Integrating the Healthcare Enterprise

5

IT Infrastructure
Technical Framework

Volume 2
10
(ITI TF-2)
Transactions

15

Revision 5.0 – Final Text

December 12, 2008

20

Contents

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 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. 5.0 for Final Text, specifies the IHE transactions defined and implemented as of September 2008. 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

155   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
160   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. For example, the following IHE Technical Framework(s) are some of those which are available:

165
- IHE IT Infrastructure Technical Framework
- IHE Cardiology Technical Framework
- IHE Laboratory Technical Framework
- IHE Patient Care Coordination Technical Framework
- IHE Radiology Technical Framework

170   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 IT Infrastructure Technical Framework Volume II

The remainder of Section 1 further describes the general nature, purpose and function of the Technical Framework. Section 2 presents the conventions used in this volume to define IHE transactions.

175   Section 3 defines transactions in detail, specifying the roles for each Actor, the standards employed, the information exchanged, and in some cases, implementation options for the transaction.

The appendices following the main body of this volume provide technical details associated with the transactions.

1.3 Audience

180   The intended audience of this document is:
- IT departments of healthcare institutions
- Technical staff of vendors planning to participate in the IHE initiative
- Experts involved in standards development
- Those interested in integrating healthcare information systems and workflows

185 ## 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
190   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.

195 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

200 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

205 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

210 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

215 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.

220 ## 1.6 Comments

HIMSS and RSNA welcome comments on this document and the IHE initiative. They should be directed to:

Didi Davis
Senior Director IHE
225 230 East Ohio St., Suite 500
Chicago, IL USA 60611
Email: ihe@himss.org

1.7 Copyright Permission

Health Level Seven, Inc., has granted permission to the IHE to reproduce tables from the HL7 standard.
230 The HL7 tables in this document are copyrighted by Health Level Seven, Inc. All rights reserved. Material drawn from these documents is credited where used.

2   Conventions

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

2.1 The Generic IHE Transaction Model

Transaction descriptions are provided in Section 3. In each transaction description, the actors, the roles they play, and the transactions between them are presented as use cases.

The generic IHE transaction description includes the following components:

240   • Scope: a brief description of the transaction.

• Use case roles: textual definitions of the actors and their roles, with a simple diagram relating them, e.g.:
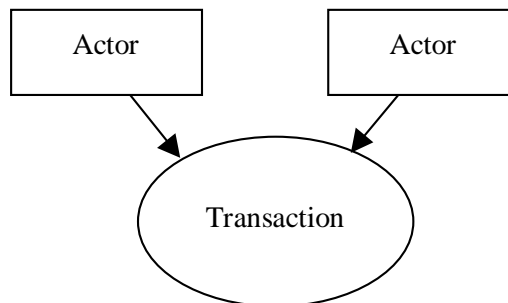
• *Referenced Standards*: the standards (stating the specific parts, chapters or sections thereof) to be
245   used for the transaction.

• *Interaction Diagram*: a graphical depiction of the actors and messages that support the transaction, with related processing within an Actor shown as a rectangle and time progressing downward, similar to:
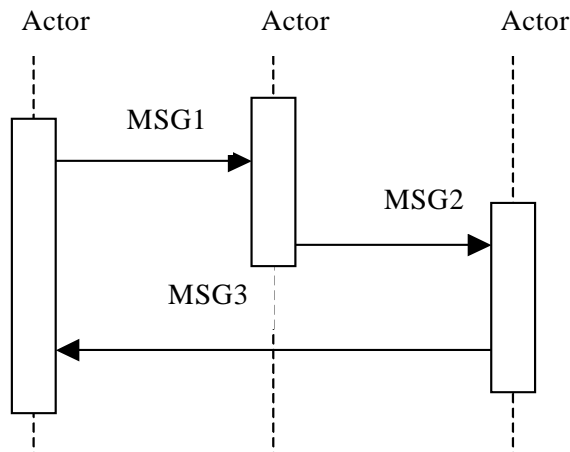
250

The interaction diagrams used in the IHE IT Infrastructure Technical Framework are modeled after those described in Grady Booch, James Rumbaugh, and Ivar Jacobson, *The Unified Modeling Language User Guide*, ISBN 0-201-57168-4. Simple acknowledgment messages are often omitted from the diagrams for brevity. One or more messages may be required to satisfy a

255 transaction. Each message is represented as an arrow starting from the Actor initiating the message.

- *Message definitions*: descriptions of each message involved in the transaction, the events that trigger the message, its semantics, and the actions that the message triggers in the receiver.

2.2 HL7 Profiling Conventions

260 See Appendix C in this volume for the HL7 profiling conventions as well as the networking implementation guidelines.

2.3 Use of Coded Entities and Coding Schemes

IHE does not produce, maintain or otherwise specify a coding scheme or other resource for controlled terminology (coded entities). Where applicable, coding schemes required by the HL7 and DICOM

265 standards take precedence. In the cases where such resources are not explicitly identified by standards, implementations may utilize any resource (including proprietary or local) provided any licensing/copyright requirements are satisfied.

3   IHE Transactions

This section defines each IHE transaction in detail, specifying the standards used, the information
270   transferred, and the conditions under which the transaction is required or optional.

3.1 Maintain Time

This section corresponds to Transaction ITI-1 of the IHE IT Infrastructure Technical Framework. Transaction ITI-1 is used by the Time Server and Time Client actors.

3.1.1 Scope

275   This transaction is used to synchronize time among multiple systems.

3.1.2 Use Case Roles
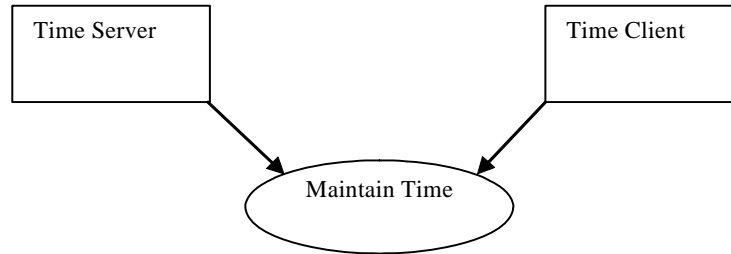
Actor: Time Server

Role: Responds to NTP time service queries.

280   **Actor:** Time Client

Role: Uses NTP or SNTP time service responses to maintain synchronization with Time Servers and maintain the local system clock.

3.1.3 Referenced Standard

NTP   Network Time Protocol Version 3. RFC1305

285   SNTP   Simple Network Time Protocol (SNTP) RFC2030

3.1.4 Interaction Diagram
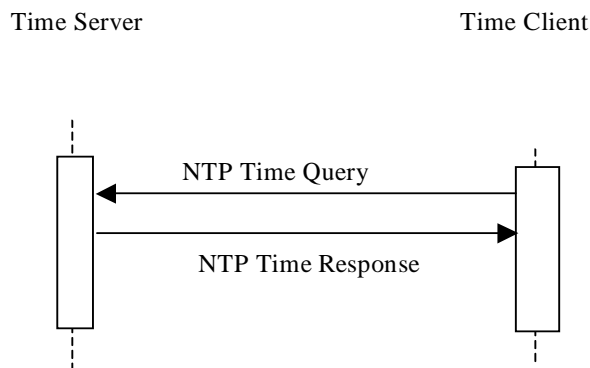
Figure 3.1.4-1. Maintain Time Messages

3.1.4.1 Maintain Time

290 The NTP transactions are described in detail in RFC1305. There is also extensive documentation on the transactions and recommendations on configurations and setup provided at http://www.ntp.org. Rather than reproduce all of that material as part of this Framework, readers are strongly encouraged to explore that site. The most common mode is the query-response mode that is described below. For other forms, see RFC1305 and the material on http://www.ntp.org.

295 The Time Server shall support NTP (which implicitly means that SNTP clients are also supported). Secure NTP may also be supported. The Time Client shall utilize NTP when it is grouped with a Time Server, or when high accuracy is required. For ungrouped Time Clients with 1 second accuracy requirements, SNTP may be useable. Time Clients may also support Secure NTP.

Table 3.1.4-1 Permissible Protocol Selections

Protocol	Time Server	Time Client grouped with a Time Server	Time Client (1s accuracy)	Time Client (High accuracy)
SNTP	Must Support	prohibited	permitted	prohibited
NTP	Must Support	Must Support	permitted	permitted
Secure NTP	Optional	Optional	Optional	Optional

300 3.1.4.1.1 Trigger Events

In a query-response mode the Time Client queries the Time Server and receives a response. This transaction includes timing estimation of network delays.

3.1.4.1.2 Message Semantics

The Time Client uses the Network Time Protocol (NTP) to synchronize its time with the Time Server.
305 NTP clients can be configured to use a specific NTP server at a specific IP address, to obtain the NTP server address automatically from DHCP, and/or to discover the NTP server address automatically. Time clients shall support at least manual configuration and may support all three modes. Time Clients usually maintain time synchronization by adjusting the system clock, so that applications continue to use the system clock facilities. The specific precision of synchronization depends upon the requirements of
310 specific actors.

Implementations must support a time synchronization accuracy of at least one second.

There is a Simple Network Time Protocol (SNTP) RFC2030 defined that can provide one second accuracy for Time Clients. It uses the exact same protocol as NTP, but does not include the measurement data used by the NTP high-accuracy statistical estimation algorithm. It has a lower
315 implementation cost because it omits the measurements and statistical estimation needed to achieve higher accuracy. This omission of the statistical estimation makes it unsuitable for use when grouped with a Time Server. Its use is permitted for Time Clients that are not grouped with a Time Server and that do not need better synchronization for another reason.

320   Note: The Time Client Actor can often be implemented by using components provided by operating systems. Some offer only SNTP while others offer the choice of SNTP or NTP clients.

The use of Secure NTP is not required. The risk of subversion of the time base to conceal penetration is considered very low, and the operational costs of maintaining Secure NTP too high in most
325   environments.

