Transaction mode	O	ITI TF-1:10.4.7.1
Document Registry	Register Document Set	R (Note 2)	ITI TF-2:3.14
	Query Registry	R	ITI TF-2:3.16
	Patient Identity Feed	R	ITI TF-2:3.8
Patient Identity Source	Patient Identity Feed	R (Note 3)	ITI TF-2:3.8

Note 1: The Provide and Register Document Set is not required in implementations where the Document Source is grouped with the Document Repository Actor.

Note 2: The Register Document Set Transaction is not required in implementations where the Document Registry Actor is grouped with the Document Repository Actor. However, it is strongly recommended that these transactions be supported to allow for future configuration with multiple Repositories.

Note 3: If Assigning Authority of Patient ID presents in the Patient Identity Feed transaction, the Patient Identity Source is required to use an OID to identify the Assigning Authority. For technical details of the assigning authority information, see Transaction 8 in Technical Framework, Volume 2.

10.1.1 Actors

10.1.1.1 Document Source

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.

10.1.1.2 Document Consumer

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.

10.1.1.3 Document Registry

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.

10.1.1.4 Document Repository

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 URI to documents for subsequent retrieval by a Document Consumer.

10.1.1.5 Patient Identity Source

The Patient Identity Source Actor is a provider of 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.

10.1.2 Transactions

10.1.2.1 Provide and Register Document Set

A Document Source Actor initiates the Provide and Register Document Set Transaction. For each document in the submitted set, the Document Source Actor provides both the documents as an opaque octet stream and the corresponding metadata to the Document Repository. The Document Repository is responsible to persistently store these documents, and to register them in the Document Registry using the Register Documents transaction by forwarding the document metadata received from the Document Source Actor.

10.1.2.2 Register Document Set

A Document Repository Actor initiates the Register Document Set transaction. This transaction allows a Document Repository Actor to register one or more documents with a Document Registry, by supplying metadata about each document to be registered. This document metadata will be used to create an XDS Document Entry in the registry. The Document Registry Actor ensures that document metadata is valid before allowing documents to be registered. If one or more documents fail the metadata validation, the Register Document Set transaction fails as a whole.

To support composite documents, an XDS Document may be a multipart document. The Document Repository must handle multi-part data sets as an “opaque entity”. The Document Repository does not need to analyze or process its multi-part structure nor the content of any parts in the context of the XDS Integration Profile.

10.1.2.3 Query Registry

The Query Registry transaction is issued by the Document Consumer Actor on behalf of a care provider (EHR-CR) to a Document Registry. The Document Registry Actor searches the

registry to locate documents that meet the provider's specified query criteria. It will return a list of document entries that contain metadata found to meet the specified criteria including the locations and identifier of each corresponding document in one or more Document Repositories.

10.1.2.4 Retrieve Document

A Document Consumer Actor initiates the Retrieve Document transaction. The Document Repository will return the document that was specified by the Document Consumer.

To support composite documents, an XDS Document may be a multipart document. In this case, the Document Consumer must take appropriate actions to make the multipart content accessible to the user.

10.1.2.5 Patient Identity Feed

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 XDS Integration Profile is to populate the registry with patient identifiers that have been registered for the affinity domain.

10.1.3 XDS Document Contents Support

The following table lists the document contents supported in other IHE Integration Profiles, which specify concrete content types for sharing of clinical documents in various domains. These profiles are built on the XDS profile, and may define additional constraints and semantics for cross-enterprise document sharing in their specific use cases.

Table 10.1-1: List of IHE Integration Profiles and Document Types They Support

IHE Technical Framework Domain	Integration Profile Name	Document Content Supported
Patient Care Coordination	Cross-Enterprise Sharing of Medical Summaries	Medical Summary in the HL7 CDA format
Radiology	Cross-Enterprise Document Sharing for Imaging (XDS-I)	Radiology Diagnostic Report in the plain text or PDF formats
		Reference to a collection of DICOM SOP Instances in a manifest document in the DICOM Key Object Selection format

10.2 Integration Profile Options

Options that may be selected for this Integration Profile are listed in the table 10.2-1 along with the Actors to which they apply. Dependencies between options when applicable are specified in notes.

Table 10.2-1 XDS - Actors and Options

Actor	Options	Vol & Section
Document Source	*Off-Line transaction mode*	ITI TF-1:10.4.7.1
	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	*Off-Line transaction mode*	ITI TF-1:10.4.7.1
Document Registry	*No options defined*	- -
Document Consumer	*Query Registry Transaction (Note 1)*	ITI TF-2:3.16
	Retrieve Document Transaction (Note 1)	ITI TF-2:3.17
Patient Identity Source	*No options defined*	- -

Note1: For the XDS Document Consumer Actor, either one or both of the two options shall be selected.

10.2.1 Multiple Documents Submission Option.

In this option the Document Source offers the ability to include multiple documents in a single Submission Request.

10.2.2 Document Life Cycle Management Option

In this option the Document Source offers the ability to perform the following operation:

- Submit a document as an addendum to another document already in the registry/repository
- Submit a document as a transformation of another document already in the registry/repository

Note: In order to support document replacement/addendum/transformation grouping with the Document Consumer may be necessary in order to Query the registry (e.g. for UUIDs of existing document entries

10.2.3 Folder Management Option

In this option the Document Source offers the ability to perform the following operation:

- Create a folder
- Add one or more documents to a folder

Note: In order to support document addition to an existing folder, grouping with the Document Consumer may be necessary in order to Query the registry (e.g. for UUIDs of existing folder).

10.3 Integration Profile Process Flow

A typical patient goes through a sequence of encounters in different care settings. In each care setting, the resulting patient information is created and managed by multiple care delivery information systems (EHR-CRs). Through a sequence of care delivery activities, a number of clinical documents are created. The EHR-LR provides the means to share the relevant subset of these documents, as they are contributed by the various EHR-CRs that are part of the same clinical affinity domain.

10.3.1 Example : Cardiac Patient Management Scenario

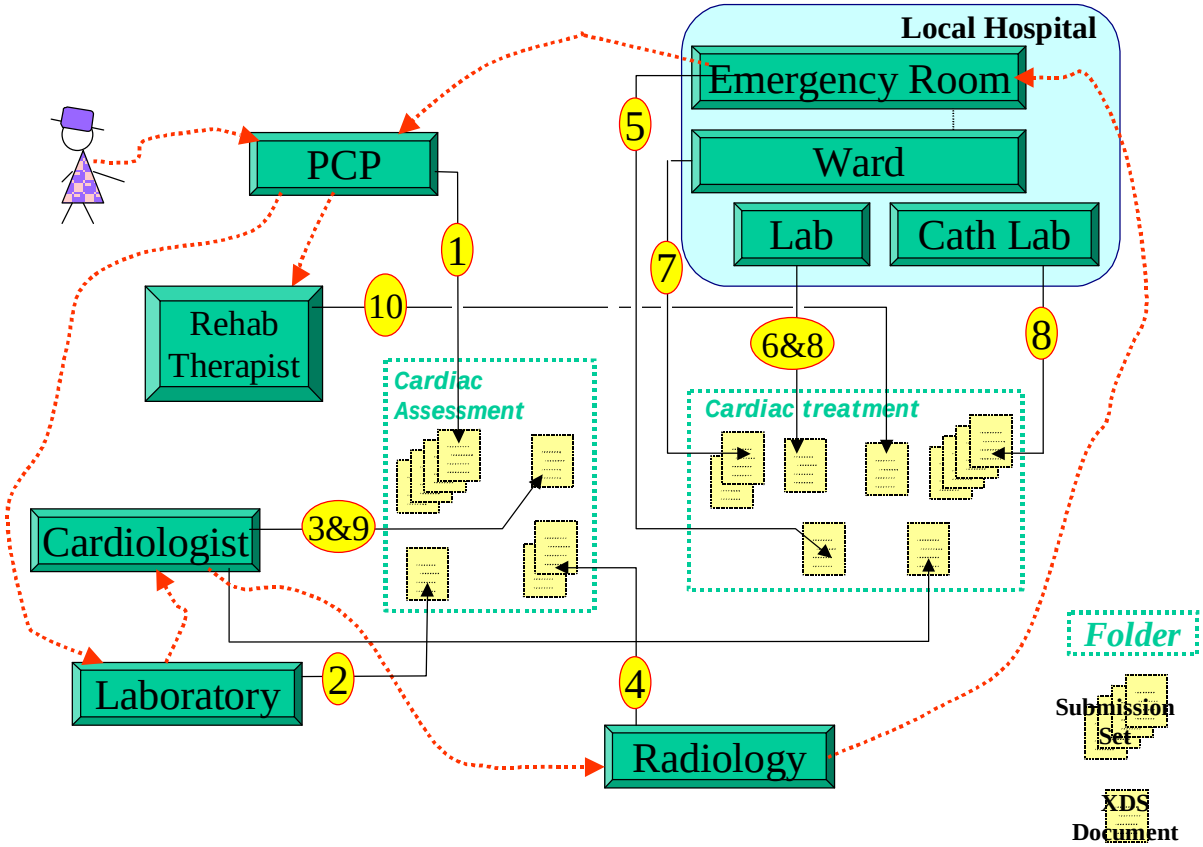


Figure 10.3-1 Cardiac Patient Management Scenario Transaction Process Flow

This scenario spans about 3 weeks of a patient's cardiac episode. The patient presents to her primary care provider (PCP) with complaints of shortness of breath, nausea, tiredness and chest pains. This doctor works closely with a local hospital that has recently established a cardiac care

network that allows PCPs, cardiologists, laboratories and two local hospitals to share clinical documents to improve patient care. This cardiac network is part of a local care data exchange community that has been set-up in this community and to which the care plan to which this patient belong has encouraged patients to subscribe. Our patient has been provided a health record account number.

1. During the patient examination, the PCP records the complaint, and determines that he should perform an ECG. He queries the cardiac care network to see if there are prior ECG reports (step 1 in Figure 10.3-2), using a coded document class "report" and a coded practice setting "cardiology" established by the cardiac care network for ECG reports. Among the matching Documents, he locates a prior ECG report that is then retrieved (step 2 in Figure 10.3-2). He compares the two results and determines that the patient should be referred to a cardiologist. He searches for additional reports in the cardiac care network (step 3 in Figure 10.3-2) for this patient, but finds none.

   Using the ambulatory EHR system, he creates a submission request onto the patients health record account number for a "PCP office visit" that includes a submission set consisting of three new documents (visit note, referral letter, new ECG report) and of one reference to the prior ECG report (step 4 in Figure 10.3-2). Following the Cardiology Network Affinity Domain policy, he creates a "cardiac assessment" Folder to contain all four documents in order to facilitate collaboration with the cardiologist.

   The repository used by the ambulatory EHR system will then register the documents that are part of this submission request (step 5 in Figure 10.3-2).

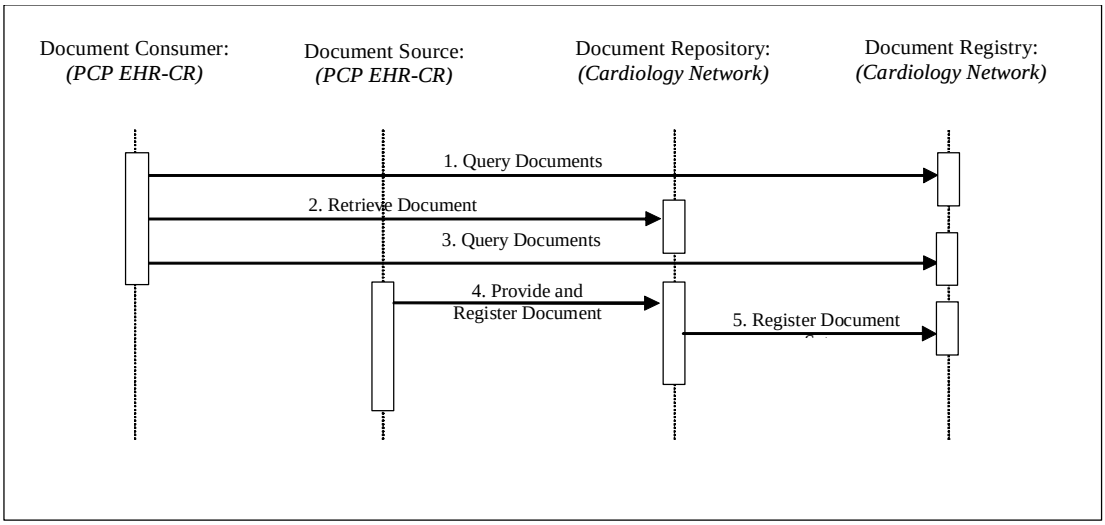


Figure 10.3-2 PCP Query Transactions Process Flow

The PCP EHR system implements the Document Consumer and Document Source actors to issue the Query, Retrieve and Provide & Register transactions as shown in Figure 10.3-2. The transactions are processed by the Document Repository and the Document Registry provided by the cardiology care network.

2. The patient appointment with the cardiologist is scheduled. The patient goes to the lab for the lab tests required before appointment. The lab creates a submission set with a clinical code of "laboratory tests" containing the lab results. The lab is not aware of the "cardiology assessment" folder.

3. The cardiologist sees the patient. He queries the repository for any patient's records in a "cardiac assessment" folder (step 1 in Figure 10.3-3). Available are the visit note from the PCP, the ECG and prior ECG, and the referral letter, which he retrieves and reviews (steps 2-5 in Figure 10.3-3). He also queries for recent lab reports, and finds the lab results (step 6 in Figure 10.3-3). This is also retrieved and reviewed (step 7 in Figure 10.3-3).

   The cardiologist performs an ultrasound, dictates a visit note, and orders a nuclear stress test. The visit note and ultrasound images and report are registered as a "cardiologist office visit" submission set and placed in the "cardiac assessment" Folder. In addition, the lab report is added to the "cardiac assessment" Folder (step 8 in Figure 10.3-3).

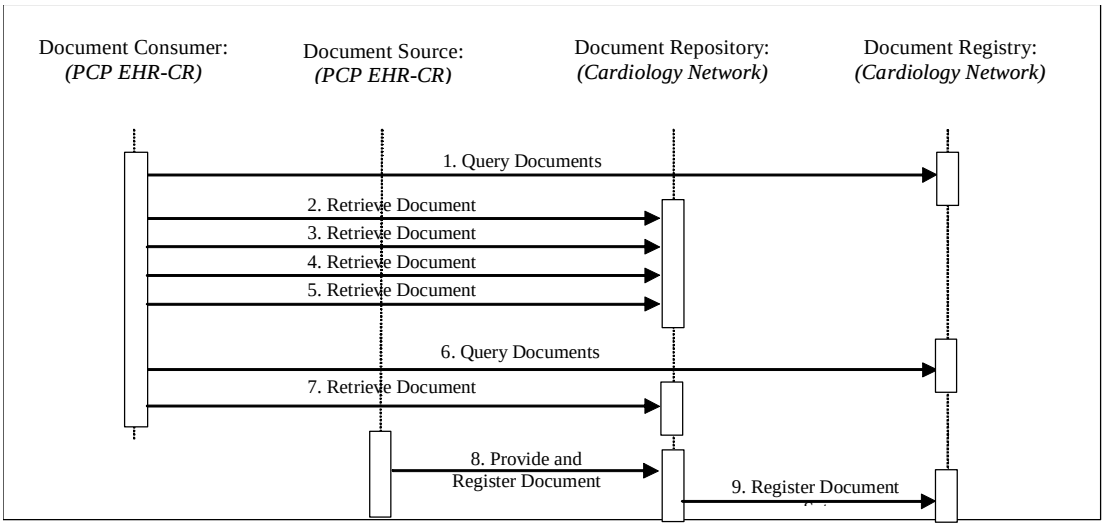


Figure 10.3-3 PCP Query Transactions Process Flow

4. The patient is seen at a radiology facility for the nuclear stress test. The test is performed, and the radiologist dictates the report. The nuclear stress test report is registered in a "radiology examination" submission set and associated with the "cardiac assessment" Folder

5. Although she has a scheduled appointment with her cardiologist in two days, she wakes up with severe chest pain. On the way to work, she decides to go to the emergency room (ER) of her local hospital.The ER doctor uses the hospital EHR system to query the cardiac care network registry and repositories for documents related to the patient in reverse chronological order (step 1 in Figure 10.3-4). Available documents from latest cardiology related Folder are the visit notes from the PCP and cardiologist, the recent

and prior ECGs, the lab results, and the ultrasound images and report, and the nuclear stress test images and report.