3.1.4.1.3 Expected Actions

The Time Server and Time Client will maintain synchronization to UTC. The Time Client maintains a statistical estimation process utilizing time estimates and network delay estimates from one or more Time Servers. This statistical estimation process yields a time estimate that is used to continually adjust
330   the system clock.

> Note: The relationship between the local reported time, UTC, and battery-backed clock is often a source of confusion. Different hardware and operating systems have different configuration requirements. These should be clearly documented and made clear in the user interface so that field service and operational staff do not introduce errors.

335 ## 3.2 Get User Authentication

This section corresponds to Transaction ITI-2 of the IHE IT Infrastructure Technical Framework. Transaction ITI-2 is used by the Client Authentication Agent and Kerberos Authentication Server actors.

3.2.1 Scope

This transaction is used to authenticate an enterprise-wide user identity. A challenge-response method
340   verifies that the user knows the correct password. Once the user is authenticated, the Kerberos Authentication Server sends a Ticket Granting Ticket (TGT) to the Client Authentication Agent to permit optimization of subsequent interactions. The TGT acts as a substitute for repeated login/password type activity.

This transaction is equivalent to what is called the "Authentication Service" in RFC1510.

345 ### 3.2.2 Use Case Roles

```
 Client Authentication              Kerberos
 Agent                              Authentication Server

              Kerberos User
              Authentication
```
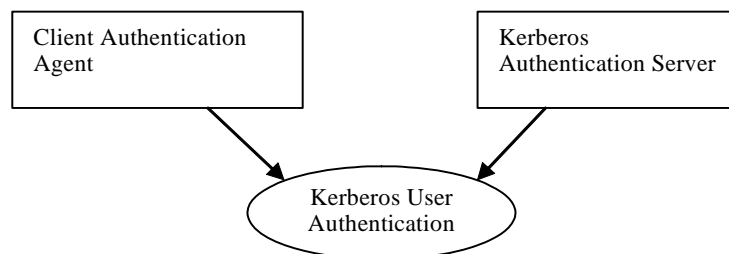
Actor: Client Authentication Agent.

Role: Communicates authentication information to the Kerberos Authentication Server, receives a TGT, and performs internal TGT management.

350 **Actor:** Kerberos Authentication Server. In RFC1510 this is called a Key Distribution Center (KDC).

Role: Verifies the authentication information, creates a TGT, and sends it to the Client Authentication Agent.

3.2.3 Referenced Standard

RFC1510   The Kerberos Network Authentication Service (V5)

355   ### 3.2.4 Interaction Diagram

The Client Authentication Agent communicates to the Kerberos Authentication Server a Kerberos
Authentication Service Request (KRB_AS_REQ). This message identifies the user, the name of the
ticket-granting service and authentication data. The authentication data is usually a timestamp encrypted
with the user's long-term key. (See RFC1510 for the exception cases.)
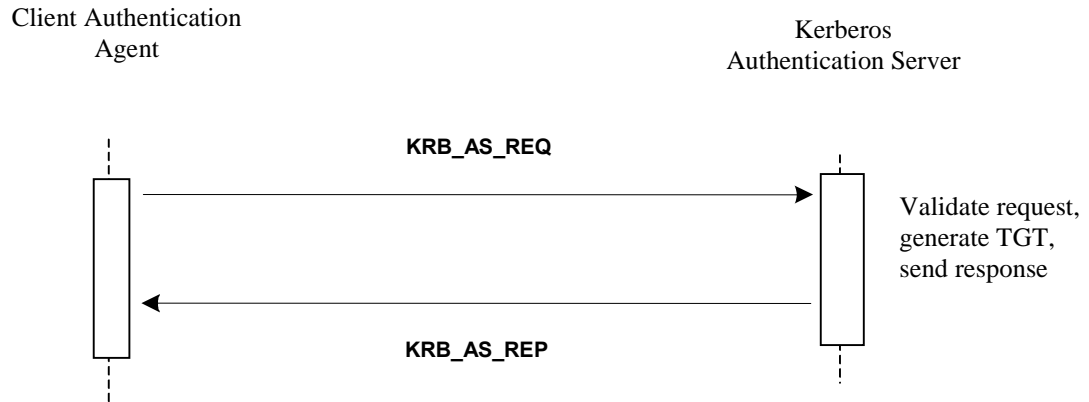
360

Figure 3.2.4-1. Get User Authentication Messages

3.2.4.1 Get User Authentication (Request/Response)

3.2.4.1.1 Trigger Events

The Kerberos User Authentication transactions normally take place:

365   1.   Upon login or session start for a new user, and

2.   Shortly before expiration of a TGT. TGT timeouts are selected to minimize the need for this
transaction, but they may expire prior to user logout/ session complete.

When the Client Authentication Agent supports the Authentication for User Context Option, the Client
Authentication Agent shall resolve any Context Manager interface issues before starting the user

370   authentication. For instance the Client Authentication Agent needs to be sure that it will be accepted by
the Context Manager as the one and only user authenticator in the context for this user session. Similar
issues may apply with non-IHE uses of CCOW.

3.2.4.1.2 Message Semantics

The Client Authentication Agent shall support use of this transaction with the Kerberos user

375   name/password system defined in RFC 1510. The username and password shall consist of the 94
printable characters specified in the International Reference Version of ISO-646/ECMA-6 (aka U.S.
ASCII).

3.2.4.1.3 Expected Actions

The Client Authentication Agent shall perform TGT management, so that subsequent activities can re-
380 use TGTs from a credentials cache. The Client Authentication Agent shall ensure that a user has access
to only to his or her own tickets (both TGT and Service Tickets). This is most often done by clearing the
credentials cache upon user logout or session completion.

When the Client Authentication Agent supports the Authenticator for User Context Option, the agent
shall perform the Change Context Transaction to set the user identity in the context managed by the
385 Context Manager Actor.

When the user session ends, the Client Authentication Agent shall remove the user credentials from its
cache. If it supports the Authenticator for User Context Option, the agent shall perform the Change
Context Transaction to set the user to NULL prior to removing the user credentials.

3.2.5 Extended Authentication Methods

390 The Kerberos challenge-response system used by this Integration Profile can be used to verify users by
means of many authentication mechanisms. The mechanism specified in this profile is the Kerberos
username and password system. Other methods such as smart cards and biometrics have also been
documented but not standardized. (See ITI TF-1: Appendix D for a discussion of alternate authentication
mechanisms.)

395 ### 3.2.6 Audit Record Considerations

The Client Authentication Agent shall produce the ATNA UserAuthenticated event for each Get
Authentication [ITI-2] transaction with the EventTypeCode equal to Login or Failure as appropriate. If
the application knows about logout, this shall produce a UserAuthentication event with the
eventTypeCode of Logout. The UserName element shall be the Kerberos identity in the form of
400 username@realm.

	Field Name	Opt	Value Constraints
Event **AuditMessage/ EventIdentification**	EventID	M	EV(110114, DCM, "UserAuthenticated")
	EventActionCode	M	"E" (Execute)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV(110122, DCM, "Login") EV(110123, DCM, "Logout")
Source (1)			
Human Requestor (1)			
Destination (0)			
Audit Source (Client Authentication Agent) (1)			
Participant Object (0)			

Where:

Source **AuditMessage/ ActiveParticipant**	UserID	M	the process ID as used within the local operating system in the local system logs.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110150, DCM, "Application")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human Requestor (if known) **AuditMessage/ ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	*U*	*not specialized*
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

|			
Audit Source **AuditMessage/ AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

405

3.3 Get Service Ticket

This section corresponds to Transaction ITI-3 of the IHE IT Infrastructure Technical Framework. Transaction ITI-3 is used by the Client Authentication Agent and Kerberos Authentication Server Actors.

410 **3.3.1 Scope**

The Client Authentication Agent uses this transaction to obtain the service ticket that will be sent to a Kerberized Server to authenticate this user to a Kerberized Server.

3.3.2 Use Case Roles
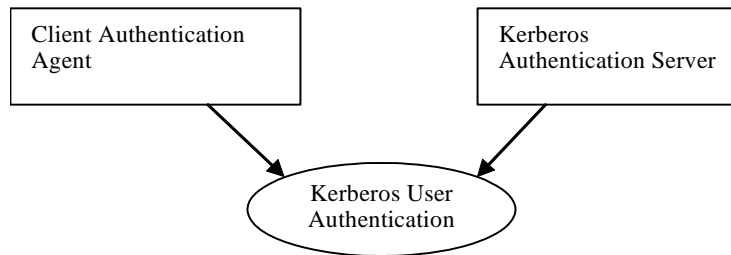
415 **Actor:** Client Authentication Agent.

Role: Client communicates authentication information to the Kerberos Authentication Server, receives a Service Ticket, and performs internal ticket management.

Actor: Kerberos Authentication Server. In RFC1510 this is called a Key Distribution Center (KDC).

Role: Verifies the authentication information, creates a ticket, and sends it to the Client Authentication
420 Agent Actor.

3.3.3 Referenced Standard

RFC1510   The Kerberos Network Authentication Service (V5)

3.3.4 Interaction Diagram

Client Authentication Agent

Kerberos Authentication
Server

KRB_TGS_REQ

KRB_TGS_REP

Utilize service
request
information and
TGT to generate
a service ticket
authenticating the
user to the
requested service
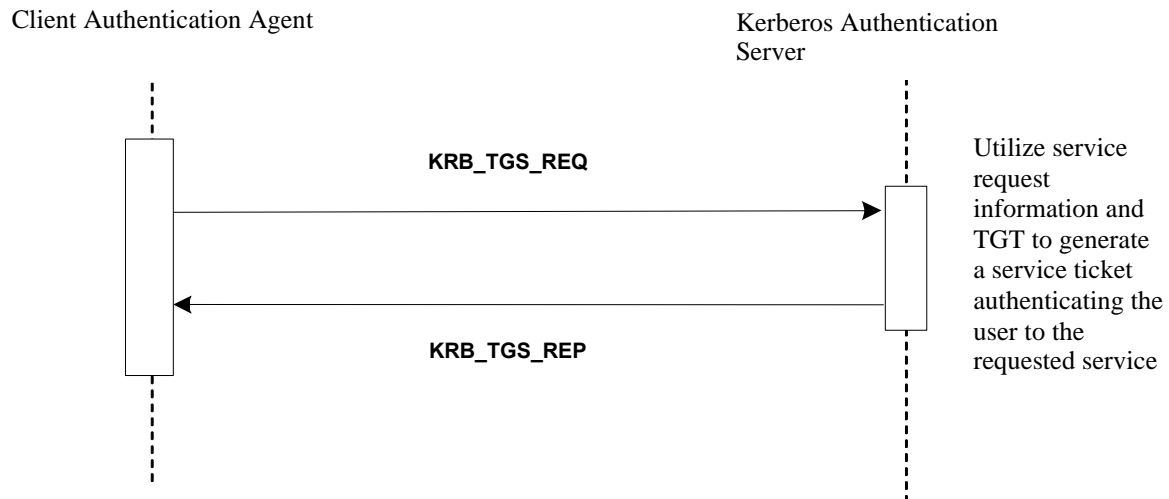
425 **3.3.4.1 Kerberos Service Ticket**

3.3.4.1.1 Trigger Events

A service ticket is requested prior to communicating with a Kerberized Server. This ticket will be
provided to that service as part of the Kerberized communication process.

3.3.4.1.2 Message Semantics

430 The Client Authentication Agent Actor requests credentials for a service by sending the Kerberos
Authentication Server a Kerberos Ticket-Granting Service Request (KRB_TGS_REQ). This message
includes the user's name, an authenticator encrypted with the user's logon session key, the TGT
obtained in the Get User Authentication Transaction, and the name of the service for which the user
wants a ticket.

435 When the Kerberos Authentication Server receives KRB_TGS_REQ, it decrypts the TGT with its own
secret key, extracting the logon session key. It uses the logon session key to decrypt the authenticator
and evaluates that. If the authenticator passes the test, the Kerberos Authentication Server extracts the
authorization data from the TGT and invents a session key for the client to share with the Kerberized
Server Actor that supports the service. The Kerberos Authentication Server encrypts one copy of this
440 session key with the user's logon session key. It embeds another copy of the session key in a ticket,
along with the authorization data, and encrypts this ticket with the service's long-term key. The
Kerberos Authentication Server then sends these credentials back to the client in a Kerberos Ticket-
Granting Service Reply (KRB_TGS_REP).

There are no IHE specific extensions or modifications to the Kerberos messaging.

445 **3.3.4.1.3 Expected Actions**

When the Client Authentication Agent receives the reply, it uses the logon session key to decrypt the
session key to use with the service, and stores the key in its credentials cache. Then it extracts the ticket
for the service and stores that in its cache.

The client shall maintain the ticket in the credentials cache for later use.

450 **3.3.4.1.4 Service Registration**

The Kerberized Communication services supported in an enterprise shall be registered on the Kerberos Authentication Server according to the RFC1510 protocol specification used. The registration of the service on the KDC is outside the scope of this profile.

3.3.5 Security Considerations

455 The Get Service Ticket [ITI-3] Transaction is not required to log an ATNA UserAuthentication event in the case of successful communications. An ATNA UserAuthentication event shall be logged when the communications fails for the purpose of authentication failure.

3.4 Kerberized Communication

This section corresponds to Transaction ITI-4 of the IHE IT Infrastructure Technical Framework.
460 Transaction ITI-4 is used by the Client Authentication Agent and Kerberized Server Actors.

3.4.1 Scope

This section specifies the details of the association of a Kerberos user identity with a session for a
session oriented protocol, or a transaction for a transaction oriented protocol.

3.4.2 Use Case Roles
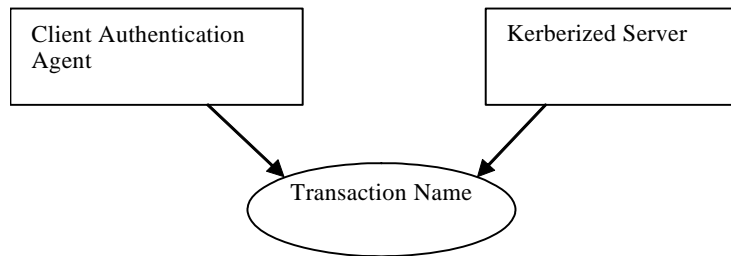
465

Actor: Client Authentication Agent

Role: Provides appropriate ticket as part of the connection or session management for another protocol.

Actor: Kerberized Server

Role: Accepts and verifies the ticket to perform user-identity-related services as part of the connection
470 or session management for another protocol.

3.4.3 Referenced Standard

RFC1510   The Kerberos Network Authentication Service (V5)

3.4.4 Interaction Diagram
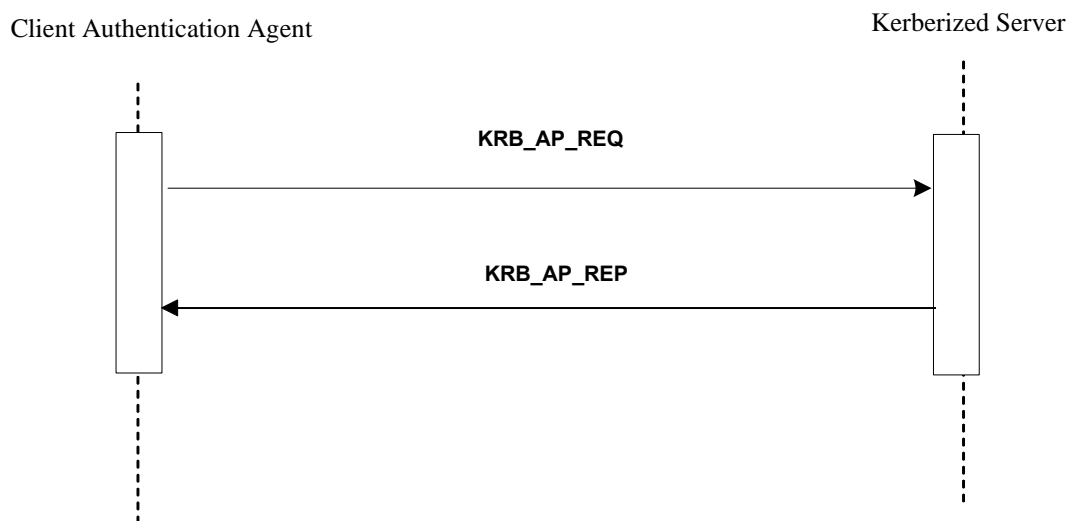
475   **Figure 3.4-1 Kerberized Communications**

3.4.4.1 Kerberized Communications

The sequence diagram above describes information flow that can be encapsulated in a variety of different protocol startup sequences. The specific details for this encapsulation are defined as part of the definition of Kerberizing a specific kind of communication protocol.

480

3.4.4.1.1 Trigger Events

This occurs at the beginning of a session or as part of each session-less transaction.

3.4.4.1.2 Message Semantics

The Client Authentication Agent Actor requests service from a Kerberized Server by sending the server a Kerberos Application Request (KRB_AP_REQ). This message contains an authenticator encrypted
485 with the session key, the ticket obtained in the Get Service Ticket Transaction, and a flag indicating whether the client wants mutual authentication. (The setting of this flag is either specified by the rules of the Kerberized communications, or is an option of the specific Kerberized protocol.)

The Kerberized Server receives KRB_AP_REQ, decrypts the ticket, and extracts the authorization data and the session key. The server uses the session key to decrypt the authenticator and then evaluates the
490 timestamp inside. If the authenticator passes the test, the server looks for a mutual authentication flag in the client's request for protocols that support mutual authentication. If the flag is set, the server uses the session key to encrypt the time supplied by the Client Authentication Actor and returns the result in a Kerberos Application Reply (KRB_AP_REP).

The actual encoding and exchange of the KRB_AP_REQ and KRB_AP_REP are defined as part of the
495 definition of the specific Kerberized protocol.

3.4.4.1.3 Expected Actions

When the Client Authentication Actor receives KRB_AP_REP, it decrypts the server's authenticator with the session key it shares with the server and compares the time returned by the service with the time in the client's original authenticator. If the times match, the client knows that the service is genuine,
500 and the connection proceeds.

If no mutual authentication is requested, the other IHE actors proceed with their IHE transactions. These transactions are identified as being requested by the authenticated user. The other actors will utilize this information for other purposes, such as confirming user authorization or logging user actions into audit trails.

505 ## 3.4.4.2 Kerberized HTTP

Kerberized HTTP shall use SPNEGO-HTTP
(see http://www.ietf.org/internet-drafts/draft-brezak-spnego-http-04.txt)

> Note: At the time of publication there were no Kerberized HTTP normative standards. There are three relatively well-documented non-normative specifications. In addition, there are commercial and open source implementations of this
510   specification for web and application servers. It was decided to use the Kerberized HTTP specification that is implemented by Microsoft Internet Explorer (MSIE) because many healthcare desktops use MSIE.