The ER doctor retrieves and reviews the two most relevant reports (step 2 and 3 in Figure 10.3-4).

The ER doctor orders lab tests, ECG, and places the patient under monitoring. The lab tests and ECG are placed in the hospital EHR that acts as a Document Repository Actor for the cardiac network. Abnormal cardiac activity requires a catheterization, diagnostics and possibly intervention. The ER doctor admits the patient to the cardiology service and contacts the cardiologist.

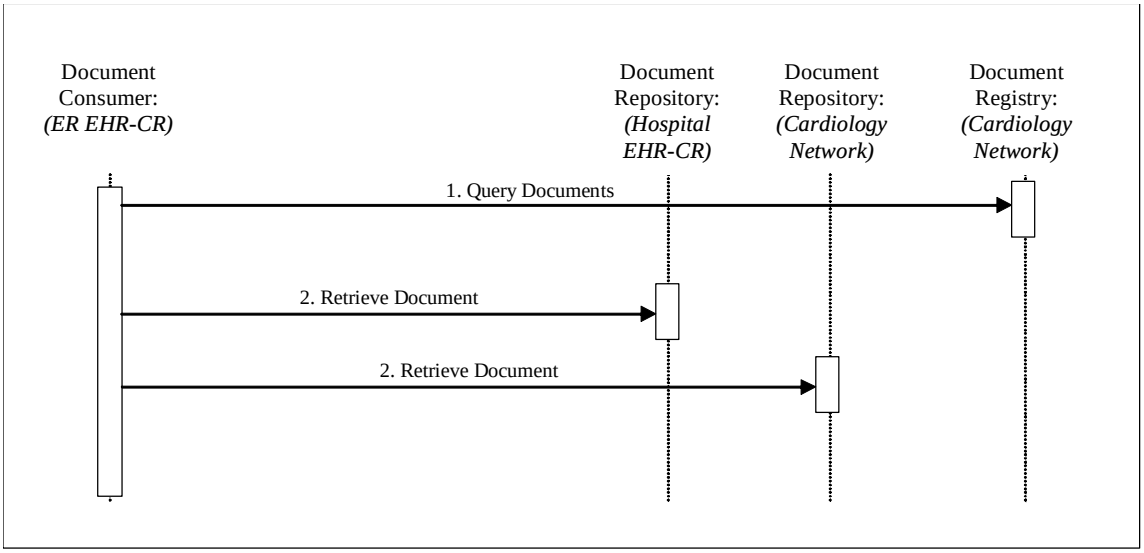


Figure 10.3-4 ER Query Transactions Process Flow

6. While talking to the ER physician, the cardiologist accesses the cardiac care network from his home office. He queries for all documents related to the patient since the last visit in his office. The nuclear stress test report that he did not previously review is available, along with lab results and ECG results from the ER. The two physicians determine a plan of care and the cardiologist makes arrangements to see the patient in the hospital.

7. As the patient is transferred from the ER, the ER visit notes are submitted as an "emergency department visit" submission set and placed in a newly created "cardiology treatment" Folder along with the earlier lab and ECG results.

8. The patient is transferred to an inpatient bed with the following sequence of events.
   - The patient is scheduled for a catheterization procedure in cath lab.
   - Additional lab tests are ordered and performed.
   - A diagnostics procedure is performed in cath lab.
   - An intervention with the placement of a stent is performed.
   - A cath intervention report is dictated.
   - Patient is returned to monitored care for recovery.

- Education given to patient and family.
- Discharge Summary dictated by cardiologist.
- Cardiologist orders lab tests to be completed prior to scheduled follow-up visit.

The admission assessment, lab results, cath intervention report and key images, and discharge summary form a "cardiology intervention" submission set, which is registered with the cardiac care network registry in the "cardiac treatment" Folder started by the ER.

9. The patient returns to the cardiologist for the post discharge follow-up visit. The resulting visit note, cardiac rehab and summary letters are placed in a "cardiology office visit" submission set and in the "cardiac treatment" Folder.

10. The patient goes to rehab sessions as scheduled by the cardiologist. The patient recovers and is seen by the PCP and cardiologist for routine visits.

10.4 General Principles

10.4.1 EDR-CR Concept

An EHR-CR or Care-delivery Record abstracts the information system or systems of a care delivery organization, which may support a broad variety of healthcare facilities: private practice, nursing home, ambulatory clinic, acute care in-patient facility, etc.

Typically a patient goes through a sequence of encounters in different care settings as depicted in the figure below.

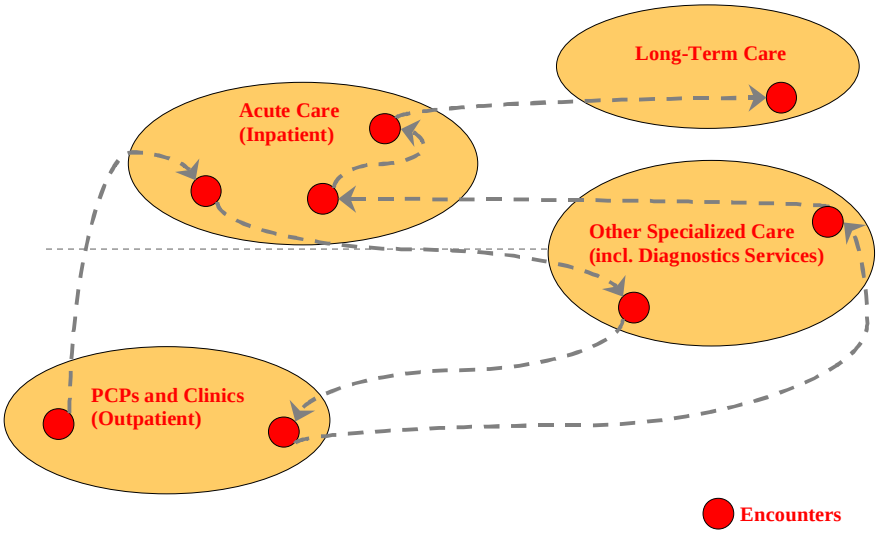


Figure 10.4.1-1 Sequence of encounters across care delivery organizations

It is out of the scope of this IHE Integration Profile to define or restrict the type of care provided, nor the internal workflow of a care delivery organization. The EHR-CR system participates only to the cross-enterprise clinical document sharing as Document Source and Document Consumer Actors according to the following principles:

1. EHR-CR as Document Source contributes documents in any one of the document formats that are supported by the XDS Affinity Domain (e.g. CDA Release 1, CDA Release 2 with specific templates, DICOM Composite SOP Classes, ASTM-CCR, CEN ENV 13606 etc).
2. This Profile does not require that the EHR-CR as Document Sources and Consumers store and manage their internal information in the form of documents as they are shared throughout the XDS Affinity Domain.

3. By grouping a Document Source with a Document Repository, an EHR-CR may leverage existing storage to provide a unified access mechanism without needing to duplicate storage.
4. EHR-CRs as Document Sources and Consumers are responsible to map their local codes into the affinity domain codes if necessary.

The XDS Documents shared by the EHR-CR and tracked by the XDS Registry form a Longitudinal Record for the patients that received care among the EHR-CRs of the XDS Affinity Domain.

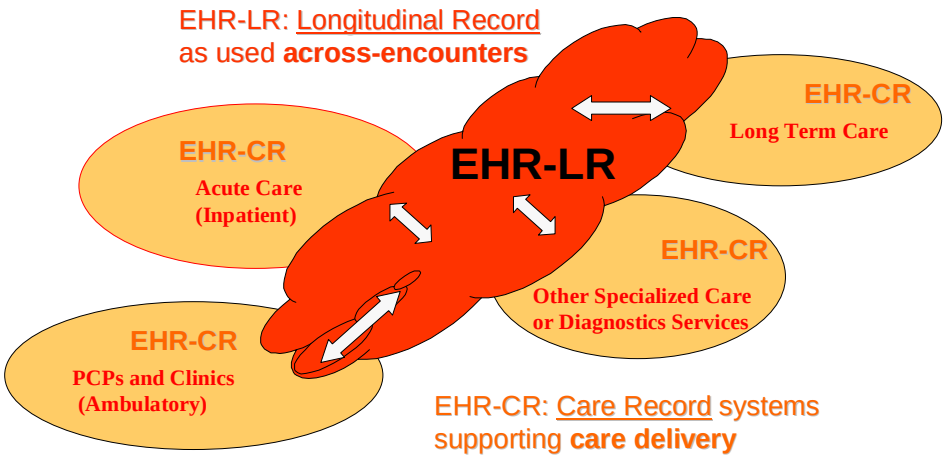


Figure 10.4.1-2 Contributing and sharing to a patients' longitudinal health record

This shared clinical record is called an EHR-LR in this Integration Profile.

10.4.2 XDS Document Concept

An XDS Document is the smallest unit of information that may be provided to a Document Repository Actor and be registered as an entry in the Document Registry Actor.

An XDS Document is a composition of clinical information that contains observations and services for the purpose of exchange with the following characteristics: Persistence, Stewardship, Potential for Authentication, and Wholeness. These characteristics are defined in the HL7 Clinical Document Architecture Release 1 specification. An XDS Document may be human readable (with the appropriate application). In any case, it should comply with a published

standard defining its structure, content and encoding. IHE intends to define content-oriented Integration Profiles relying on such content standards to be used in conjunction with XDS.

The XDS Integration Profile manages XDS Documents as a single unit of information; it does not provide mechanisms to access portions of an XDS Document. Only the Document Sources or Document Consumers have access to the internal information of the XDS Document. When submitted for sharing, an XDS Document is provided to the Document Repository Actor as an octet stream. When retrieved through the Retrieve Document transaction, it shall be unchanged from the octet stream that was submitted.

The Document Source Actor is responsible to produce the metadata that will be submitted to the Document Registry Actor to form the XDS Document Entry that will be used for query purposes by XDS Consumer Actors. The Document Source maintains responsibilities over the XDS Documents it has registered. It shall replace XDS Documents that may have been submitted in error. See ITI TF-1: Appendix K for a more detailed discussion of the concept of XDS Document.

XDS Documents are required to be globally uniquely identified. See ITI TF-2:Appendix B for a definition of globally unique identifiers.

10.4.3 Submission Request

An XDS Submission Request is a means to share XDS Documents. It may be conveyed:

- by a Document Source Actor in a *Provide and Register Document Set Transaction* to the Document Repository Actor, or
- by a Document Repository Actor in a *Register Document Set Transaction* to the Document Registry Actor

An XDS Submission Request contains elements of information that will ensure the proper registration of XDS Documents. These are:

1. Metadata to be placed in Document Entries for new XDS Documents being submitted,
2. A Submission Set that includes the list of all new XDS Documents and Folders being submitted and optionally a list of previously submitted XDS Documents,
3. If desired, Folders to be created with the list of included XDS Documents (new document being submitted as well as previously submitted),
4. If desired, addition to previously created Folders of lists of XDS Documents (new document being submitted as well as previously submitted), and
5. Zero or more XDS Document octet streams for the new XDS Documents being submitted.

Following a successful Submission Request, new XDS Documents, Submission Set, and Folders included in the Submission Request are available for sharing in an XDS Clinical Affinity

Domain. In case of failure to process a Submission Request, the Submission Set and any XDS Documents and Folders shall not be registered.

10.4.4 Submission Set Concept

An XDS Submission Set is related to care event(s) of a single patient provided by the care delivery organization EHR-CR performing the submission request. It creates a permanent record of new XDS Documents as well as pre-existing (i.e. already registered) XDS Documents that have a relationship with the same care event(s). It also includes the record of new XDS Folders creation.

An XDS Submission Set shall be created for each submission request. It is related to a single Document Source Actor and is conveyed by a single Provide & Register Document Set Transaction or a Register Document Set Transaction.

The Document Registry may be queried to find all documents registered in the same XDS Submission Set.

The same XDS Document, initially registered as part of a Submission Set, may also be referenced by later XDS Submission Set. This allows older documents relevant to the present care of a patient to be associated with more recent Submission Sets.

XDS provides complete flexibility to EHR-CRs to relate Documents and Submission Sets to an encounter, a visit, an episode of care, or various workflow processes within EHR-CRs.

10.4.5 Concept of Folder

The purpose of an XDS Folder is to provide a collaborative mechanism for several XDS Document Sources to group XDS Documents for a variety of reasons (e.g. a period of care, a problem, immunizations, etc.) and to offer the Document Consumers a means to find all Document Entries placed in the same Folder. The following principles apply to an XDS Folder:

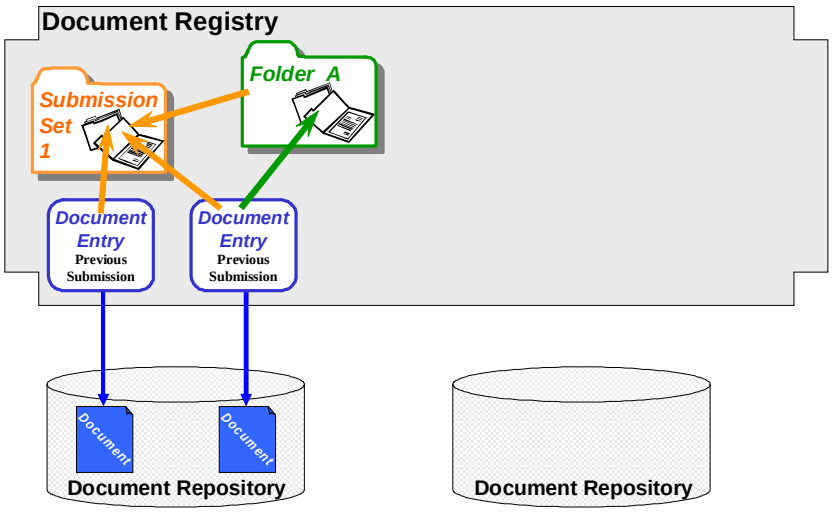
1. A Folder groups a set of XDS Documents related to the care of a single patient,
2. One or more Document Source Actors may submit documents in a given Folder,
3. A Folder may be created by a Document Source and/or predefined in an Affinity Domain,
4. The content of a Folder is qualified by a list of codes/meaning,
5. Document Source Actors may find existing Folders by querying the Document Registry or by means outside the scope of XDS (e.g. Cross-enterprise workflow, such ePrescription, eReferral, etc),
6. Once created a Folder is permanently known by the Document Registry,
7. Placing previously existing Documents in Folders is not recorded as part of the Submission Set,
8. Folders in XDS may not be nested,
9. The same documents can appear in more than one Folder, and

10. Folders have a globally unique identifier.

10.4.6 Example of use of Submission Request, Submission Set and Folder

The sequence of figures below shows an example of a submission request that includes two new documents, a reference to a pre-existing document and the use of two folders. The first figure depicts the initial state of a Document Registry in which two Documents have been submitted where one is associated with a Folder A. The second figure depicts a submission request that adds two new documents, placing one of them into a pre-existing folder and the other one into a new Folder B.