The following Figure shows a typical message sequence for Kerberized HTTP.
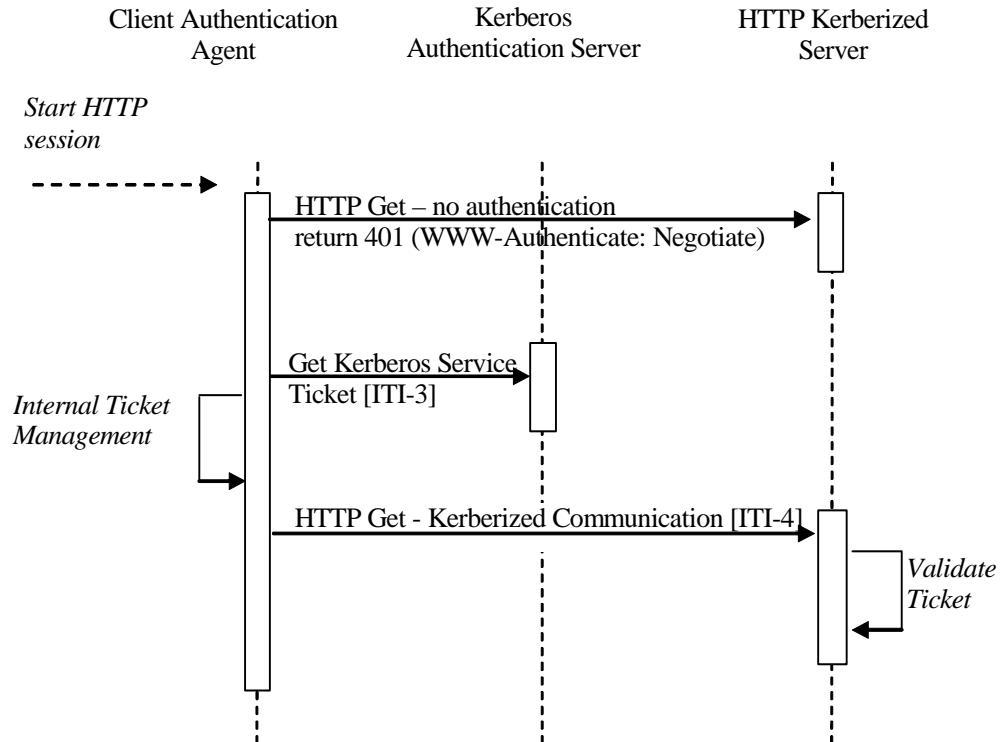
515 **Figure 3.4-2 Kerberized HTTP**

There is also documentation on the transactions, configuration, and troubleshooting these configurations. Rather than reproduce all of that material as part of this Framework, readers are strongly encouraged to explore these references.
(See http://support.microsoft.com/default.aspx?scid=kb;ben-us;326985)

520 **3.4.4.2.1 Trigger Events**

This transaction occurs at the beginning of each HTTP transaction.

> Note: When the workstation is properly configured utilizing Microsoft Internet Explorer these transactions are transparent. A prompt for username, password, and domain is an indication of an improperly configured component.

525 **3.4.4.2.2 Message Semantics**

This IHE profile recognizes that the SPNEGO-HTTP method allows the client side to return Kerberos credentials or NTLM credentials. This IHE profile thus restricts the transactions to the Kerberized credentials.

3.4.4.3 Kerberized DICOM

530 The Kerberization of DICOM has been proposed and is under development. There is not a finished standard at this time.

3.4.4.4 Kerberized HL7

The Kerberization of HL7 has been proposed and is under development. There is not a finished standard at this time.

535 ### 3.4.5 Security Considerations

The Kerberized Communications [ITI-4] Transaction is not required to log an ATNA UserAuthentication event in the case of successful communications. An ATNA UserAuthentication event shall be logged when the communications fails for the purpose of authentication failure.

540 **3.5 Join Context**

This section corresponds to Transaction ITI-5 of the IHE IT Infrastructure Technical Framework. Transaction ITI-5 is used by the Patient Context Participant, User Context Participant, Client Authentication Agent and Context Manager Actors.

3.5.1 Scope

545 Any of the context participant actors using this Transaction (Patient Context Participant, User Context Participant, and Client Authentication Agent) may locate and join a context management session specific to the workstation on which the instigating user is interacting.

A Context Participant Actor shall first locate the instance of the Context Manager Actor via technology specific methods as defined in the *HL7 Context Management "CCOW"* technology mapping documents.
550 Once the context manager reference is returned, the Context Participant Actor issues a join method to the context manager, which returns a unique participant identifier. User Context Participant and Client Authentication Agent shall use this identifier along with a shared secret as inputs to a two stage secure binding process, which results in the exchange of public keys between the two actors.

If an implementation groups two or more context participant actors, this Transaction shall be performed
555 only once on a launch of an application in which those actors are grouped. All grouped actors share the same common context. If at least one of the grouped actors is a User Context Participant or a Client Authentication Agent, this transaction shall include the two-stage secure binding process.

The semantics of the methods used in this Transaction are defined in the documents HL7 Context Management "CCOW" Standard: Component Technology Mapping: ActiveX or HL7 Context
560 Management "CCOW" Standard: Component Technology Mapping: Web. A Context Participant Actor can implement either technology. The Context Manager Actor shall support both technologies in order to interoperate with joining participants implementing the technology of their choice.

3.5.2 Use Case Roles
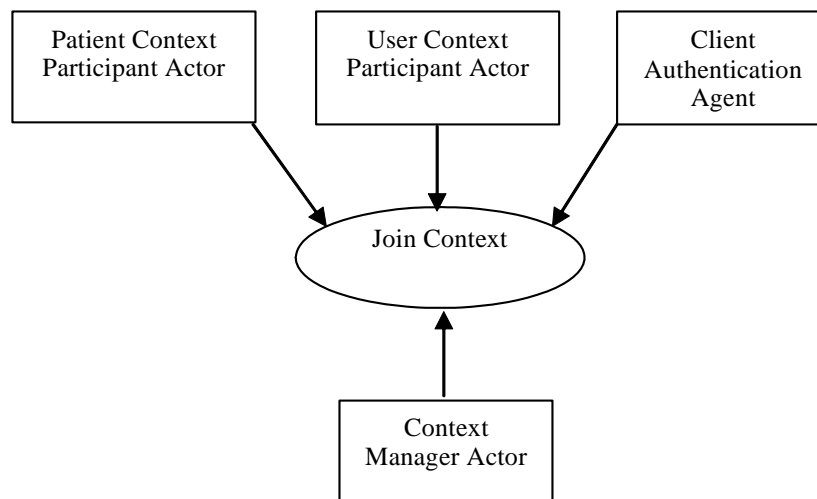
565

Actor: Patient Context Participant

Role: Initiates establishment of context session connection with the Context Manager so as to be able to change and follow Patient Subject changes in the common context.

Actor: User Context Participant

570 **Role:** Initiates establishment of a secure context session connection with the Context Manager so as to be able to follow User Subject changes in the common context.

Actor: Client Authentication Agent

Role: Initiates establishment of a secure context session connection with the Context Manager so as to be able to perform User Subject changes in the common context.

575 **Actor:** Context Manager

Role: Responds to the request to join the context session from the context participant.

3.5.3 Referenced Standard

HL7 Context Management "CCOW" Standard, Version 1.4:

      Technology and Subject Independent Architecture

580   Component Technology Mapping: ActiveX

      Component Technology Mapping: Web

3.5.4 Interaction Diagrams

The Join Context Transaction involves a different set of messages depending on the type of subjects the context participant is interested in, either Patient subject, User subject or both Patient and User subjects.
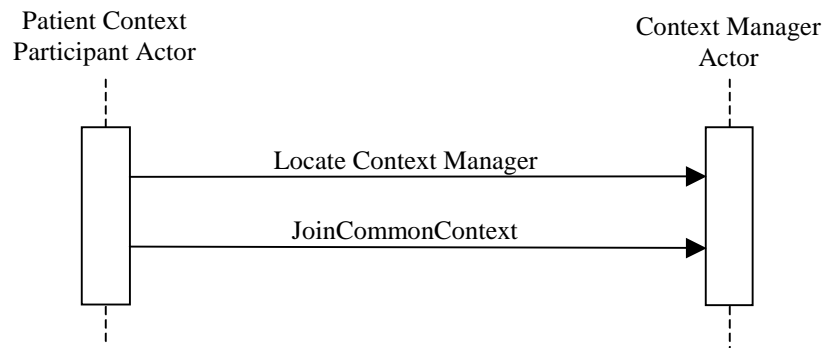
585

Figure 3.5-1 Patient Subject Join Context Interaction Diagram
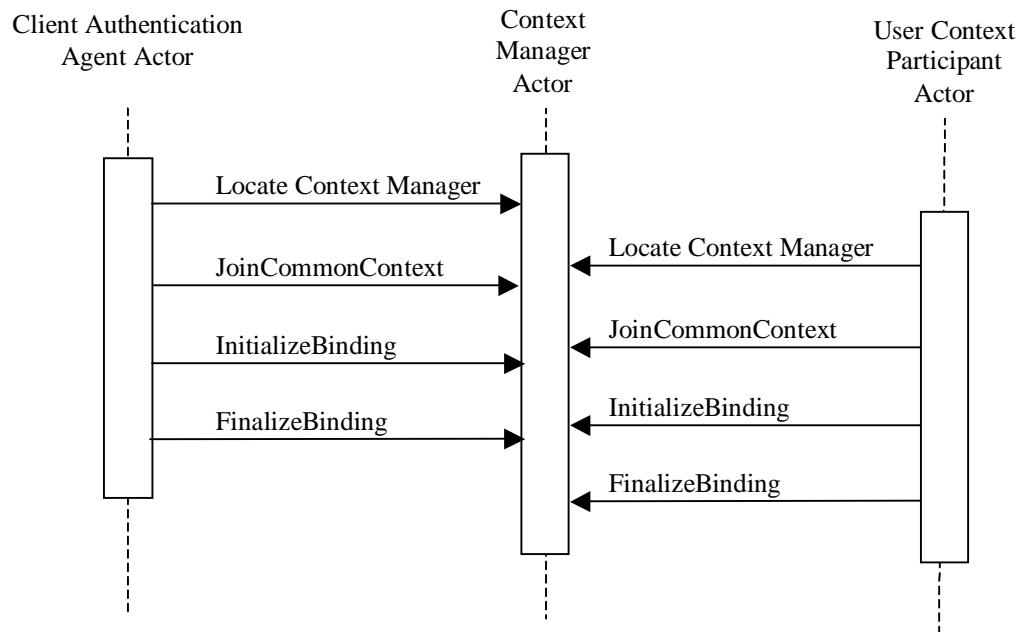
Figure 3.5-2 User Subject Join Context Interaction Diagram

590   3.5.4.1 Join Context – Locate Method

To join the common context upon launch of an application, it is necessary for the context participant to locate the Context Manager that supports context management for the user's workstation. This is achieved by the invocation of the Locate method in accordance with specifications of the *HL7 Context Management "CCOW" Standard.*

595   3.5.4.1.1 Trigger Events

The Locate method is triggered by the user launch of an application that contains one of the following actors: Patient Context Participant, User Context Participant or Client Authentication Agent.