Document Repository and Registry – Initial State



Document Repository and Registry – Submission Request

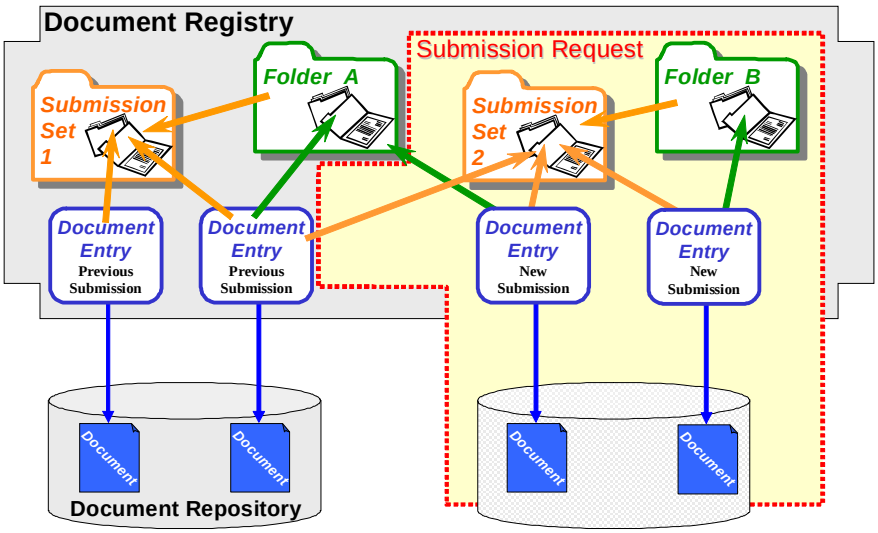


Figure 10.4.6-1 Example of a submission flow to an XDS Registry

From the above example, the contents of a Submission Set are shown by the figure below. The Document Entries associated with the Submission Set are logical part of the Submission Set.

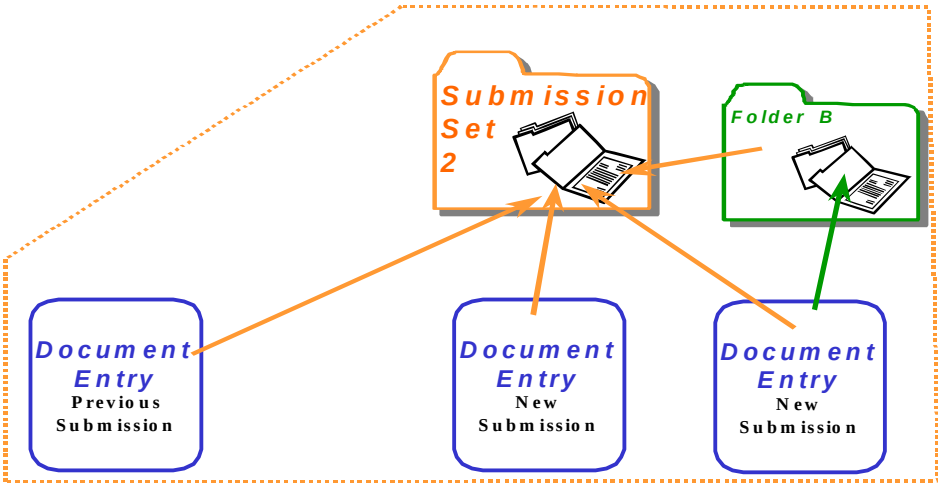


Figure 10.4.6-2 The logical content of a Submission Set

10.4.7 XDS Registry Data Model and Attributes

The XDS Integration Profile provides a means to place documents in a repository chosen by the Document Source, and also to place information about this document (or metadata) in an entry of the Document Registry that manages the Affinity Domain.

The term metadata reflects that this information is "about" the documents. The purpose of well-specified document metadata is to enable a uniform mechanism for Document Consumers to locate clinical documents of interest much in the way a card catalog in a library helps readers find the book they want.

This section addresses the high-level data model in which the metadata is registered and against which queries of the XDS registry are performed. Then it presents the specific attributes that may be registered and used to filter the document entries of the registry.

10.4.7.1 XDS Document Registry Data Model

The following entities are used in the XDS Document Registry Data Model:

XDS Document Entry: Information entity managed by a Document Registry Actor that contains a set of metadata describing the major characteristics of an XDS Document along with a link to the Document Repository Actor where the actual XDS Document may be retrieved.

XDS Document: A stream of bytes stored in a Document Repository Actor and pointed to by an XDS Document Entry.

XDS Folder: A logical container that groups one or more XDS Document Entries in any way required (e.g. by source care delivery activities, by episode, care team, clinical specialty or clinical condition). This kind of organizing structure is used variably: in some centers and systems the Folder is treated as an informal compartmentalization of the overall health record; in others it might represent a significant legal portion of the EHR relating to the originating enterprise or team. The Folder is a means of providing organization of XDS Documents (or Composition in EHRCOM). The same XDS Document Entry may belong to zero or more Folders.

XDS Submission Set: When XDS Documents are registered by a Document Source Actor, they shall be included in one and exactly one Submission Set. An XDS Submission Set groups zero or more new XDS Documents and references to already registered XDS Documents to ensure a persistent record of their submission.

XDS Submission Request: A Submission Request includes one and only one Submission Set, zero or more new XDS Folders and assignment of XDS Documents into new or existing Folders. A Submission Request is processed in an atomic manner by the Document Repository and the Document Registry (i.e. all XDS Documents included or referenced in a Submission Set as well

as the Folders and inclusion of Folders references are registered or none will). This ensures that they are all made available to Document Consumer Actors at the same time.

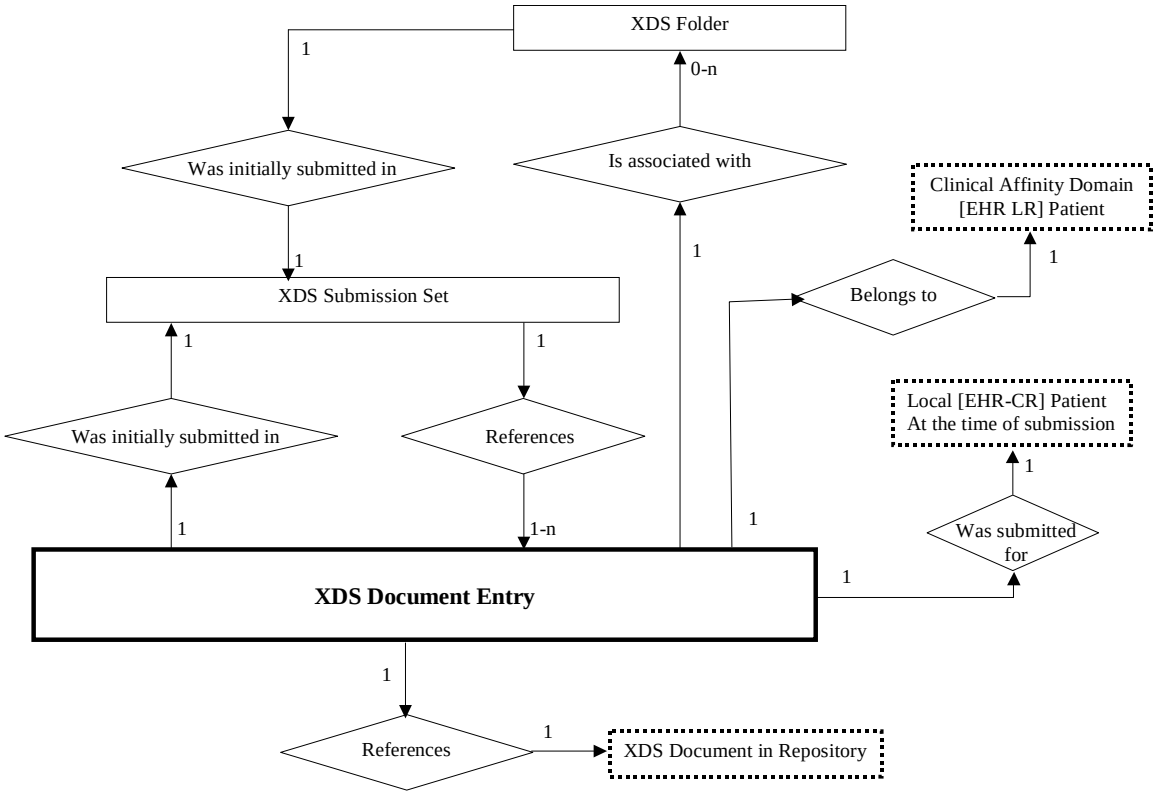


Figure 10.4.7-1 XDS Document Registry Data Model

10.4.7.2 Attributes of the XDS Document Entries

The specific attributes of each entity in the above registry data model have been selected from document header attributes from several standards (see ITI TF-2:Appendix L), including:

- ANSI/HL7 CDA R1-2000
- HL7 CDA Release 2 (draft) Document header definition (Dec 2003 Committee Ballot)
- Composition attributes from EHR ENV 13606 (draft).

XDS defines a well focused set of primary attributes that support the most common use cases to search the most relevant documents. These include:

Patient Id
Service Start and Stop Time
Document Creation Time
Document Class Code and Display Name
Practice Setting Code and Display Name
Healthcare Facility Type Code and Display Name
Availability Status (Available, Deprecated)
Document Unique Id

The three codes (Document Class, Practice Setting and Healthcare facility Type) are code set that are expected to generally include a limited number of values (between 10 and 100), thus ensuring a reasonably easy search capability.

A number of additional query attributes or attributes used to perform a secondary selection in order to decide to retrieve a specific document are also defined by this Integration Profile. At the Document Level, these include a fine grained Document Type (e.g. LOINC classification), a list of Event Code that can be used as key word, the document author and associated institution, the document relationship to manage replacement addendum and a variety of transformations, a confidentiality code, language code, etc.

The complete list of attributes and their definition is documented in the IHE ITI Register Transaction (see Volume II section 3.12).

10.4.8 Concept of an XDS Affinity Domain

An XDS Affinity Domain is an administrative structure made of a well-defined set of Document Source Actors, set of Document Repositories, set of Document Consumers organized around a single Document Registry Actor that have agreed to share clinical documents.

Note: Document Sources, Repositories and Consumers may belong to more than one Affinity Domain and share the same or different documents. This is an implementation strategy and will not be further described.

Note: the XDS Integration Profile does not support the federation of Affinity Domains. It is expected that a future IHE Integration Profile will address the cooperation of multiple Document Registry Actors serving different Affinity Domains.

A number of policies will need to be established in an Affinity Domain in order to ensure effective interoperability between Document Sources and Consumers. Some of the key technical policies include (A more extensive list of policy agreements that need to be made by Affinity Domains is discussed in ITI TF-1: Appendix L):

1. The document formats that will be accepted for registration
2. The various vocabulary value sets and coding schemes to be used for the submission of metadata of document, submission set and folders registration.

3. The Patient Identification Domain (Assigning Authority) used by the Document Registry.

See ITI TF-1: Appendix K for a detailled discussion of the concepts of XDS Affinity Domain.

10.4.9 Patient Identification Management

Since the central focus of the DS Integration Profile is "sharing documents", it is critical that each document be reliably associated with the corresponding patient (Patient Id).

The XDS Document Registry is not intended to be an authority for patient identification and demographics information. This Integration Profile uses a Patient Identity Source Actor as the authoritative source of Patient Identifiers (master patient ID) for the Affinity Domain.

Note: This Integration Profile can be easily extended to support a scenario where no master patient ID is defined (i.e. no Patient Identity Source for the Affinity Domain). Such option, would requiring the use of federated patient identities at the time of query of the XDS Document Registry, may be expected as a future addition to this Integration Profile.

The following principles are defined:

1. The Patient Identifier Domain managed by the Patient Identity Source Actor in the Affinity Domain is the source of patient identifiers (and merge operations) used by the XDS Document Registry to link Documents to a specific Patient. This Patient Identifier Domain is called the XDS Affinity Domain Patient Identification Domain (XAD-Pid Domain).
2. Submission Requests for Documents related to Patients with IDs not registered in the XDS Affinity Domain Patient Identifier Domain shall be rejected by the XDS Document Registry.
3. The XDS Document Registry will contain certain patient information (e.g. source patient ID, Surname, Given Name, Sex, Birthdate) for the purpose of audits and potential verification by Document Consumers. As this Integration Profile does not make any assumptions about the referential integrity and update of this information, these fields[1] shall not be used as query matching keys.
4. As XDS Document Sources and Consumers may belong to different Patient Identification Domains, these systems need to cross-reference their own local Patient ID to the corresponding patient ID in the XAD-Pid Domain of the Registry. Preferably, these systems may choose to use the IHE Patient Identifier Cross-referencing Integration Profile (See Appendix E.3) for this purpose.

[1] It is possible to submit a new document to replace a previously submitted one, with a new document entry created in the registry to correct for errors in the submitted document in the original submission request. However this is not a mechanism that updates only the metadata, as the replaced document is only deprecated and remains pointed by the original metadata.

5. The XDS Document Registry is responsible for validating Document metadata in accordance with the XDS Affinity Domain's policies. The Document Registry should reject submissions Requests that do not conform to these policies.

The figure below depicts an example of an Affinity Domain with its Patient Identifier Domain (called XAD) and two EHR-CRs where the cross-referencing is performed internally to the Document Source and the Document Consumer Domains (Domain C and Domain D2 respectively).

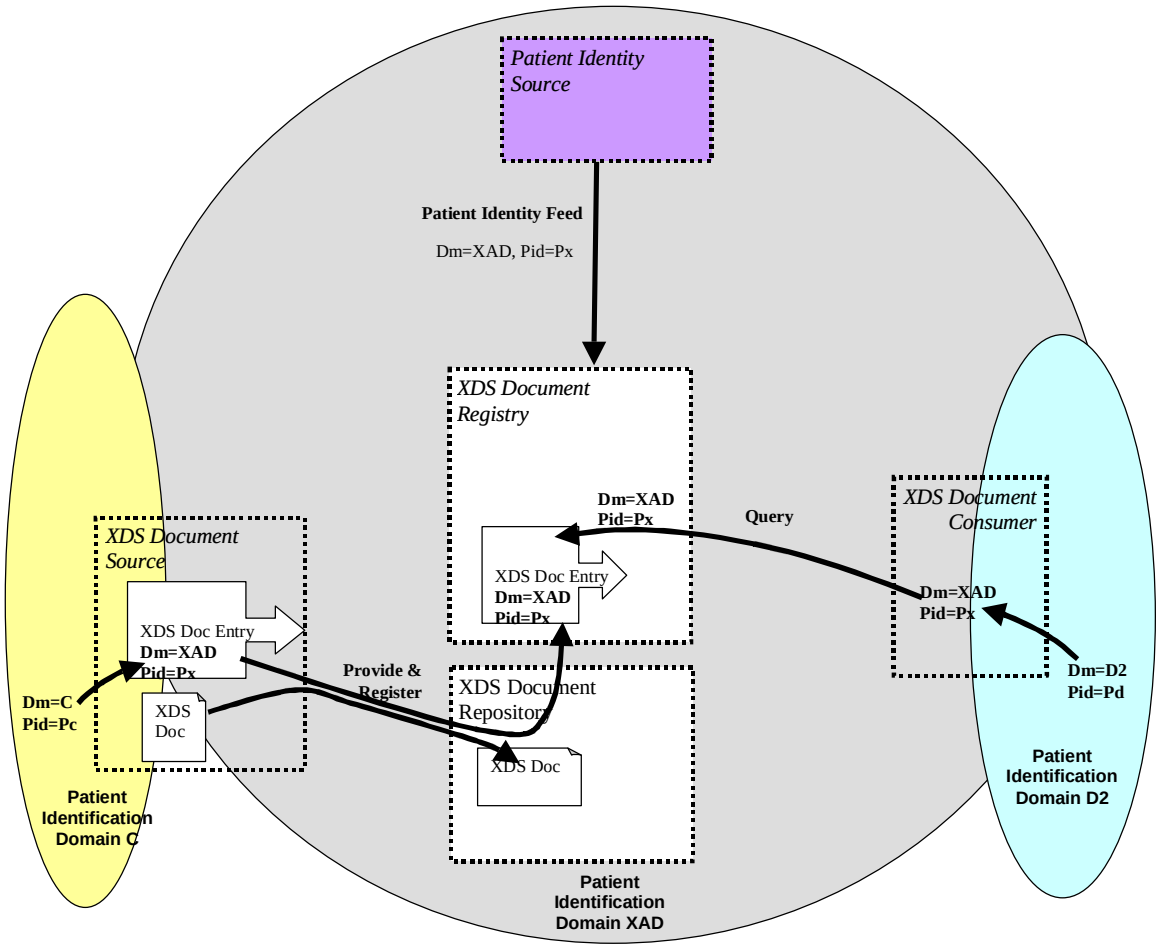


Figure 10.4.9-1 Affinity Domain with patient ID cross-referencing internal to the EHR-CRs

10.4.10 Document Lifecycle

10.4.10.1 Document Availibility Status

Each XDS Document contained in a XDS Document Registry will be assigned one of the following Availability Status codes:

Approved: Available for patient care (assumes that it is authenticated, if applicable)

Deprecated: Obsolete, but may still be queried and retrieved

The XDS Document availability status is set to "approved" after the XDS Document Repository and the XDS Document Registry have successfully processed a submission request.

Note: ebXML Registry Services defines a Status of Submitted, which is used in a transient manner to provide an atomic submission. It is not significant to make this specific status externally visible.

An "approved" XDS Document may be changed to "deprecated" under the primary responsibility of its original Document Source with possible patient supervision. It is part of security policies that are beyond the scope of the XDS Integration Profile to have the XDS Repository/Registry enforce this ownership. The reason and responsible party for deprecating a document are tracked as part of the XDS Document Registry audit trail, which is a required capability. A "deprecated" Document remains available for Document Consumer queries. Except for the status change, a "deprecated" Document Entry metadata remains the same as when it was in the "approved" status.

An "approved" or "deprecated" XDS Document Entry may be deleted. This change is associated with the decision to completely remove a Document from an XDS Document Repository and the corresponding Document Entry from the XDS Document Registry. The XDS Affinity Domain shall establish the security policies associated with Document deletion. There are no transactions defined by this Integration Profile to support such operation.

See ITI TF-1: Appendix K for a detailled discussion of the concepts of XDS Document life cycle.

10.4.10.2 Document Relationships

XDS Documents may be related to predecessor documents by one of three methods:

- Replacement,
- Addendum
- Transformation
- Transformation-Replacement

These relationships between XDS Documents are tracked in the XDS Document Registry. The parent relationship attribute contained in the metadata of such Documents is a coded value that describes the type of relationship. An original Document has no parent and consequently its

parent Id and parent relationship are absent. XDS Document Registry shall reject submissions that contain relationships to documents that are not registered or have been "deprecated". Document stubs are supported by XDS to allow for a valid relationship to a known but not registered Document.

A replacement document is a new version of an existing document. The replacement document has a new document Id; its parent Id attribute contains the document Id of the Document Entry associated with the previous version of the XDS Document, and parent relationship contains the code "RPLC". The Document Entry for the previous version shall have its Availability Status changed to "deprecated".

An addendum is a separate XDS Document that references a prior document, and may extend or alter the observations in the prior document. It modifies the parent document, but the parent document remains a valid component of the patient record and shall remain in the state "approved" or available for care. The addendum XDS Document metadata contains the identifier of the previous XDS Document version in parent Id, and its parent relationship contains the code "APND".

A transformed document is derived by a machine translation from some other format. Examples of transformed documents could be CDA documents converted from DICOM Structured Reporting (SR) reports, or a rendering of a report into a presentation format such as PDF. The transform XDS Document contains the document Id of the previous version in parentId, and its parent relationship contains the code "XFRM". Affinity Domains may define rules that determine whether or not a transformed XDS Document replaces the source, but typically this would not be the case. If it is, an additional parent relationship of type "RPLC" is to be used.

10.4.11 Document Query

Query return info shall be either:

- a list of Registry Objects Values (e.g. XDS Document Entries)
- a list of Registry Objects UUIDs. This allows an XDS Document Consumer to receive a potentially long list of matching entries and to request them by subsets.

10.4.12 Transport Modes

The XDS Integration Profile defines an on-line mode of transport for all transactions except for the Provide & Register transactions where an off-line mode option is supported both for the Document Source and the Document Repository. In the "on-line mode" the transaction between two actors (computer applications) requires their simultaneous presence (e.g. an HTTP GET). In the "off-line mode" the transaction between the two actors (computer applications) does not require their simultaneous presence (e.g. a store and forward e-mail exchange).

1. An HTTP-based protocol (SOAP with Attachments) will be used for on-line operation.

2. The SMTP protocol will be used for off-line operation.

10.5 Implementation Strategies

The XDS Integration profile addresses the requirements of three major implementation strategies reflecting different groupings of actors within an EHR-CR as well as different configurations of the EHR-LR. This range of implementation strategies reflects the need to accommodate a variety of workflows and configurations. These implementation strategies may coexist in some environments. Other implementation strategies are possible.

Ø Strategy 1: Repository at the Source. A single information system acts as both the Document Source and Document Repository for the documents it creates and registers with the Document Registry

Upon completion of a phase of care, an EHR-CR will register a submission-set of documents in a Document Repository Actor with which it is grouped (same system). Then it registers this set of documents (newly created and priors documents of interest) with the Document Registry Actor[2].

Any other Document Consumer Actor in the Affinity Domain may query the Document Registry Actor to find documents related to all phases of care for the patient [3]. It may choose to retrieve some of these documents from any Document Repository Actor [4].

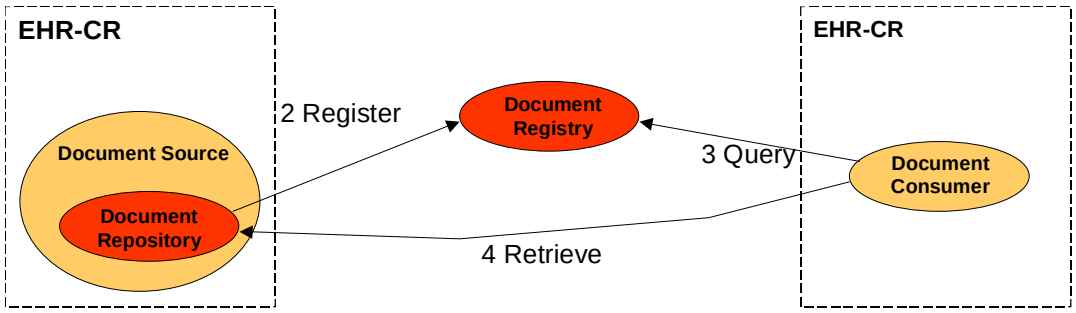


Figure 10.5-1 Implementation Strategy with Repository at the Source

Ø Strategy 2: Third Party Repository. The EHR-CR does not wish to be a Document Repository Actor, but rather uses the services of a third party Document Repository Actor to which it entrusts the documents it creates. First it provides both the metadata and the set of documents to this Document Repository Actor [1], which in turn forwards the registration request for the set of documents (newly created and prior documents of interest) to the Document Registry Actor [2].

Any other Document Consumer Actor may query the Document Registry Actor to find out about documents related to all phases of care for the patient [3]. It may choose to retrieve some of these documents from any Document Repository Actor [4].

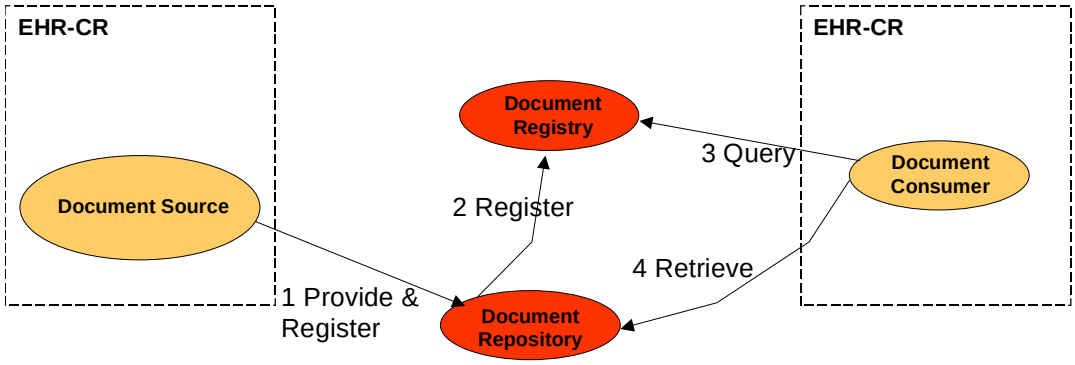


Figure 10.5-2 Implementation Strategy with 3rd party repository

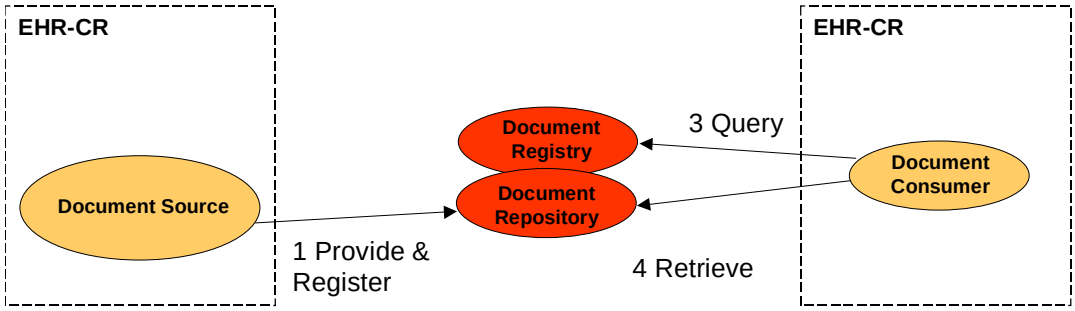


Table 10.5-3 Implementation Strategy with 3rd party central repository and registry

- Strategy 3: Direct Patient Transfer-Referral. The Document Source Actor completes a phase of care for a patient. It decides to directly provide and register [1] the set of documents (newly created and prior documents of interest) with a Document Repository [2] that has been grouped along with the Document Registry with the EHR-CR Document Consumer (Grouped Actors).

  In this case the span of the Clinical Affinity Domain may be quite limited as it could be defined to cover only the two EHR-CRs. However the same transaction [1] applies. Note that, in this implementation strategy the other transactions, although supported by the actors, are not used by the Document Consumer since the Document Registry and Document Repository reside within the Document Consumer.

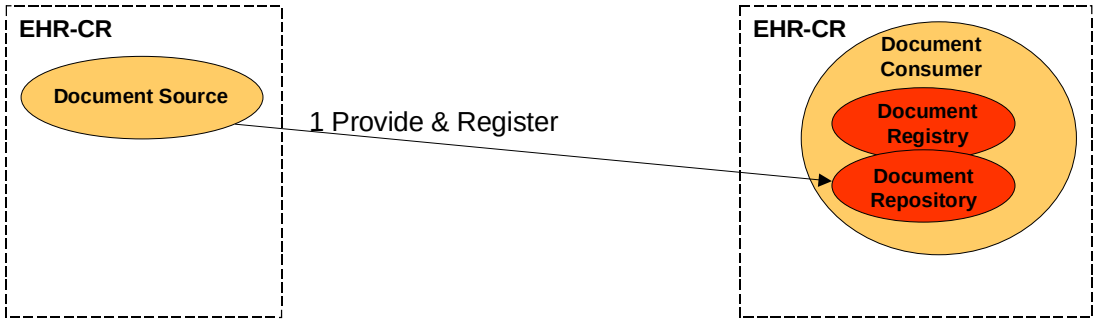


Figure 10.5-4 Direct patient referral with registry and repository at consumer

Patient access to an EHR-LR may be supported by a specialized EHR-CR (i.e. a portal) implementing the Document Source and Document Consumer Actors.

11 Personnel White Pages (PWP)

The Personnel White Pages (PWP) Profile provides access to basic directory information on human workforce members to other workforce members within the enterprise. This information has broad use among many clinical and non-clinical applications across the healthcare enterprise. The information will be used to

1. enhance the clinical workflow
    i. contact information,
    ii. phone numbers,
    iii. email address
2. enhance the user interface
    i. displayable names,
    ii. titles

This Personnel White Pages Profile specifies a method of finding directory information on the User Identities (user@realm) supplied by the Enterprise User Authentication (EUA) Integration Profile. This Profile assumes but does not define access controls, and audit trails. The use of the PWP Profile is intended for use within a healthcare enterprise. Extension to support sharing of the PWP between healthcare enterprises is possible but not fully addressed by this profile. The PWP profile is the first step on an IHE roadmap that includes Digital Certificates, Encryption, Digital Signatures, Medical Credentials, and Roles.

The directory need not support use cases beyond healthcare operations (e.g. Human Resource Operations), but does not forbid a properly designed overlap with other use cases. This profile does not intend for patients or other individuals that are not acting as part of the human healthcare workforce.

11.1 Actors/ Transactions

Figure 11.1-1 shows the actors directly involved in the PWP Integration Profile and the relevant transactions between them. Other actors that may be indirectly involved due to their participation in EUA profile are not necessarily shown.