3.5.4.1.2 Message Semantics

In a Web/HTTP implementation, Locate is defined as a method of the ContextManagementRegistry
600   interface. The IHE Context Manager Actor provides this interface for the context participants to call upon, and thus implements the CCOW defined Context Management Registry, which is used to locate the appropriate instance of the Context Manager.

In an ActiveX implementation, the context participants determine the location of the instance of Context Manager from the operating system registry.

605   3.5.4.1.3 Expected Actions

The Locate method invocation is specific to the Web technology mapping. In this case, the Content Manager shall return the valid URL of the Context Manager instance or a CCOW defined UnableToLocate exception. Refer to the *HL7 Context Management "CCOW" Standard: Component Technology Mapping: Web/HTTP*, Chapter 3 for the details of the response specifications.

610   **3.5.4.2 Join Context – JoinCommonContext Method**

The JoinCommonContext method is invoked by the one of the following actors: Patient Context Participant, User Context Participant or Client Authentication Agent.

3.5.4.2.1 Trigger Events

The JoinCommonContext method is triggered by the valid response of the Locate method with a
615   reference to the context manager.

3.5.4.2.2 Message Semantics

JoinCommonContext is defined as a method on the ContextManager interface. It shall be invoked by a Context Participant Actor to complete the establishment of the secure context session. A Context Participant Actor shall provide parameters for this method as specified in the CCOW Standard.

620   Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.6.3, for a detailed description of the parameters associated with this method.

3.5.4.2.3 Expected Actions

If the JoinCommonContext method is successful, the Context Manager shall issue the invoking Actor a
625   unique context participant identifier which is to be used until the context session is terminated by either a Context Participant Actor or the Context Manager Actor.

If the method fails a descriptive CCOW exception will be returned.

After the context session is established, the Context Manager Actor shall periodically verify availability of a Context Participant Actor by invoking the Ping method on the ContextParticipant interface as
630   specified in the CCOW Standard. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.7.6, for a detailed description of the parameters associated with this method.

Should the Context Manager Actor need to terminate an established context session (for example, in a case of restart), it shall inform the context participants of such action by invocation of the
635   CommonContextTerminated method on the ContextParticipant interface as specified in the CCOW Standard. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.7.5, for a detailed description of the parameters associated with this method.

The success of this method signifies completion of the Join Context Transaction for the actors intending
640   to participate only in the patient context.

3.5.4.3 **Join Context – InitializeBinding Method**

The InitializeBinding method is invoked by the one of the following actors intending to participate in a user context: User Context Participant or Client Authentication Agent.

3.5.4.3.1 Trigger Events

645   The InitializeBinding method is triggered by the valid response of the JoinContext method.

3.5.4.3.2 Message Semantics

InitializeBinding is defined as a method on the SecureBinding interface and allows a Context Participant Actor and Context Manager to verify each other's identity and supply the Context Manager's public key to the requesting context participant.

650 In the invocation of this method, context participant supplies the application identification and a digest produced from that identification concatenated with a shared secret. The shared secret is known in CCOW terms as an applications passcode. The passcode shall be site configurable.

Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.12.2, for a description of the parameters associated with this
655 method, to be issued by the Context Participant Actor.

3.5.4.3.3 Expected Actions

Performing the InitializeBinding method, the Context Manager verifies the identity of a requesting context participant and responds with the message containing its public key. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section
660 17.3.12.2, for the specifics of the response formation.

3.5.4.4 Join Context – FinalizeBinding Method

The FinalizeBinding method is invoked by the one of the following actors: User Context Participant or Client Authentication Agent.

3.5.4.4.1 Trigger Events

665 The FinalizeBinding method is triggered by the valid response of the InitializeBinding method.

3.5.4.4.2 Message Semantics

FinalizeBinding is defined as a method on the SecureBinding interface and allows a Context Participant Actor to supply the Context Manager with its public key.

In the invocation of this method, the context participant supplies its public key and a digest digitally
670 signed with its private key.

Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.12.3, for a description of the parameters associated with this method, to be issued by the Context Participant Actor.

3.5.4.4.3 Expected Actions

675 Performing the FinalizeBinding method, the Context Manager verifies the identity of a requesting context participant and accepts or rejects its public key. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.12.3, for the specifics of the response formation.

The success of this method signifies completion of the Join Context Transaction for the actors intending
680 to participate in the user context.

3.6 Change Context

This section corresponds to Transaction ITI-6 of the IHE IT Infrastructure Technical Framework. Transaction ITI-6 is used by the Context Participant and Context Manager actors.

3.6.1 Scope

685   This transaction allows for an application supporting the Context Participant Actor to change the values for one or more context subjects, forcing other Context Participant actors to synchronize based on the new context values.

The Change Context Transaction is composed of multiple methods as defined by the *HL7 Context Management "CCOW" Standard*. There are two key characteristics to this transaction. The first is that
690   the transaction has multiple phases consisting of instigating the change, surveying the other participants, and finally publishing the decision as to whether the context changed or not. The second characteristic is that the context change involves a specific subject. For the Patient Context Participant Actor the subject being changed is the patient subject. For the Client Authentication Agent Actor the subject being changed is the user subject. Applications that implement only the Patient Context Participant Actor shall
695   not expect the user subject to be set in context.

The semantics of the methods used are defined in the documents HL7 Context Management "CCOW" Standard: Component Technology Mapping: ActiveX or HL7 Context Management "CCOW" Standard: Component Technology Mapping: Web, in conjunction with the HL7 Context Management "CCOW" Standard: Subject Data Definitions document. The Context Participant Actor can choose the technology
700   implementation it wishes to implement. The Context Manager Actor must support both technology implementations in order to accommodate whichever implementation a participant ends up choosing.

In the case where Patient Context Participant Actors use identifiers from different patient identifier domains the Context Manager Actor shall be grouped with the Patient Identifier Cross-reference Consumer Actor and the corresponding PIX Query Transaction as defined in ITI TF-2: 3.9 to retrieve all
705   identifiers the patient is known by. The IHE Context Manager Actor encompasses more than a CCOW context manager function. See ITI TF-2: Appendix D for a complete discussion of the grouping of these two actors.

The CCOW architecture is defined as a set of components that implement defined interfaces and their detailed methods as specified in the *HL7 Context Management "CCOW" Standard: Technology*
710   *Independent Architecture* document. This structure is different than the traditional IHE network transaction. As is depicted in the interaction diagram in Section 3.6.4, the IHE Change Context Transaction is composed of multiple CCOW-defined methods.

3.6.2 Use Case Roles
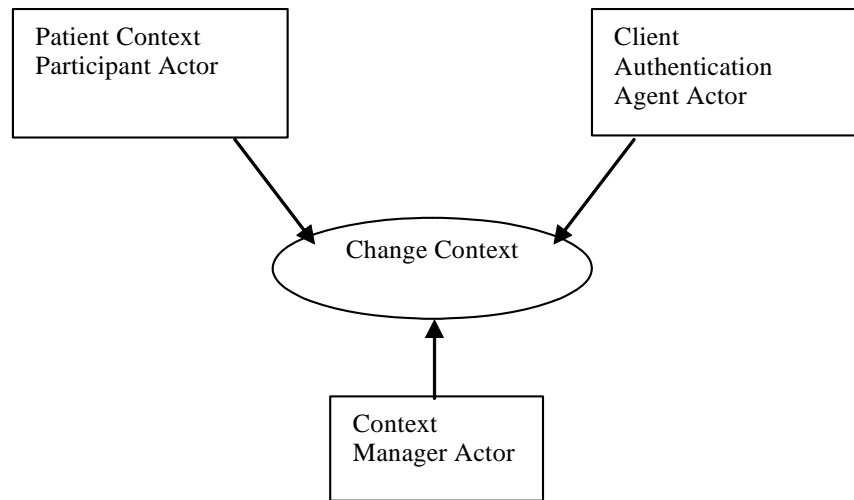
715

Actor: Client Authentication Agent

Role: Initiates context change for user subject by supplying new context values.

Actor: Patient Context Participant

Role: Initiates context change for patient subject by supplying new context values. After receiving the
720   context survey results it finalizes context change decision. Applications containing this Actor without a
patient lookup function would not use this transaction.

Actor: Context Manager

Role: Manages Change Context Transaction lifecycle.