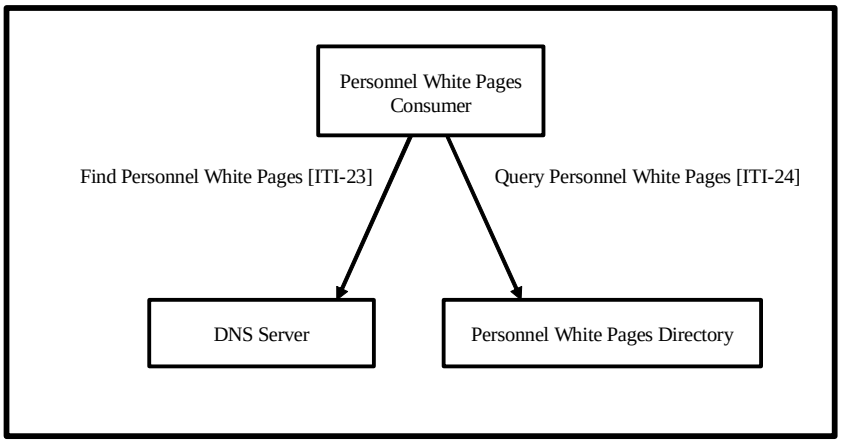


Figure 11.1-1: Personnel White Pages Profile Actor Diagram

Table 11.1-1 lists the transaction for each actor directly involved in the PWP Profile. In order to claim support of this Integration Profile, an implementation must perform the required transactions (labeled "R"). Transactions labeled "O" are optional. A complete list of options defined by this Integration Profile and that implementations may choose to support is listed in Section 11.2.

Table 11.1-1: PWP Integration Profile - Actors and Transactions

Actors	Transactions	Optionality	Section in Vol. 2
Personnel White Pages Consumer	Find Personnel White Pages	O	ITI TF-2: 3.23
	Query Personnel White Pages	R	ITI TF-2: 3.24
DNS Server	Find Personnel White Pages	R	ITI TF-2: 3.23
Personnel White Pages Directory	Query Personnel White Pages	R	ITI TF-2: 3.24

11.2 PWP Integration Profile Options

Options that may be selected for this Integration Profile are listed in the table 11.2-1 along with the Actors to which they apply. Dependencies between options when applicable are specified in notes.

Table 11.2-1 PWP Integration Profile - Actors and Options

Actor	Options	Vol & Section
Personnel White Pages Consumer	*no option*	
DNS Server	*no option*	
Personnel White Pages Directory	*no option*	

11.3 PWP Integration Profile Process Flow

The Personnel White Pages Profile addresses the following use cases:

- A Clinical user logs into an acquisition device that is acting as a Personnel White Pages Consumer. The clinical application queries the DNS Server Actor using [ITI-23] to find the Personnel White Pages Directory. The clinical application then queries [ITI-24] the Personnel White Pages Directory using the user's username and displays the user's full name with First Name, Middle, and Last. There are information fields to support both European and Asian naming conventions.

- The Clinical user acquires clinical data. The application queries [ITI-24] the Personnel White Pages Directory for the user's demographics to include the user's organization identification to embed in the data record.

- The User then needs to send this report by means of email to a colleague. The application allows the user to search [ITI-24] the Personnel White Pages Directory for the destination user, and selects the destination user's email address.

- The User reviews an existing clinical report and finds initials have been recorded in the report. The user system does a query [ITI-24] of the Personnel White Pages Directory for the initials found in the report and the system displays the displayable name(s).

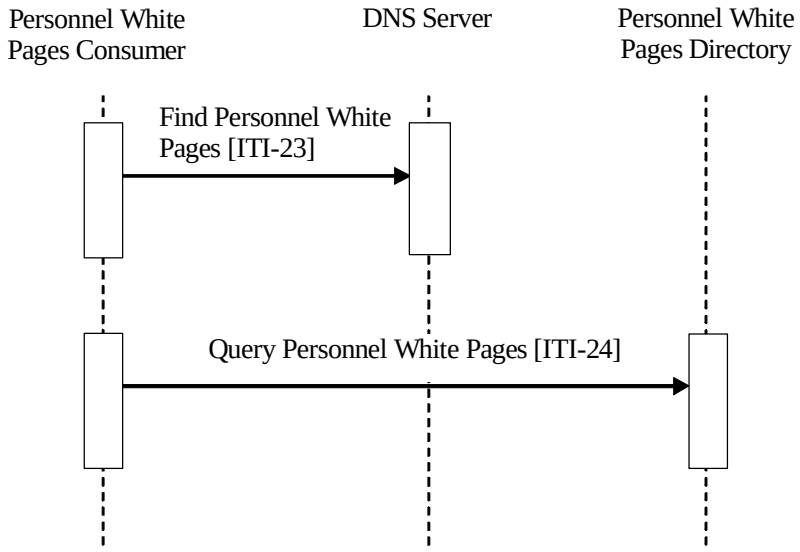


Figure 11.2-1: Basic Process Flow in PWP Profile

Appendix A: Actor Descriptions

Actors are information systems or components of information systems that produce, manage, or act on information associated with operational activities in the enterprise. The following are definitions of actors used in the IHE IT Infrastructure Integration Profiles:

Audit Repository – This actor provides a repository for audit events. IHE does not specify what analysis and reporting features should be implemented for an audit repository.

Client Authentication Agent – Provides local management of user authentication.

Context Manager – This actor serves as a broker for the communication between two or more context participant actors (either Patient Context Participant or User Context Participant). It supports the passing of the user and patient subjects.

Display – A system that can request specific information or documents from an Information Source and display them.

Document Source - 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.

Document Consumer - 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.

Document Registry - 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.

Document Repository - 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 URI to documents for subsequent retrieval by a Document Consumer.

DNS Server – This actor has authoritative location information.

Information Source – A system that responds to requests for specific information or documents and returns ready for presentation information to be displays on the requesting actor.

Kerberos Authentication Server – Provides central authentication of enterprise users.

Kerberized Server – Receives user authentication information for further use by the service that contains this actor

Patient Context Participant – This actor participates in a shared context environment by both setting the patient context and responding to context changes as communicated by the Context Manager Actor. This actor shall respond to all patient context changes.

This actor shall set the patient context, if the application containing this actor has patient selection capability.

Patient Demographics Consumer – This actor allows a user to associate information with a patient at the point of care.

Patient Demographics Supplier – A repository of patient information that can be searched on demographic or visit-related fields.

Patient Identifier Cross-reference Consumer – This actor allows a system in a Patient Identifier Domain to determine the identification of a patient in a different Patient Identifier Domain by using the services of a Patient Identifier Cross-Reference Manager Actor.

Patient Identifier Cross-reference Manager – Serves a well-defined set of Patient Identifier Domains. Based on information provided in each Patient Identifier Domain by a Patient Identification Source Actor, it manages the cross-referencing of patient identifiers across Patient Identifier Domains.

Patient Identity Source – - The Patient Identity Source Actor is a provider of unique identifier for each patient and maintains a collection of identity traits. Each Patient Identifier Domain requires this Actor to assign patient identities and to notify other Actors (e.g. a Patient Identifier Cross-reference Manager or a Registry Actor) of all events related to patient identification (creation, update, merge, etc.). **Personnel White Pages Consumer** – This actor has a use for information that can be found in the Personnel White Pages Directory.

Personnel White Pages Directory – This actor has authoritative Personnel White Pages information on the human workforce members of the enterprise.

Secure Node – The presence of this actor on a system means that all of the other actors and other non-IHE software complies with the IHE rules for user authentication, communications authentication, and security policies.

Time Client – Establishes time synchronization with one or more Time Servers using the NTP protocol and either the NTP or SNTP algorithms. Maintains the local computer system clock synchronization with UTC based on synchronization with the Time Servers.

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

User Context Participant - Receives notification of user context changes and follows them for the application that contains it.

Appendix B: Transaction Descriptions

Transactions are interactions between actors that transfer the required information through standards-based messages. The following are brief descriptions of the transactions defined by IHE.

1. **Maintain Time:** NTP transactions used to maintain time synchronization.
2. **Get User Authentication:** The Client Authentication Agent requests user authentication from the Kerberos Authentication Server. When the user is authenticated, the Kerberos Authentication Server returns a Ticket Granting Ticket (TGT) to optimize future activity.
3. **Get Service Ticket:** Obtain a ticket using Kerberos protocol for use with a service.
4. **Kerberized Communication:** The Kerberized Communication transaction is an aspect of the connection between a local client and a remote server.
5. **Join Context**: Allows a Context Participant Actor to locate and establish communication with the Context Manager Actor.
6. **Change Context:** Includes all messages required to initiate and finalize a context change transaction:
   - Initiation of a context change request from the instigating participant actor
   - Delivery of survey results to instigating actor and display of associated replies
   - Communication of context change decision to the Context Manager Actor
7. **Leave Context**: Allows Context Participant Actor to notify the Context manager Actor that it is breaking off communication.
8. **Patient Identity Feed**: Allows a Patient Identity Source Actor to notify a Patient Identifier Cross-Reference Manager Actor of all events related to patient identification (creation, update, merge, etc.).
9. **PIX Query**: This transaction allows a Patient Identifier Cross-reference Consumer to find out the identification of a patient in different Patient Identifier Domains by using the services of a Patient Identifier Cross-reference Manager Actor.
10. **PIX Update Notification:** Allows a Patient Identifier Cross-reference Consumer to be notified by the Patient Identifier Cross-reference Manager Actor of changes to the identification of all patients in Patient Identifier Domains the Consumer is interested in.
11. **Retrieve Specific Information for Display:** A request issued by a display system for specific information related to a patient returned in a ready for presentation information format.
12. **Retrieve Document for Display:** A display system requests an instance of a uniquely identified persistent document under custodianship by an information source and receives its content ready for presentation.

13. **Follow Context:** Accounts for all messages required to propagate a context change to a responding participant actor:
    - Survey of all other Context Participant Actors by the Context Manager Actor and display by the instigating Participant Actor of any associated replies
    - Notification of context change result from the Context manager Actor to the Context Participant Actors
    - Retrieval of the context data by the Context Participant Actors
14. Provide and Register Document Set

    A Document Source Actor initiates the Provide and Register Document Set Transaction. For each document in the submitted set, the Document Source Actor provides both the documents as an opaque octet stream and the corresponding metadata to the Document Repository. The Document Repository is responsible to persistently store these documents, and to register them in the Document Registry using the Register Documents transaction by forwarding the document metadata received from the Document Source Actor.
15. Register Document Set

    A Document Repository Actor initiates the Register Document Set transaction. This transaction allows a Document Repository Actor to register one or more documents with a Document Registry, by supplying metadata about each document to be registered. This document metadata will be used to create an XDS Document Entry in the registry. The Document Registry Actor ensures that document metadata is valid before allowing documents to be registered. If one or more documents fail the metadata validation, the Register Document Set transaction fails as a whole.
16. Query Registry

    The Query Registry transaction is issued by the Document Consumer Actor on behalf of a care provider (EHR-CR) to a Document Registry. The Document Registry Actor searches the registry to locate documents that meet the provider's specified query criteria. It will return a list of document entries that contain metadata found to meet the specified criteria including the locations and identifier of each corresponding document in one or more Document Repositories.
17. Retrieve Document

    A Document Consumer Actor initiates the Retrieve Document transaction. The Document Repository will return the document that was specified by the Document Consumer.
18. **Intentionally Left Blank**
19. **Node Authentication:** This transaction is embedded within all network communications activity. All DICOM, HL7, and HTML connections shall comply with the IHE specification for bi-directional authentication and authorization of

communications of Protected Healthcare Information (PHI). IHE does not specify how other protocols that transfer PHI shall perform bi-directional authentication and authorization, but requires that other protocols perform such authentication and authorization.

20. **Record Audit Event**: The delivery of an audit event description from any secure node to the Audit Repository.
21. **Patient Demographics Query**: Look up and return patient demographic information in a single patient demographics source, based upon matches with full or partial demographic information entered by the user.
22. **Patient Demographics and Visit Query:** Look up and return patient demographic and visit information in a single patient demographics source, based upon matches with full or partial demographic/visit information entered by the user.
23. **Find Personnel White Pages:** This transaction will find the LDAP Directory by querying the DNS.
24. **Query Personnel White Pages:** This transaction provides for read-only access to the Personnel White Pages directory.

Appendix C: IHE Integration Statements

IHE Integration Statements are documents prepared and published by vendors to describe the conformance of their products with the IHE Technical Framework. They identify the specific IHE capabilities a given product supports in terms of IHE actors and integration profiles (described in ITI TF-1: 2).

Users familiar with these concepts can use Integration Statements to determine what level of integration a vendor asserts a product supports with complementary systems and what clinical and operational benefits such integration might provide. Integration Statements are intended to be used in conjunction with statements of conformance to specific standards (e.g. HL7, IETF, DICOM, W3C, etc.).

IHE provides a process for vendors to test their implementations of IHE actors and integration profiles. The IHE testing process, culminating in a multi-party interactive testing event called the Connect-a-thon, provides vendors with valuable feedback and provides a baseline indication of the conformance of their implementations. The process is not intended to independently evaluate, or ensure, product compliance. In publishing the results of the Connect-a-thon and facilitating access to vendors' IHE Integration Statements, IHE and its sponsoring organizations are in no way attesting to the accuracy or validity of any vendor's IHE Integration Statements or any other claims by vendors regarding their products.

IMPORTANT -- PLEASE NOTE: Vendors have sole responsibility for the accuracy and validity of their IHE Integration Statements. Vendors' Integration Statements are made available through IHE simply for consideration by parties seeking information about the integration capabilities of particular products. IHE and its sponsoring organizations have not evaluated or approved any IHE Integration Statement or any related product, and IHE and its sponsoring organizations shall have no liability or responsibility to any party for any claims or damages, whether direct, indirect, incidental or consequential, including but not limited to business interruption and loss of revenue, arising from any use of, or reliance upon, any IHE Integration Statement.

C.1 Structure and Content of an IHE Integration Statement

An IHE Integration Statement for a product shall include:

1. The Vendor Name
2. The Product Name (as used in the commercial context) to which the IHE Integration Statement applies.
3. The Product Version to which the IHE Integration Statement applies.
4. A publication date and optionally a revision designation for the IHE Integration Statement.
5. The following statement: “This product implements all transactions required in the IHE Technical Framework to support the IHE Integration Profiles, Actors and Options listed below:”
6. A list of IHE Integration Profiles supported by the product and, for each Integration Profile, a list of IHE Actors supported. For each integration profile/actor combination, one or more of the options defined in the IHE Technical Framework may also be stated. Profiles, Actors and Options shall use the names defined by the IHE Technical Framework Volume I. (Note: The vendor may also elect to indicate the version number of the Technical Framework referenced for each Integration Profile.)

Note that implementation of the integration profile implies implementation of all required transactions for an actor as well as selected options.

The statement shall also include references and/or internet links to the following information:

7. Specific internet address (or universal resource locator [URL]) where the vendor’s Integration Statements are posted
8. URL where the vendor’s standards conformance statements (e.g., HL7, DICOM, etc.) relevant to the IHE transactions implemented by the product are posted.
9. URL of the IHE Initiative’s web page for general IHE information www.himss.org/ihe.