3.6.3 Referenced Standard

725   HL7 Context Management "CCOW" Standard, Version 1.4:

Technology and Subject Independent Architecture

Component Technology Mapping: ActiveX

Component Technology Mapping: Web

Subject Data Definitions

730 **3.6.4 Interaction Diagram**
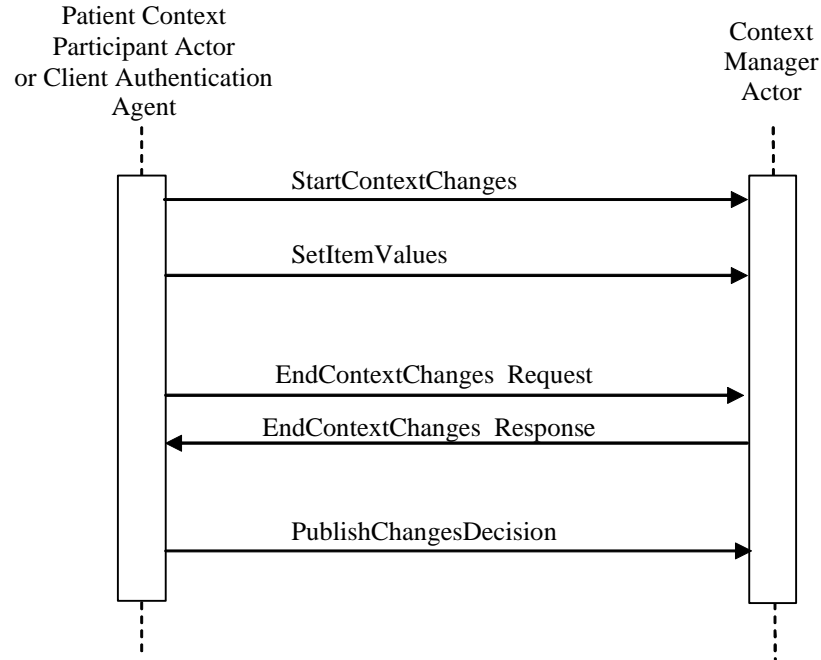
Figure 3.6-1 Change Context sequence

3.6.4.1 Context Change – StartContextChanges Method

3.6.4.1.1 Trigger Events

735   This method is triggered by a specific user gesture. The user gesture that triggers this transaction in for the Patient Context Participant Actor is one of selecting a patient. The user gesture that triggers this transaction for the Client Authentication Agent Actor is authentication of a user.

3.6.4.1.2 Message Semantics

The Patient Context Participant and/or the Client Authentication Agent Actor will issue a
740   StartContextChanges method of the ContextManager interface. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.6.5, for a more detailed description of the parameters associated with this method. IHE specifies no restrictions or extensions to the CCOW definition of the StartContextChanges method.

3.6.4.1.3 Expected Actions

745   The Context Manager Actor returns the pending context coupon. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.6.5, for a more detailed description of the response issued by the Context Manager Actor. IHE specifies no restrictions or extensions to the CCOW definition of the StartContextChanges method.

3.6.4.2 Change Context – SetItemValues Method

750 #### 3.6.4.2.1 Trigger Events

The SetItemValues method is triggered by the return of a context coupon in response to the StartContextChanges method.

3.6.4.2.2 Message Semantics

3.6.4.2.2.1 Patient Context Participant Actor support for CCOW Patient Subject

755 The Patient Context Participant Actor issues an invocation of the SetItemValues method of the ContextData interface to the Context Manager Actor. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.4.4, for a more detailed description of the parameters associated with this method, to be issued by the Patient Context Participant Actor. The Patient Context Participant Actor supports synchronization around the CCOW

760 patient subject. A Patient Context Participant Actor performing a Change Context Transaction shall set the Patient.Id.IdList.1 patient identifier item. All other patient identifier items as defined by the CCOW standard and shown in Table 3.6.4.2-1 Patient Subject Identifier Items, are subject to deprecation in future releases of the standard.

Table 3.6.4.2-1 Patient Subject Identifier Items

Patient Subject Identifier Item Name	HL7 Meaning	HL7 Data Type	HL7 Semantic Constraints on Values	Case Sensitive
Patient.Id.MRN.*Suffix*	Patient's medical record number, per PID-2	ST	HL7 Table 0203Identifier Type = MR	No
Patient.Id.MPI	Patient's identifier in the "Master Patient Index", per PID-2	ST	HL7 Table 0203Identifier Type = PT or PI (as agreed upon by context sharing systems) and Assigning Authority represents the MPI system	No
Patient.Id.NationalIdNumber	Patient's national identifier number, per PID-2	ST	HL7 Table 0203Identifier Type = PT and Assigning Authority represents agreed-upon National Authority	No
Patient.Id.IdList	A list of patient identifiers for a patient, per PID-3	CX	May be a repeating set of CX item values each of which contains an identifier that denotes the same patient	No

765   Adapted from the HL7 Context Management "CCOW" Standard, version 1.4

The Patient.Id.IdList.1 item shall populate component 1, (the patient identifier), and either sub-component 1, (namespace ID), of component 4, (the assigning authority), of the CX data item. This is to be consistent with the requirements for the patient identifier as defined in the PIX Query transaction documented in ITI TF-2: 3.9.4.1.2.2.

770 The Patient Context Participant Actor should use the SetItemValues associated with the ContextData interface, as defined in Sections 17.3.4.4 and 17.3.4.5 respectively of the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document.

3.6.4.2.2.2 Client Authentication Agent Actor support for CCOW User Subject

The Client Authentication Agent Actor supports synchronization around the CCOW user subject. A
775   Client Authentication Agent Actor performing a Change Context Transaction shall set the
User.Id.Logon.*Suffix* identifier item, where the *Suffix* is assigned as Kerberos. This would make the
item name to be used by the Client Authentication Agent Actor User.Id.Logon.Kerberos. The value
of User.Id.Kerberos shall be the username@realm.

The Client Authentication Agent Actor shall use the SetItemValues associated with SecureContextData
780   interface as defined in Section 17.3.13.3 of the *HL7 Context Management "CCOW" Standard:
Technology and Subject-Independent Architecture* document.

3.6.4.2.3 Expected Actions

The Context Manager Actor returns an acknowledgement of the changed data. IHE specifies no
restrictions or extensions to the CCOW definition of the SetItemValues method. Refer to the *HL7*
785   *Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document,
Section 17.3.4.4, for a more detailed description of the response issued by the Context Manager Actor to
the Patient Context Participant Actor. Refer to the *HL7 Context Management "CCOW" Standard:
Technology and Subject-Independent Architecture* document, Section 17.3.13.3, for a more detailed
description of the response issued by the Context Manager Actor to the Client Authentication Agent
790   Actor.

3.6.4.3 Context Change – EndContextChanges

3.6.4.3.1 Trigger Events

The EndContextChanges method is triggered by the completion of the SetItemValues method.

3.6.4.3.2 Message Semantics

795   The Patient Context Participant and Client Authentication Agent Actors issue an EndContextChanges
method of the ContextManager interface to the Context Manager Actor. Refer to the *HL7 Context
Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section
17.3.6.6, for a description of the parameters associated with this method. IHE specifies no restrictions or
extensions to the CCOW definition of the EndContextChanges method.

800   ### 3.6.4.3.3 Expected Actions

The EndContextChanges method triggers the ContextChangesPending method as defined in ITI TF-2:
3.13.4.1. The Context Manager Actor returns the results of the context survey to the instigating Patient
Context Participant or Client Authentication Agent Actor.

If the instigating Patient Context Participant or Client Authentication Agent Actor receives a unanimous
805   acceptance in the survey results, then it triggers an accept in the PublishChangesDecision method.

If the instigating Patient Context Participant or Client Authentication Agent Actor receives one or more
Conditional Accept responses in the survey results, then the application containing the Actor must ask
the user to continue, suspend context participation, or cancel the pending context change transaction.
The user's decision to continue will result in the context change being accepted. The user's decision to

___

810 suspend context participation will cancel the change transaction and allow the user to temporarily use the application without affecting the current context session. The user's decision to cancel will cancel the pending context change transaction. At this point the Patient Context Participant or Client Authentication Agent Actor triggers the PublishChangesDecision with the user's response.

815 In the event a participant application does not respond to the survey, after a configurable period of time the Context Manager Actor will deem the application as "busy". If the instigating participant application receives one or more busy responses, it shall only present the suspend or cancel choices. This prevents an application from inadvertently becoming out of synch with the context, unbeknownst to the user.

820 Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.6.6, for a more detailed description of the response issued by the Context Manager Actor and actions required by the Patient Context Participant and or Client Authentication Agent Actors. IHE specifies no restrictions or extensions to the CCOW definition of the EndContextChanges method.

3.6.4.4 Context Change – PublishChangesDecision

3.6.4.4.1 Trigger Events

825 The PublishChangesDecision method is triggered by the return of EndContextChanges method.

3.6.4.4.2 Message Semantics

The Patient Context Participant and Client Authentication Agent Actors shall issue either an accept or cancel via the PublishChangesDecision method of the ContextManager interface to the Context Manager Actor. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent*
830 *Architecture* document, Section 17.3.6.8, for a more detailed description of the parameters associated with this method. IHE specifies no restrictions or extensions to the CCOW definition of the PublishChangesDecision method.

3.6.4.4.3 Expected Actions

When the PublishChangesDecision method is received by the Context Manager Actor it triggers the
835 ContextChangesAccepted or ContextChangesCancelled method as defined in ITI TF-2: 3.13.4.2 or ITI TF-2: 3.13.4.3 respectively. IHE specifies no restrictions or extensions to the CCOW definition of the PublishChangesDecision method. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.6.8, for a description of the response issued by the Context Manager Actor.

840   **3.7 Leave Context**

This section corresponds to Transaction ITI-7 of the IHE IT Infrastructure Technical Framework. Transaction ITI-7 is used by the Patient Context Participant, User Context Participant, Client Authentication Agent, and Context Manager Actors.

3.7.1 Scope

845   This transaction allows for an application supporting the Patient Context Participant, User Context Participant, or Client Authentication Agent Actor to terminate participation in a context management session in which it is participating.

A Context Participant Actor notifies the Context Manager Actor that is leaving the common context. The semantics of the methods used are defined in the documents *HL7 Context Management "CCOW"*
850   *Standard: Component Technology Mapping: ActiveX* or *HL7 Context Management "CCOW" Standard: Component Technology Mapping: Web*. The Context Participant Actor can choose the technology implementation it wishes to implement. The Context Manager Actor must support both technology implementations in order to accommodate whichever implementation a joining participant ends up choosing.