An IHE Integration Statement is not intended to promote or advertise aspects of a product not directly related to its implementation of IHE capabilities.

C.2 Format of an IHE Integration Statement

Each Integration Statement shall follow the format shown below. Vendors may add a cover page and any necessary additional information in accordance with their product documentation policies.

2505

IHE Integration Statement		**Date**	**12 Oct 2003**
Vendor	**Product Name**	**Version**	
Any Medical Systems Co.	IntegrateRecord	V2.3	
This product implements all transactions required in the IHE Technical Framework to support the IHE Integration Profiles, Actors and Options listed below:			
Integration Profiles Implemented	**Actors Implemented**	**Options Implemented**	
Retrieve Information for Display	Information Source	none	
Enterprise User Authentication	Kerberized Server	none	
Patient Identity Cross-referencing	Patient Identifier Cross-reference Consumer	PIX Update Notification	
Internet address for vendor's IHE information:	www.anymedicalsystemsco.com/ihe		
Links to Standards Conformance Statements for the Implementation			
HL7	www.anymedicalsystemsco.com/hl7		
Links to general information on IHE			
In North America: www.himss.org/ihe	In Europe: www.ihe-europe.org	In Japan: www.jira-net.or.jp/ihe-j	

Appendix D: User Authentication Techniques - Passwords, Biometrics, and Tokens

Authentication techniques are based on one or more of three factors: Something you know, something you are, or something you have. There are many different authentication techniques in use today. The technologies supporting these techniques are not well standardized. There are also excellent security reasons to avoid specifying any single set of technologies for authentication use.

The Kerberos protocol was originally defined to work with any user authentication technique. Kerberos has been shown to support a wide variety of authentication technologies. These include various forms of tokens and biometric technologies. Specific implementations of these technologies often include proprietary components. There is often a pair of proprietary components added – one at the user workstation and a matching component at the authentication server. Once the user authentication is complete, the subsequent Kerberos transactions are the same.

These extensions are not yet standardized. The IHE specification for the use of Kerberos does not prevent the use of these extensions at a specific site, nor does it ensure that the extensions will work.

The Kerberos system specified for the Enterprise User Authentication utilizes a challenge response system together with a username and password system to authenticate the user. The minimal support of passwords provides a standardized baseline for the IHE “Enterprise User Authentication”. Kerberos enables enforcement of a central password policy which facilitates stronger passwords. Such password policies are beyond the scope of IHE. Kerberos does not prevent the use of weak passwords. The password strength policy must be chosen and enforced by the site security administration.

Appendix E: Cross Profile Considerations

E.1 Combined use of RID, EUA and PIX Integration Profiles

When used alone, the Retrieve Information for Display Integration Profile assumes that the Patient Identifier Domain is the same for both the Display and the Information Source Actors. Furthermore, any user authentication on the Information Source is not addressed explicitly. This Appendix discusses combination of the Retrieve Information for Display Integration Profile with other IHE Integration Profiles to address these two problems.

When used in conjunction with the Patient Identifier Cross-referencing Integration Profile, implementations of the Retrieve Information for Display Integration Profile shall take into account that the Information Source Actor may need to map Patient IDs from different identifier domains to the one used in its own domain. The combined use of these Integration Profiles is achieved by grouping the Information Source and the Patient Identifier Cross-reference Consumer Actors. This is depicted in Figure E-1.

Similarly, the Information Source Actor may perform certain access control functions based on the requesting user authentication performed by the actors implementing the Enterprise User Authentication Integration Profile. The combined use of these Integration Profiles is achieved by grouping the Display Actor with the Client Authentication Agent Actor and the Information Source Actor with the Kerberized Server Actor. This is also shown in Figure E-1.

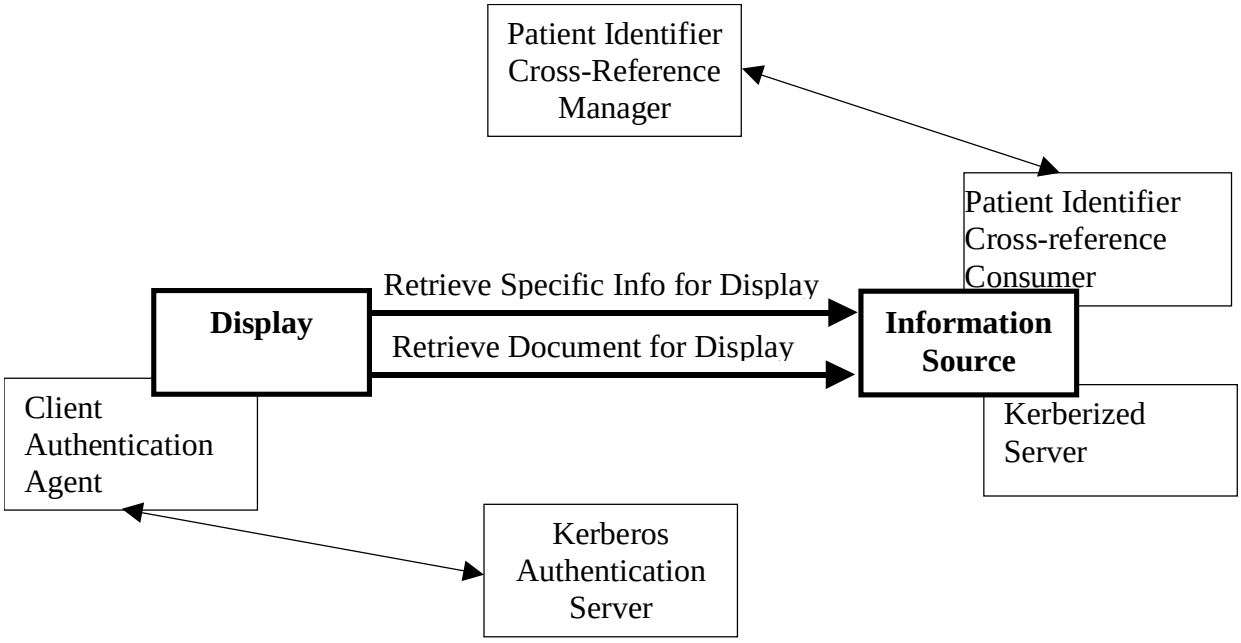


Figure E-1. Combined use of actors implementing multiple Integration Profiles

E.2 XDS Integration with RID

The RID Retrieve Document for Display transaction [ITI-12] is compatible with the XDS Retrieve Document transaction [ITI-17]. Thus, an RID Information Source implementing the Retrieve Document for Display transaction can be used to implement the XDS Retrieve Document transaction. In this instance, the RID Information Source must be a secure node [see ATNA].

E.3 XDS Integration with PIX

All Patient IDs managed in the XDS transactions (either in XAD-Pid Domain or in an EHR-CR Domain) shall include the related Patient Domain ID (OID of the Assigning Authority) associated with the patient ID. It is recommended that this unambiguous patient identification be used with Patient IDs within the Documents also.

Because XDS is Document content neutral, there is no verification by the XDS Repository that the Patient IDs included inside the documents are consistent with the patient IDs managed by the Registry in the document entry related to that document.

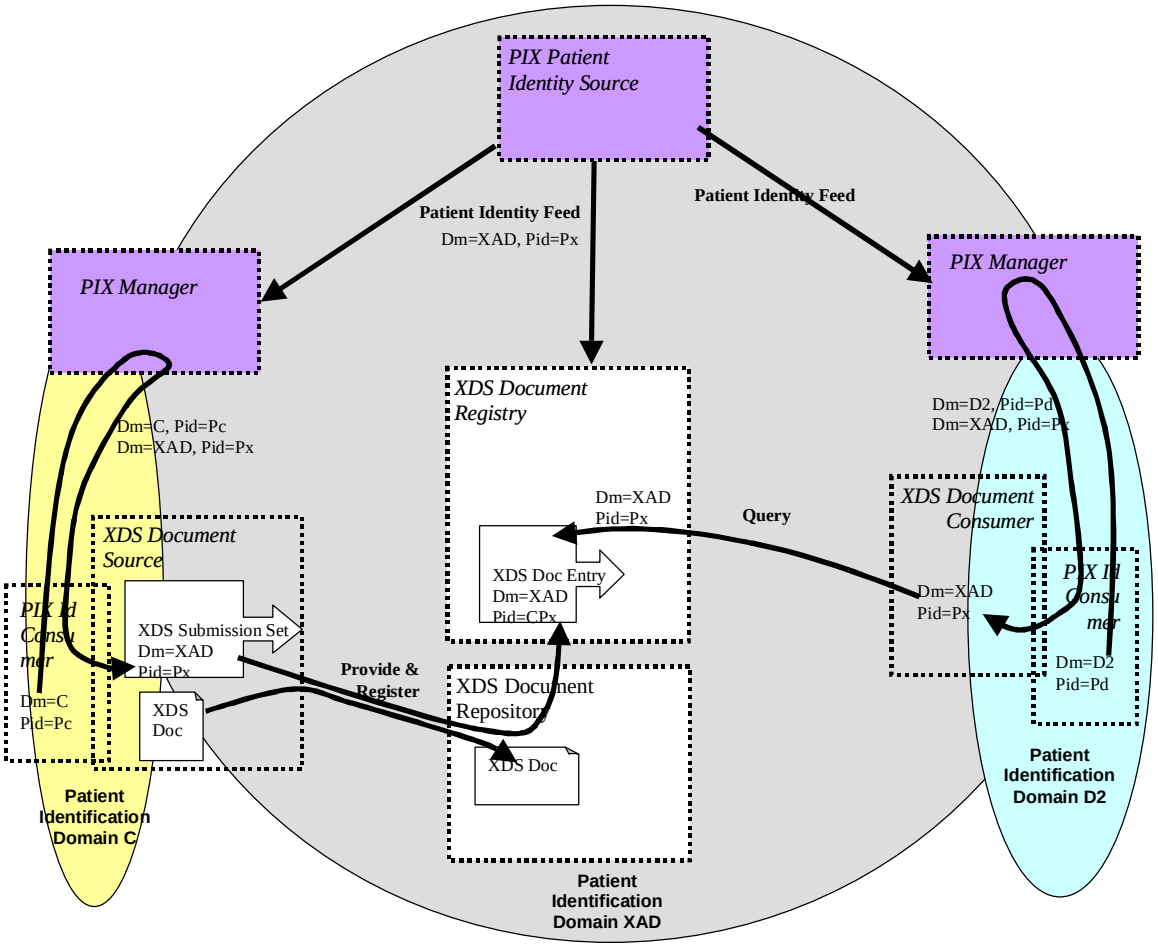


Figure E.3-1 Affinity Domain with patient ID cross-referencing with IHE PIX Managers

Figure E.3-1 depicts an example of a Affinity Domain with a Patient Identifier Domain (called XAD) and two EHR-CRs where the cross-referencing is performed by Patient Identifier Cross Referencing Managers internal to both the Document Source and the Document Consumer Domains (called C and D2 respectively).

A Document Source may choose to perform the cross-referencing of its own patient IDs in that of the XAD-Pid Domain by leveraging the IHE PIX Integration Profile (See Figure). The Patient ID Feed Transaction from the XAD Patient ID Source may be used to provide input to the Patient Identifier Cross-Referencing Manager used by the Document Source. The PIX manager may either be internal to the EHR-CRs or be shared across the XDS Affinity Domain.

E.4 XDS Integration with PWP

The XDS Document Source Actor in the XDS Integration Profile may choose to utilize the PWP Query Personnel White Pages [ITI-24] transaction to obtain information needed to fill the authorPerson and legalAuthenticatorName fields for the XDS Register Document Set [ITI-14] and Provide & Register Document Set [ITI-15] transactions.

The Personnel White Pages transaction defines, in ITI-TF 2:3.24.4.1.2.3.1, a "cn" attribute with "lang-x-ihe" that contains the information in the HL7 XCN (extended composite ID number and name for persons) format for personal information. These fields are optional in the PWP Integration Profile. A care delivery organization may choose to populate these fields in their Personnel White Pages Directory and utilize the ITI-24 transaction to support its XDS activities. This is not a required dependency, but is a possible reason to group a Document Source Actor with a Personnel White Pages Consumer Actor.

The PWP Integration Profile only provides the personnel information. Organizational information must be obtained via other means, e.g. extending the LDAP directory with organizational objects.

E.5 XDS Integration with PDQ

The Patient Demographics Query (PDQ) Integration Profile may be used in conjunction with the XDS Integration Profile to provide a lookup for XDS Affinity Domain Patient Identifiers to XDS Document Consumer and Document Source Actor. In this case a Patient Demographics Supplier Actor needs to be grouped with the XDS Patient Identifier Source Actor on one hand, and on the other hand a Patient Demographics Consumer Actor needs to be grouped with the Document Source/Consumer where one may want to query based on local patient traits and obtain a pick-list of candidate Patient Ids in the XAD Patient Identifier Domain. This offers a simpler solution that the use of the PIX Integration Profile.

Appendix F: Request to Standards Development Organizations

The following requests have been made to standards development organizations. They are now under development. These extensions to standards will allow addition of new integration profiles or combination of integration profiles. **HL7**

- Kerberization of HL7 version 2 messaging
- Support for Kerberized CCOW Context Participants

DICOM

- Addition of SOP class for Kerberization of DICOM messages

Appendix G: Security Considerations

G.1 Cross Profile Considerations

IHE compliant systems usually process private healthcare information. This is subject to national privacy regulations, and possibly other state and contractual requirements. The IHE Infrastructure profiles do not fully define the security mechanisms necessary to protect this information. The Enterprise User Authentication profile provides one component of this solution.

IHE assumes that actors will be installed on nodes with the following characteristics:

- Each node has a security policy and procedure that applies to its operation. This is assumed to be part of the healthcare enterprise security policy.
- Any user (human, or application process) external to the node boundaries is submitted to an access control procedure in which the user/application will be authenticated.
- All required audit trail events are captured and recorded.

The profiles in this framework assume the following environment:

- Physical Security Environment
  - The equipment is assumed to be located in a physically protected and actively monitored area. This is normally the case with modality equipment because of other patient safety, privacy, and operational concerns. Similarly, the HIS systems and various archives are normally protected. Equipment like PACS workstations is sometimes placed in unprotected areas, but it is usually located where hospital staff monitors and limit access. It assumes that the threat of equipment modification is protected against by means of the physical security mechanisms.
  - The network equipment that connects the computers is also assumed to be physically protected against unauthorized connections and unauthorized modifications. In the treatment areas of most hospitals the network equipment is in ceilings, cableways, locked cabinets, and other protected areas. There is usually staff present to monitor that no unauthorized activity is taking place.
  - Local procedures and operations will be in place to ensure that the physical security assumptions are valid for other areas of the hospital, such as administrative offices, that may be at greater risk.
  - Remote locations, especially home offices, are not physically protected. Other means will be used to provide equivalent protection. This may include the use of technology such as VPN connections or HTTPS encryption. Use of encryption or VPN is not a complete replacement for physical security but may be part of an overall protection system.
  - The home computer that is used for both personal and professional purposes is difficult to protect. It will be protected from inadvertent modification by malicious software or its use will be prohibited.
- Network Security Environment

- In addition to the physical security of the network, there will be protection against network access by unsupervised systems. This is typically provided by mechanisms such as firewalls and VPNs.

The threat profile is assumed to be:

- Accidental and inadvertent misuse
- Individual abuse for personal gain, malice, revenge, or curiosity. The abusers are assumed to have only limited access to the underlying systems and software. They are not expert at the internal structure of the systems.
- Random untargeted abuse, such as from an Internet hacker.

The threat profile also assumes that the following threats are either not present or otherwise protected.

- Individual abuse by a system administrator, system developer, or other expert.
- Military or hostile government action
- Organized criminal attack

IHE addresses only those security requirements related to IT systems within the scope of IHE healthcare applications. It does not address security requirements for defending against network attacks, virus infection, etc.

IHE does not mandate the use of encryption because the performance impact of current encryption algorithms is excessive. Most hospital networks provide adequate security through physical and procedural mechanisms. The additional performance penalty for encryption is not justified for these networks. The profiles permit the use of encryption so that it can be used as part of an overall security plan.

G.2 XDS Security Considerations

Security and privacy

Coordinating the security and privacy policies of all the care delivery organizations in an Affinity Domain may be a challenge. An agreement is needed on security procedures, goals, auditing, record keeping, etc. This can result in changes to other enterprise policies, such as human resources procedures. Affinity Domain members are delegating full access to their published data to the other members of the Affinity Domain. This relationship requires a close ongoing partnership that ensures ongoing maintenance of policies, procedures, and activities. If laws change, relevant policies must be adjusted throughout the group. Corporate changes to group members affect the policies. Security events must be managed as a group. This must be managed as a long-term activity, not a one-time event.

Particular problem areas are likely to be:

- Authorized access and modification policies. The details of access policies are likely to have enterprise differences and conflicts that must be resolved. The Affinity Domain

relationships also introduce new policy requirements. For example, changes to employment (e.g. employee hiring and firing) must now include suitably rapid notifications to other Affinity Domain members. Changes to privacy restrictions (e.g. divorces) now require full Affinity Domain notifications, not merely enterprise notifications.

- Audit trail and access record keeping are often quite sensitive internal enterprise activities that must now be appropriately coordinated with the full Affinity Domain.
- Changes to laws and regulations now affect not only the policies of the individual enterprises; they also must be reflected in the Affinity Domain relationship contracts, policies, and procedures.
- Patient access and patient identity management. Patients usually have insecure computers. Patients often object to security procedures.
- Transborder communication of Personal Health Information (PHI) often presents legal and regulatory issues.

ITI TF-2: Appendix J in volume II goes into more detail listing many of the threats, objectives, policies, and mitigations that need to be coordinated among Affinity Domain members.

The XDS Integration Profile for two main reasons does not prescribe such Security and Privacy policies. First, it is clear that the broad range of possible solutions to these policies that will depend on the legal framework and the types of healthcare system, calls for XDS to be offer such flexibility. Decisions in this domain will have some impact on the implementations of XDS Actors, but it is expected that these will be minimal.

Appendix H: Intentionally Left Blank

Appendix I: Intentionally Left Blank

Appendix J: Content and Format of XDS Documents

The XDS Integration Profile purposely leaves a number of policies up to the XDS Affinity Domain to decide, including the structure and format of the content of XDS Documents to be shared, the mapping of content metadata into the XDS Document Registry, the coding of XDS Document metadata, the events that trigger an XDS Submission Request, and the policies concerning the use of XDS Folders to facilitate sharing.

It is important to recognize that until sufficient experience has been gained in cross-enterprise document sharing, it is not possible to establish common or even best practices in the use of the XDS Integration Profile. IHE has therefore chosen to abstain to make recommendations in these topics at this time.

IHE also recognizes that there will be a need for content-oriented integration profiles to be used in cooperation with this Integration Profile. It is expected that in the future the various IHE Domains (Patient Care Coordination, Cardiology, Laboratory, Radiology, IT Infrastructure, etc.) will produce IHE Integration Profiles refining the use of XDS within the domain. These various content-oriented integration profiles may rely on XDS, but would further constrain the forms of documents to be shared, or the uses of XDS features such as Folders and Submission Sets, et cetera.

Content Neutrality

XDS is content neutral. It neither prescribes nor prohibits the format, content, structure or representation of documents that can be retrieved from an XDS Document Repository. For the XDS Integration Profile to have immediate value to an Affinity Domain, it must be able to adapt to the documents that are present and available from its members. Thus, prohibitions on content would only serve to limit the utility and adoption of the XDS Integration Profile. Similarly, Clinical Affinity Domains must be able to adapt to emerging standards, which cannot be enumerated in any list of prescribed content formats.

IHE strongly recommends that XDS Affinity Domains adopt rules that require documents to comply with widely accepted standards where possible (*e.g.*, HL7 CDA, CEN ENV 13606, ASTM CCR, DICOM Composite Object).

Document Headers and Metadata

Because XDS is content neutral, XDS cannot validate metadata contained within the body of an XDS document against the metadata supplied to the XDS Document Registry. XDS Affinity shall therefore select content where IHE has defined Integration Profiles, or until that point, the Affinity Domains shall carefully define how the attributes in the XDS Document Registry are filled.

Metadata and the Patient Record

Although metadata in the document header may be duplicated in the XDS Document Registry, the XDS Document Registry metadata has a particular role in term of being part of the legal medical record stored. It is definitively not part of the clinical record as managed by the XDS Document Repositories where documents reside. Furthermore, XDS does not provide for transactions to "sign" or legally authenticate the content of an XDS Submission Set (See IHE Document Digital Signature Content Profile- DSG), although it offers the ability to track its author, if the Affinity so desires to enforce it. The contents of XDS Folders are tracked, through the Submission Sets that contributed to placing document references in folders. However, the existence of document metadata in the registry and the potential medical acts involved in creating an XDS Submission Set or XDS Folder may make the contents of the XDS Document Registry part of the patient's legal medical record. It will be up to individual XDS Affinity Domains to decide how to address the issues involved with these clinical acts and to resolve them in accord with common sense, acceptable medical practices, and local regulations.

Appendix K: XDS Concept Details

K.1 XDS Document Concept

An XDS Document is the smallest unit of information that may be provided to a Document Repository Actor and be registered as an entry in the Document Registry Actor.

An XDS Document is a composition of clinical information that contains observations and services for the purpose of exchange with the following characteristics: Persistence, Stewardship, Potential for Authentication, and Wholeness. These characteristics are defined in the HL7 Clinical Document Architecture Release 1 specification.

An XDS Document may be human and/or application readable. In either cases, it shall comply with a published standard defining its structure, content and encoding. IHE intends to define content-oriented Integration Profiles relying on such content standards to be used in conjunction with XDS.

Furthermore:

1. When submitted for sharing, an XDS Document shall be provided to the Document Repository Actor as an octet stream with an associated MIME type.

2. When retrieved through the Retrieve Document transaction, an XDS Document shall be unchanged from the octet stream that was submitted (full fidelity repository).

   Note: An XDS Document may be a MIME multipart document (e.g. an HL7 CDA as its first part followed by attachments as files). The first part of the multi-part contains the primary part of the document, other parts are direct attachments to the primary part. The Document Repository handles this multi-part data set as an "opaque entity". The Document Repository does not need to analyze or process its multi-part structure nor the content of any parts in the context of the XDS Integration Profile.

   Note: An XDS Document may be retrieved using alternate methods using document specific retrieval methods. Such optional capabilities are not provided in the current specification of XDS, but are possibly candidates for addition as future options this Integration Profile.

3. An XDS Document shall be associated with metadata defined by the Document Source. This metadata information shall be placed by the XDS Registry Actor in an XDS Document Entry, and is used for query purposes by XDS Consumer Actors.

4. The XDS Integration Profile manages XDS Documents as a single unit of information, it does not provide mechanisms to access portions of an XDS Document. Only the Document Sources or Document Consumers have access to the internal information of the XDS Document.

5. An XDS Document is globally uniquely identified, so that no two XDS Documents with different content shall bear the same Unique Identifier. This identifier is unique across all Clinical Affinity Domains, which allows potential merger of XDS Document Repositories from different domains, or exchange of XDS Documents between Clinical Affinitiy Domains, if so desired.

6. The XDS Document Registry Actor shall maintain a single document entry for each XDS Document stored in a Document Repository Actor. Duplicate copies of the same XDS Document (with the same unique identifier) may be stored and registered. Registration of an XDS Document with the same unique identifier but a different content is rejected.

7. This Integration Profile specifies the metadata required for each XDS document registered in the Document Registry. It is the responsibility of the Document Source to ensure that the XDS Document metadata reflects the actual content of the associated XDS Document. Neither the Document Repository nor the Document Registry checks this consistency.

8. The Document Source maintains the following responsibilities over the XDS Documents it has registered:

    a. It has rights to change the status of any of these Documents from "approved" to "deprecated" or to delete them outright.

    b. It has rights to submit an XDS Document with a "Parent Relationship" of replacement ("RPLC") for one of its previously submitted document[2].

    Clinical Affinity Domains should have policies and procedures to provide patient access to these operations where necessary. For example, in certain regions, patients may request the removal of documents from the EHR-LR. The Registry and Repositories implementations should be ready to support these local operations although there are no IHE transactions defined at this time.

K.2 Concept of an XDS Affinity Domain

An XDS Affinity Domain is made of a well-defined set of Document Repositories and Document Consumers that have agreed to share the clinical documents. An Affinity Domain has a number of properties defined:

1. An Affinity Domain does not deliver care. Only the EHR-CRs belonging to an XDS Affinity Domain as Document Sources and Consumers do.
2. An Affinity Domain is managed by a single Document Registry Actor.

[2] For example, in DICOM, where the document identity does not change even though its internal patient metadata may have been updated, the Document Source would submit an updated DICOM Document as a replacement for the existing one.

Note: A distributed registry approach will be considered as a future and separate Integration Profile. For Document Source and Document Consumer Actors, the perception of a single Document Registry Actor hides the complexity of a distributed registry.

3. It includes any number of Document Repository Actors (a distributed configuration is the default, however, a centralized configuration with a grouped Registry/Repository is also supported).
4. It contains an explicit list of Document Consumer and Document Repository actors that participate in document sharing. The addition of a Document Repository or Document Consumer Actor is an administrative task that requires involvement of authorities maintaining the Registry and Repositories.
5. There is a chain of trust established between the users (healthcare staff) in each EHR-CR and the Affinity Domain.
6. Document Repositories and Document Consumers may belong to more than one Affinity Domain and share the same or different documents. This is an implementation strategy and will not be further described.
7. The Affinity Domain supports a primary Patient Identification Domain that is used by the Document Source and Consumers to communicate with the Document Registry. When Document Sources and Consumers in the Affinity Domain belong to different Patient Identifier Registration Domains, the Document Source and Consumers must cross-reference their own Patient Identifier Registration Domains to that of the Registry. They may use the IHE Patient Identifier Cross-referencing Integration Profile, the IHE Patient Demographics Query Integration Profile or other Affinity Domain specific mechanisms for cross-referencing (See ITI TF-2 Appendix E Sections E.3 and E.5).
8. A Document Source may only contribute documents with Document Codes and Health Facility Codes that draw from a Vocabulary Value Set that is approved by the Affinity Domain.

K.3 Other Principles of XDS

The XDS Integration Profile has been designed with the following limitations and principles:

1. A Document may contain references to other documents in its content which are not under the management of the XDS Document Registry. Such references may be available to the EHR-CR that registered the document that includes the reference. It is beyond the scope of XDS to provide access to such documents internal to the EHR-CR.
2. The XDS Repositories are not expected to perform any processing or translations on document content. Processing and translation are the responsibility of a Source EHR-CR or Consumer EHR-CR. The analysis, cross-document combination and presentation of document content is outside the scope of the XDS Integration Profile and its actors.
3. The custodianship for the clinical information contained in a registered document remains with the Source Actor of the EHR-CR. The EHR-LR offers only a “shared space” under the responsibility of each contributing EHR-CR. Through XDS,

replacement or deletion of documents in the EHR-LR may only be initiated by the corresponding EHR-CR Source.

4. When an XDS Document that has already been registered in the XDS Registry of a Clinical Affinity Domain is resubmitted as if it was a new XDS Document with the same Document Unique identifier, this "duplicate submission" is detected by the Repository and/or Registry based on the fact that the XDS Document Unique Identifier already exists in a Document Entry. The submission request to which that resubmitted Document belongs shall be rejected in the case where the identifiers match but the actual content differs (detected by use of a hash key computed by the Document Repository at the time of submission).

K.4 Document Identification

In order to reduce the number of unique identifiers associated with an XDS Document, the globally unique Document Id assigned by the document source and the unique XDS Document Id used by the Repository are the same. It is strongly recommended to limit the use of the Document Entry UUID created per ebRS in order to reference the document entry for referencing internally to the encoding of the IHE transactions operations, and to encourage the use of the globally unique Document Id for all external operations (e.g. links maintained in data bases internal to the Document source Actor, links within documents, etc.).

The XDS Document Entry includes two separate attributes: an XDSDocument.uniqueId and XDSDocument.URI, a Universal Resource Identifier. The URI is a "self contained" web method that allows any Document Consumer to perform a Retrieve Document transaction (See ITI TF-2: Section 3.17). The Document Unique ID is a location independent identifier. As the result of XDS Document migration from one XDS Document Repository to another one within an Affinity Domain, the URI would be changed, but not the Document unique ID.

K.5 Example of Document Relationship

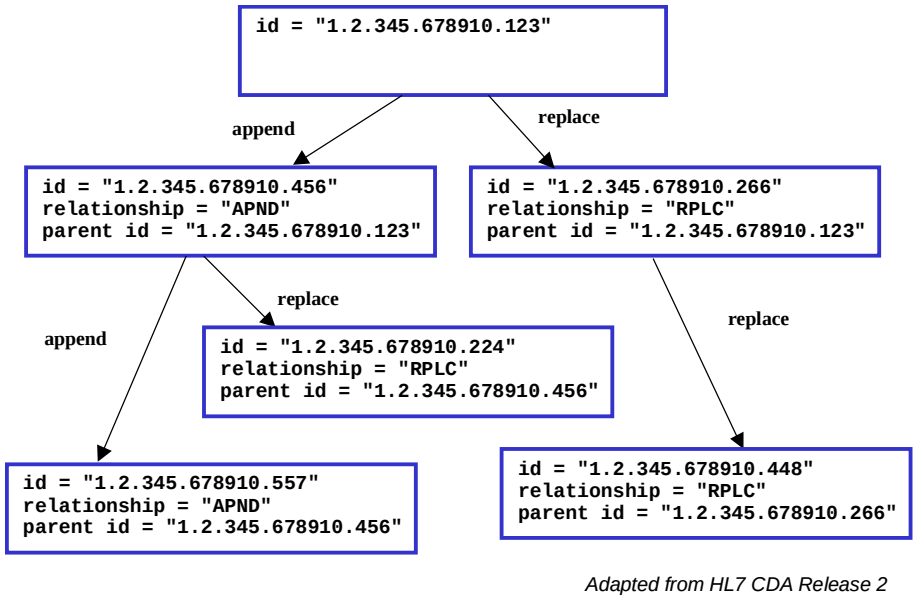


Figure 10.4.10-5 Example of Document Relationships

These relationships are illustrated in the above figure. Typical scenarios are a simple relacement (e.g. XDSDocument.id "1.2.345.678910.266" replacing XDSDocument.id "1.2.345.678910.123") and a simple addendum (e.g. XDSDocument.id "1.2.345.678910.456" appends XDSDocument.id "1.2.345.678910.123"). More complex scenarios that might be anticipated include:

1. Replacement of an addendum (e.g. XDSDocument.id "1.2.345.678910.224" replaces XDSDocument.id "1.2.345.678910.456", which itself is an addendum to XDSDocument.id "1.2.345.678910.123") - expected behavior would be to render the replacement as the addendum (e.g. render XDSDocument.id "1.2.345.678910.224" as the addendum to XDSDocument.id "1.2.345.678910.123");
2. Addendum to a replaced document (e.g. XDSDocument.id "1.2.345.678910.456" appends XDSDocument.id "1.2.345.678910.123", which has been replaced by XDSDocument.id "1.2.345.678910.266") - expected behavior would be to render the addendum along with the replacement (e.g. render XDSDocument.id "1.2.345.678910.456" as an addendum to XDSDocument.id "1.2.345.678910.266").