855   **3.7.2 Use Case Roles**
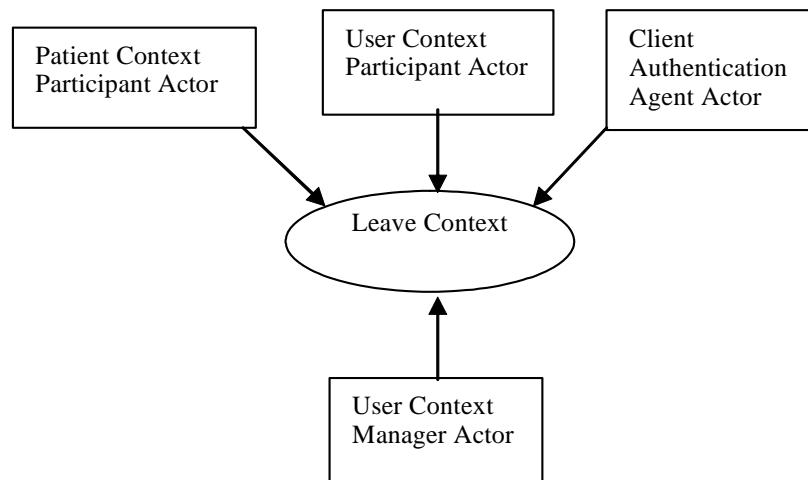
Actor: Patient Context Participant

Role: Initiates notification to the Context Manager that it will no longer be participating in the context management session.

860   **Actor:** User Context Participant

Role: Initiates notification to the Context Manager that it will no longer be participating in the context management session.

Actor: Client Authentication Agent

Role: Initiates notification to the Context Manager that it will no longer be participating in the context
865   management session.

Actor: Context Manager

Role: Responds to the request to leave the context session from the context participant.

3.7.3 Referenced Standard

HL7 Context Management "CCOW" Standard, Version 1.4:

870   Technology and Subject Independent Architecture

            Component Technology Mapping: ActiveX

            Component Technology Mapping: Web

3.7.4 Interaction Diagram
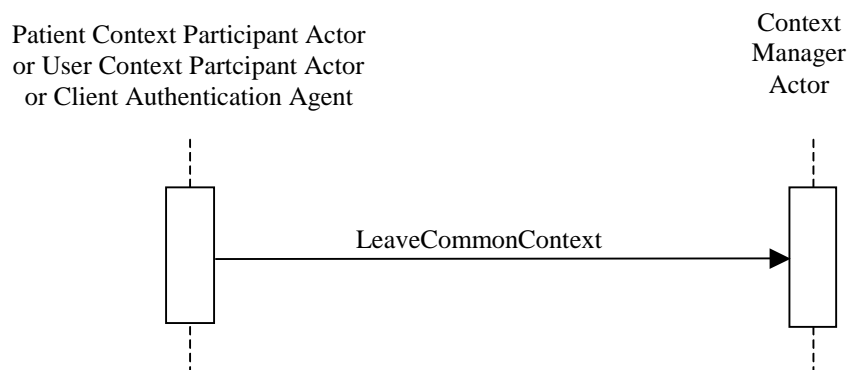
875   **Figure 3.7-1 Leave Context Sequence**

3.7.4.1 Leave Context – LeaveCommonContext Method

3.7.4.1.1 Trigger Events

This transaction is triggered by the user closing an application that contains a Patient Context Participant Actor, a User Context Participant Actor, or Client Authentication Agent Actor.

880   ### 3.7.4.1.2 Message Semantics

LeaveContext is defined as a method on the ContextManager interface. It shall be invoked by a Context Participant Actor to announce its departure from the secure context session. A Context Participant Actor shall provide parameters for this method as specified in the CCOW Standard.

Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent*
885   *Architecture* document, Section 17.3.6.4, for a description of the parameters associated with this method.

3.7.4.1.3 Expected Actions

The Context Manager Actor acknowledges the receipt of the notification. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section
890   17.3.6.4, for a description of the response issued by the Context Manager Actor.

The context participant is expected to dispose of all context manager interface references upon receipt of the message reply. No further context change transactions will be processed by the Context Manager for this context participant.

895 ## 3.8 Patient Identity Feed

This section corresponds to Transaction ITI-8 of the IHE IT Infrastructure Technical Framework. Transaction ITI-8 is used by the Patient Identity Source, Patient Identifier Cross-reference Manager and Document Registry actors.

3.8.1 Scope

900 This transaction communicates patient information, including corroborating demographic data, after a patient's identity is established, modified or merged or after the key corroborating demographic data has been modified.

3.8.2 Use Case Roles
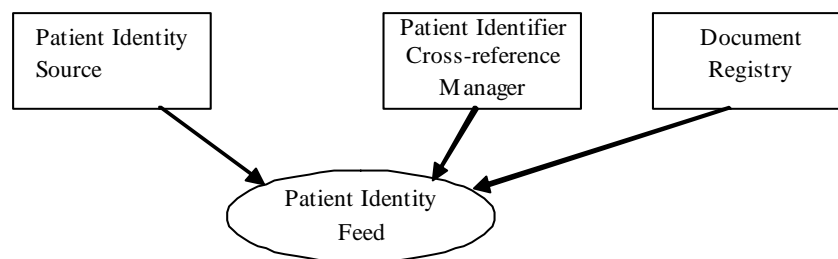
905 **Actor:** Patient Identity Source

Role: Provides notification to the Patient Identifier Cross-reference Manager and Document Registry for any patient identification related events including: creation, updates, merges, etc.

Actor: Patient Identifier Cross-reference Manager

Role: Serves a well-defined set of Patient Identification Domains. Based on information provided in
910 each Patient Identification Domain by a Patient Identification Source Actor, it manages the cross-referencing of patient identifiers across Patient Identification Domains.

Actor: Document Registry

Role: Uses patient identifiers provided by Patient Identity Source to ensure that XDS Documents metadata registered is associated with a known patient and updates patient identity in document
915 metadata by tracking identity change operations (e.g. merge).

3.8.3 Referenced Standards

HL7 Version 2.3.1 Chapter 2 – Control, Chapter 3 – Patient Administration

HL7 version 2.3.1 was selected for this transaction for the following reasons:

- It provides a broader potential base of Patient Identity Source Actors capable of participating in
920 the profiles associated with this transaction.
- It allows existing ADT Actors from within IHE Radiology to participate as Patient Identity Source Actors.

3.8.4 Interaction Diagram
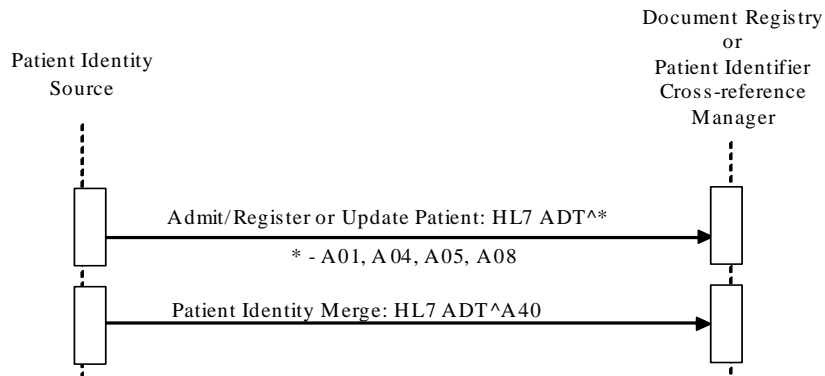
925 **Figure 3.8-1 Patient Identity Sequence**

3.8.4.1 Patient Identity Management – Admit/Register or Update Patient

3.8.4.1.1 Trigger Events

The following events from a Patient Identity Source Actor will trigger one of the Admit/Register or Update messages:

930
- A01 – Admission of an in-patient into a facility
- A04 – Registration of an outpatient for a visit of the facility
- A05 – Pre-admission of an in-patient (i.e., registration of patient information ahead of actual admission).

Changes to patient demographics (e.g., change in patient name, patient address, etc.) shall trigger the
935 following Admit/Register or Update message:

- A08 – Update Patient Information

The Patient Identifier Cross-reference Manager shall only perform cross-referencing logic on messages received from Patient Identity Source Actors. For a given Patient Identifier Domain there shall be one and only one Patient Identity Source Actor, but a given Patient Identity Source Actor may serve more
940 than one Patient Identifier Domain.

3.8.4.1.2 Message Semantics

The Patient Identity Feed transaction is conducted by the HL7 ADT message, as defined in the subsequent sections. The Patient Identity Source Actor shall generate the message whenever a patient is admitted, pre-admitted, or registered, or when some piece of patient demographic data changes. Pre-
945 admission of inpatients shall use the A05 trigger event. The segments of the message listed below are required, and their detailed descriptions are provided in the following subsections.

> Note: Conventions used in this section as well as additional qualifications to the level of specification and HL7 profiling are stated in Appendix C and C.1 in this Volume.

950 Required segments are defined below. Other segments are optional
Table 3.8-1 ADT Patient Administration Messages

ADT	Patient Administration Message	Chapter in HL7 2.3.1
MSH	Message Header	2
EVN	Event Type	3
PID	Patient Identification	3
PV1	Patient Visit	3

Each message shall be acknowledged by the HL7 ACK message sent by the receiver of ADT message to its sender. See Appendix C.1.3, "Acknowledgement Modes", for definition and discussion of the ACK message.

955   This transaction does not require Patient Identity Source Actors to include any attributes not already required by the corresponding HL7 message (as is described in the following sections). This minimal set of requirements enables inclusion of the largest range of Patient Identity Source Actor systems.

This transaction **does** place additional requirements on the Patient Identifier Cross-reference Manager and Document Registry Actors, requiring them to accept aset of HL7 attributes beyond what is required by HL7. (See Section 3.8.4.1.3 for a description of these additional requirements)..

960

3.8.4.1.2.1 MSH Segment

The MSH segment shall be constructed as defined in Appendix C.1.2 "Message Control".

Field *MSH-9 Message Type* shall have at least two components. The first component shall have a value of **ADT**; the second component shall have one of the values of **A01**, **A04**, **A05** or **A08** as appropriate.