K.6 Off-Line transaction mode

Document Source Actors are allowed to be off-line part of the time, as in the case of a doctor's office system connected only by a dial-up line acting as a Document Source.

The Document Registry and Document Repositories should be designed to be on-line all the time (see note for exception).

Note: The Document Repository may be off-line also in the degenerate case of point-to-point e-mail transmission, where the affinity domain is made only of two systems; on one hand a document source and on the other a document repository grouped with the Document registry and Document Consumer (See ITI TF-1: 10;5 Strategy 3).

Information sent to off-line systems will be supported through Internet e-mail protocols. E-mail protocols provide mechanisms for sending acknowledgments:

(1) Delivery receipts from the end-user, and

(2) Delivery failure notices from intermediate store-and-forward SMTP servers.

When using e-mail protocols, the asynchronous nature of the acknowledgments, which are delivered by e-mail messages, requires that the Send and Acknowledge components of the transaction be separated into distinct messages.

Body of the e-mail message should contain a simple notice (in English/ASCII), fixed subject line, address should be used for automated processing. An attachment formatted in the local language should contain instructions. Transaction should be included in a separate attachment.

Appendix L: XDS Affinity Domain Definition Checklist

The concept of an XDS Affinity Domain is defined in ITI TF-1:10 and Appendix K. This informative appendix summarizes the key policies that need to be agreed to in order to deploy a EHR-LR document sharing environment.

L.1 Configuration of an XDS Affinity Domain

A number of systems implementing IHE Actors defined in the XDS Integration Profile need to be identified and configured to communicate. This includes defining addressing information and ATNA Secured Node certificate:

1. Identify the system that will support the Document Registry Actor.
2. Identify the systems that will support the Document Repository Actors.
3. Identify the systems that will support Document Source and/or Document Consumer Actors.

L.2 Patient Identification

Initialize the XDS Document Registry (See ITI TF-2:Appendix H) with the proper patient identification information:

1. Assign an Assigning Authority (OID) for the XDS Affinity Domain Patient Id Domain.
2. Assign an Assigning Authorities (OID) for the each one the Local Patient Id Domains in which the EHR-CR Document Source and/or Document Consumer operate.
3. Identify the system that will support the Patient Identity Source and if some of the systems that support Document Source and/or Document Consumer Actors also support a Patient Identity Cross-reference Manager (needs to receive a patient identity feed Transaction).

L.3 XDS Registry Related Vocabularies

Initialize the XDS Document Registry (See ITI TF-2:Appendix H) with the proper vocabulary information:

1. Select and initialize the XDS Document Registry as well as the Document Sources and/or Document Consumers with the vocabulary definitions specified in Registry Enforcement (ITI TF-2:3.14.4.1.2.9) where either the Coding Scheme or the Coding Scheme/Code Values are enforced.

L.4 Document Sharing Practice Policies

1. Define the care events and the corresponding expected level of information that is expected to be shared within the EHR-LR.
2. Define the usage policies for XDS Folder (creation and update) in the selected care pathways supported.

L.5 XDS Document Content

1. For each Document Format Code Value, establish the necessary interoperability agreements (e.g. by selecting IHE Document Content Profiles) to ensure that the Document Consumers may find (e.g. Document UniqueId structure) and process the XDS Documents content (e.g. MIME type, template definitions, archetypes, etc.) they retrieve from the XDS Repositories of the XDS Affinity Domain.

L.6 Document Update and Maintenance Policies

Document Sources are responsible for the on-going accuracy (custodianship) of the XDS Documents they have elected to shared in the EHR-LR supported by the Affinity Domain. This includes:

1. Replacement of documents in the EHR-LR
2. Cases and means to possibly delete documents in the EHR-LR

L.7 Security and Privacy Policies

1. Establish agreed policies and procedures among care delivery organizations in the Affinity Domain. In particular address security considerations in ITI TF-2:Appendix K.
2. Establish operational security infrastructure, including certificate exchange.
3. Maintain operational security infrastructure, configuration management, audit management, periodic inspections, etc.

Appendix M: Cross-Enterprise Document Sharing and IHE Roadmap

The IHE Cross-Enterprise Document Sharing Integration Profile is part of a family of IHE Integration Profiles grouped in a number of domain-specific Technical Frameworks Patient Care Coordination, Cardiology, Laboratory, Radiology, IT Infrastructure, etc.). XDS is a central foundation for Cross-Enterprise interoperability that may be combined with a number of the existing IHE Integration Profiles (See ITI TF-1:Appendix E). However a number of new IHE Integration Profiles need to be developed, pending the availability of the relevant base standards.

M.1 Document Content Integration Profiles for XDS

It is expected that the various IHE Domains (Cardiology, Laboratory, Radiology, IT Infrastructure, etc.) will produce new IHE Integration Profiles addressing the content of the documents that need to be shared. These various "content-oriented" Integration Profiles will rely on the XDS Integration Profile for managing the registration, discovery and access processes in a common manner.

Such an effort is underway with the IHE Patient Care Coordination Domain for medical summaries used in referrals and discharge summaries. See www.ihe.net.

M.2 Cross-Enterprise Dynamic Information Sharing

The management of dynamic information (non-document-oriented) such as allergy lists, medication lists, problem lists, etc is not addressed by XDS. However, a means to access this information in a structured form and to manage updates to such dynamic clinical information is a candidate for a specific Integration Profile.

M.3 Collaborative Workflow Process Management

There is a wide array of shared care delivery collaborative processes such as the placing and tracking of orders (e.g. drug prescriptions, radiology orders, etc.) for which XDS provides only a partial solution (the creation of the patient record with the resulting persistent artifacts). XDS offers a critical infrastructure for ePrescribing and eReferral in that it can ensure that the various providers share access to orders, prescriptions, dispensations, and results. The means to interoperate on the command/control part of these collaborative workflow processes is a candidate for specific Integration Profiles in the future.

M.4 Security and Privacy Management

The operation of any XDS Clinical 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 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 Authentication, Document Digital Signature, etc).

M.5 Federation of Affinity Domains

XDS is an effective means to establish Affinity Domains that include care delivery organizations at any level, local, regional or national. However, 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 transferring information from one Clinical Affinity Domain to another, or to allow access from one Affinity Domain to documents managed in other Affinity Domains. XDS has been designed with this extension in mind. An XDS Domains Federation Integration Profile that complements XDS may be anticipated in the future.

GLOSSARY

Actor: An entity within a use case diagram that can perform an action within a use case diagram. Possible actions are creation or consumption of a message

ADT: Admit, Discharge & Transfer.

CCOW: ANSI certified technology neutral specification for the Health Level Seven Context Management Architecture (CMA). This architecture enables multiple applications to be automatically coordinated and synchronized in clinically meaningful ways at the point of use. The architecture specified in this document establishes the basis for bringing interoperability among healthcare applications to point-of-use devices, such as a personal computer that serves as a clinical desktop

Context Management Registry: An HTTP technology specific service defined by the HL7 Context Management "CCOW" Standard to locate an instance of a context manager servicing a specific desktop.

Context Session: A collection of participant applications that are sharing context on one or more subjects.

CDA: Clinical Document Architecture (specified by HL7).

CT: Consistent Time Integration Profile.

Clinical Affinity Domain: A group of healthcare enterprises that have agreed to work together using a common set of policies and which share a common infrastructure of repositories and a registry.

Directory: A book containing the names and residences of the inhabitants of any place, or of classes of them; an address book; as, a business directory.

EHR-CR: An EHR-CR or Care-delivery Record abstracts the patient information managed by the IT system or set of systems of a Care Delivery Organization, which may support a broad variety of healthcare facilities: private practice, nursing home, ambulatory clinic, acute care in-patient facility, etc.

EHR-LR: The documents shared by the EHR-CR and tracked by the Registry form a Longitudinal Record for the patients that received care among the EHR-CRs of the Clinical Affinity Domain. This is known as the EHR-LR.

eMPI: Enterprise Master Patient Index.

EUA: Enterprise User Authentication Integration Profile.

Expected Actions: Actions which should occur as the result of a trigger event.

Globally Unique Identifier (GUID): An identifier of an entity, such as persistent document, that has been generated by an algorithm guaranteeing its global uniqueness.

HIMSS: Healthcare Information and Management Systems Society.

HIS: Hospital Information System.

IETF: Internet Engineering Task Force

IHE: Integrating the Healthcare Enterprise.

inetOrgPerson: The inetOrgPerson [RFC 2798] object class is a general purpose object class that holds attributes about people. The attributes it holds were chosen to accommodate information requirements found in typical Internet and Intranet directory service deployments. The inetOrgPerson object class is designed to be used within directory services based on the LDAP v3 [RFC 2251] and the X.500 family of protocols, and it should be useful in other contexts as well.

Interaction Diagram: A diagram that depicts data flow and sequencing of events.

IT: Information Technology.

JPEG: – Joint Photographic Experts Group.

KDC: Key Distribution Center (the Kerberos server that issues Ticket Granting Tickets and service tickets. See RFC1510).

LDAP: Lightweight Directory Access Protocol is designed to provide access to directories supporting the X.500 models, while not incurring the resource requirements of the X.500 Directory Access Protocol (DAP). This protocol is specifically targeted at management applications and browser applications that provide read/write interactive access to directories. When used with a directory supporting the X.500 protocols, it is intended to be a complement to the X.500 DAP.

Local Authentication: In the ATNA profile the term “local authentication” means that the user identification, authentication, and authorization method is chosen by the local system administration and does not necessarily comply with any IHE profile. It may be a local username password system, a secure token system, or any other system that is considered acceptable by the local security administration.

MPI: Master Patient Index.

MRN: Medicare Record Number.

NEMA: National Electrical Manufacturers Association.

NTP: Network Time Protocol. This is the standard Internet protocol for synchronizing computer clocks. The web site http://www.ntp.org provides extensive background documentation at the introductory and expert level on how to synchronize computers.

OID: Object Identifier. (See also 'Globally Unique Identifier’).

PACS: Picture Archive and Communication System.

Patient: (When used in the context of ATNA) RFC-3381 defines the means of identifying the person who is a patient. The patient information in audit event records corresponds to the information available to identify a patient at the time the audit record was generated, and does not reflect later updates (e.g. patient reconciliation).

PatientID: (When used in the context of ATNA) A free text that holds the system-internal patient identifier being unique within that system domain. The patient identifier domain is that assigned to the system that generated the audit event record. The patient information in audit event records corresponds to the information available to identify a patient at the time the audit record was generated, and does not reflect later updates (e.g. patient reconciliation).

Patient Identifier Cross-reference Domain: Consists of a set of Patient Identifier Domains known and managed by a Patient Identifier Cross-reference Manager Actor. The Patient Identifier Cross-reference Manager Actor is responsible for providing lists of "alias" identifiers from different Patient Identifier Domains.

Patient Identifier Domain: A single system or a set of interconnected systems that all share a common identification scheme for patients. Such a scheme includes: (1) a single identifier-issuing authority, (2) an assignment process of an identifier to a patient, (3) a permanent record of issued patient identifiers with associated traits, and (4) a maintenance process over time. The goal of Patient Identification is to reduce errors.

Patient Mapping Agent: The CCOW defined component that provides for the mapping of patient identifiers across disparate patient identity domains.

Patient Subject: The PSA defined subject that supports sharing the currently selected patient identifier amongst disparate applications running on the desktop.

PDF: Portable Document Format.

Personnel White Pages: Information on human workforce members within the authority of the PWP directory. This information has broad use among many clinical and non-clinical applications across the healthcare enterprise. The information can be used to enhance the clinical workflow (contact information), enhance the user interface (user friendly names and titles), and ensure identity.

PIX: Patient Identifier Cross-referencing Integration Profile.

PMA: Patient Mapping Agent component as defined by CCOW.

Process Flow Diagram: A graphical illustration of the flow of processes and interactions among the actors involved in a particular example.

PSA: Patient-Synchronized Applications Integration Profile.

RID: Retrieve Information for Display Integration Profile.

RIS: Radiology Information System.

Role: The actions of an actor in a use case.

RSNA: Radiological Society of North America.

Scope: A brief description of the transaction.

Secure Domain: A network, hardware systems, secure nodes, and physical environment for which a single set of security policies is defined and enforced for access to its addressable objects.

Secure Node: A network-addressable system that conforms to a secure domain's access policies and management. A secure node often supports IHE actors.

SNTP: Simple Network Time Protocol. This is a reduced accuracy version of NTP. The protocol fields are the same, but the data values and algorithms used are greatly reduced accuracy so that it can be implemented on limited capacity systems.

Submission Set: A set of XDS documents registered together to a Document Repository concerning information related to one care event of a single patient, provided by an EHR system.

SUID: The Study Instance UID from a DICOM SOP instance, or collection of SOP instances.

TGT: Ticket Granting Ticket. The initial credentials that verify that the user has been authenticated. It is used to avoid repeated user authentication events and as a token to request access to services.

Trigger Event: An event such as the reception of a message or completion of a process, which causes another action to occur.

UID: Unique Identifier (See also Globally Unique Identifier).

Universal ID: Unique identifier over time within the UID type. Each UID must belong to one of specifically enumerated species. Universal ID must follow syntactic rules of its scheme.

Use Case: A graphical depiction of the actors and operation of a system.

Username: A sequence of characters, different from a password, that is used as identification and is required when logging on to a multiuser computer system, LAN, bulletin board system, or online service. Also called user ID, or uid.

User Subject: The PSA defined subject that supports sharing the user identity of the currently logged in to the applications on the desktop.

UTC: Universal Coordinated Time. This is the replacement for GMT. It defines a reference time base that is internationally recognized and supported.

XDS Document: An XDS Document is the smallest unit of information that may be provided to a Document Repository and registered in a Document Registry. An XDS Document may contain 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, CCR), or may be made up of a mixture of the above types of content.

XDS Folder: An XDS Folder allows document sources to group the documents they submit with other related documents. What constitutes a Folder and the vocabulary associated with the specific Folders used by an EHR-CR is decided by an agreement between the care delivery organization members of a Clinical Affinity Domain.