965   The third component is optional; however, if present, it shall have the following value for each corresponding message type:

- ADT_A01 for A01 message type
- ADT_A01 for A04 message type
- ADT_A05 for A05 message type

970   - ADT_A01 for A08 message type

3.8.4.1.2.2 EVN Segment

The Patient Identity Source Actor is not required to send any attributes within the EVN segment beyond what is specified in the HL7 standard. See Table C.1-4 in Appendix C.1.4 "Common Segment Definitions" for the specification of this segment.

975   ### 3.8.4.1.2.3 PID Segment

The Patient Identity Source Actor is not required to send any attributes within the PID segment beyond what is specified in the HL7 standard.

This message shall use the field PID-3 Patient Identifier List to convey the Patient ID uniquely identifying the patient within a given Patient Identification Domain.

980   The Patient Identity Source Actor shall provide the patient identifier in the ID component (first component) of the PID-3 field (PID-3.1). The Patient Identity Source Actor shall use component PID-3.4 to convey the assigning authority (Patient Identification Domain) of the patient identifier.Either the first subcomponent (namespace ID) or the second and third subcomponents (universal ID and universal

ID type) shall be populated. If all three subcomponents are populated, the first subcomponent shall
985 reference the same entity as is referenced by the second and third components.

3.8.4.1.2.4 PV1 Segment

The Admit/ Register or Update Patient message is not required to include any attributes within the PV1 segment beyond what is specified in the HL7 standard.

3.8.4.1.3 Expected Actions – Patient Identifier Cross-reference Manager

990 The Patient Identifier Cross-reference Manager shall be capable of accepting attributes in the PID segment as specified in Table 3.8-2. This is to ensure that the Patient Identifier Cross-reference Manager can handle a sufficient set of corroborating information in order to perform its cross-referencing function.

Table 3.8-2 IHE Profile - PID segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	4	SI	O		00104	Set ID - Patient ID
2	20	CX	O		00105	Patient ID
3	250	CX	R		00106	Patient Identifier List
4	20	CX	O		00107	Alternate Patient ID
5	250	XPN	R		00108	Patient Name
6	250	XPN	R+		00109	Mother's Maiden Name
7	26	TS	R+		00110	Date/Time of Birth
8	1	IS	R+	0001	00111	Administrative Sex
9	250	XPN	O		00112	Patient Alias
10	250	CE	O	0005	00113	Race
11	250	XAD	R2		00114	Patient Address
12	4	IS	O	0289	00115	County Code
13	250	XTN	R2		00116	Phone Number - Home
14	250	XTN	R2		00117	Phone Number - Business
15	250	CE	O	0296	00118	Primary Language
16	250	CE	O	0002	00119	Marital Status
17	250	CE	O	0006	00120	Religion
18	250	CX	O		00121	Patient Account Number
19	16	ST	R2		00122	SSN Number – Patient
20	25	DLN	R2		00123	Driver's License Number - Patient
21	250	CX	O		00124	Mother's Identifier
22	250	CE	O	0189	00125	Ethnic Group
23	250	ST	O		00126	Birth Place
24	1	ID	O	0136	00127	Multiple Birth Indicator
25	2	NM	O		00128	Birth Order
26	250	CE	O	0171	00129	Citizenship
27	250	CE	O	0172	00130	Veterans Military Status
28	250	CE	O	0212	00739	Nationality
29	26	TS	O		00740	Patient Death Date and Time

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
30	1	ID	O	0136	00741	Patient Death Indicator

995   Adapted from the HL7 standard, Version 2.3.1

> Note: This table reflects attributes required to be handled by the Patient Identifier Cross-reference Manager (receiver). It is likely that not all attributes marked as R2 or R+ above will be sent in some environments.

If the PID-3.4 (assigning authority) component is not included in the message (as described in Section 3.8.4.1.2.3) the Patient Identifier Cross-reference Manager shall fill PID-3.4 prior to storing the ID
1000   information and performing its cross-referencing activities. The information filled by the Patient Identifier Cross-reference Manager is based on the configuration associating each of the Patient Identity Source actors with the subcomponents of the correct assigning authority (namespace ID, UID and UID type). (See 3.8.4.1.3.1 below for a list of required Patient Identifier Cross-reference Manager configuration parameters).

1005   A single Patient Identity Source Actor can serve multiple Patient Identification domains. The Patient Identifier Cross-reference Manager Actor shall only recognize (by configuration) a single Patient Identity Source Actor per domain. (See 3.8.4.1.3.1 below for a list of required Patient Identifier Cross-reference Manager configuration parameters).

The cross-referencing process (algorithm, human decisions, etc.) is performed within the Patient
1010   Identifier Cross-reference Manager Actor, but its specification is beyond the scope of IHE.

Once the Patient Identifier Cross-reference Manager has completed its cross-referencing function, it shall make the newly cross-referenced identifiers available to PIX queries and send out notification to any Patient Identifier Cross-reference Consumers that have been configured (as being interested in receiving such notifications) using the PIX Update Notification transaction (see Section 3.10 for the
1015   details of that transaction).

3.8.4.1.3.1 Required Patient Identifier Cross-reference Manager Configuration

The following items are expected to be parameters that are configurable on the Patient Identifier Cross-reference Manager Actor. For each Patient Identification Domain included in the Identification Cross-reference Domain managed by a Patient Identifier Cross-reference Manager Actor, the following
1020   configuration information is needed:

- Identifier of the Domain. This identifier shall specify all 3 components of the HL7 assigning authority (including the namespace ID and/or both the universal ID and universal ID type subcomponents) of the PID-3 field for the identification of the domain.

- Patient Identity Source Actor for the domain. This is expected to be the MSH-3 Sending
1025   Application and the corresponding MSH-4 Sending Facility fields in the HL7 ADT message. (Alternative identification schemes might include IP address of the Patient Identity Source Actor or Node Authentication if the Audit Trail and Node Authentication Integration Profile is used.)

3.8.4.1.4 Expected Actions – Document Registry

The Document Registry shall be capable of accepting attributes in the PID segment as specified in Table
1030   3.8-2. The Patient Identity Feed transaction contains more triggers and data than what the XDS Document Registry needs for its operation. In particular, A08 – Update Patient Information, if received shall be ignored.

Table 3.8-2 IHE Profile - PID segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
3	250	CX	R		00106	Patient Identifier List

Adapted from the HL7 standard, Version 2.3.1

1035   Note: This table reflects only the attributes required to be handled by the Document Registry (receiver). Other attributes of the PID Segment may be ignored.

If subcomponents 2 and 3 (the universal ID and the universal ID Type of Assigning Authority) of the Patient Identification Domain of the XDS Affinity Domain in PID-3.4 are not filled in the message (as described in Section 3.8.4.1.2.3) the Document Registry shall fill subcomponents 2 and 3 of the Patient
1040   Identification Domain of the XDS Affinity Domain prior to storing the patient identity in the registry. The assigning authority information filled by the Document Registry is based on its configuration of the Patient Identification Domain of the XDS Affinity Domain (See 3.8.4.1.4.1 below for a list of required Document Registry configuration parameters).

The Document Registry shall store only the patient identifiers of the patient identification domain
1045   designated by the XDS Affinity Domain for document sharing in the registry. Patient identifiers of other patient identification domains (assigning authorities), if present in a received message, shall be ignored.

3.8.4.1.4.1 Required Document Registry Configuration

The following items are expected to be parameters that are configurable on the Document Registry Actor:

1050   • Identifier of the Patient Identification Domain of the XDS Affinity Domain. This identifier shall be specified with 3 components of the HL7 assigning authority (data type HD): namespaceID, universal ID and universal ID type. The universal ID shall be an ISO OID (Object Identifier), and therefore the universal ID Type must be "ISO".

1055   ## 3.8.4.2 Patient Identity Management –Patient Identity Merge (Merge Patient ID)

3.8.4.2.1 Trigger Events

When two patients' records are found to identify the same patient by a Patient Identity Source Actor in a Patient Identifier Domain and are merged, the Patient Identity Source shall trigger the following message:

1060   • A40 – Merge Patient – Internal ID

An A40 message indicates that the Patient Identity Source Actor has done a merge within a specific Patient Identification Domain. That is, MRG-1 (patient ID) has been merged into PID-3 (Patient ID).

3.8.4.2.2 Message Semantics

The Patient Identity Feed transaction is an HL7 ADT message. The message shall be generated by the
1065   system (Patient Identity Source Actor) that performs the update whenever two patient records are found to reference the same person.

Note: Conventions used in this section as well as additional qualifications to the level of specification and HL7 profiling are stated in Appendix C and C.1 in this Volume.

The segments of the HL7 Merge Patient message listed below are required, and the detailed description
1070   of the message is provided in Section 3.8.4.2.2.1–3.8.4.2.2.6. The PV1 segment is optional.

Table 3.8-3 ADT A40 Patient Administration Message

ADT A40	Patient Administration Message	Chapter in HL7 v2.3.1
MSH	Message Header	2
EVN	Event Type	3
PID	Patient Identification	3
MRG	Merge Information	3
[PV1]	Patient Visit	3

Each message shall be acknowledged by the HL7 ACK message sent by the receiver of ADT message to
its sender. See Appendix C.1.3 "Acknowledgement Modes" for definition and discussion of the ACK
message.

1075   A separate merge message shall be sent for each pair of patient records to be merged. For example, if
Patients A, B, and C are all to be merged into Patient B, two ADT^A40 messages would be sent. In the
first ADT^A40 message, patient B would be identified in the PID segment and Patient A would be
identified in the MRG segment. In the second ADT^A40 message, patient B would be identified in the
PID segment, and Patient C would be identified in the MRG segment.

1080   Modification of any patient demographic information shall be done by sending a separate Update Patient
Information (A08) message for the current Patient ID. An A40 message is the only method that may be
used to update a Patient ID.

3.8.4.2.2.1 MSH Segment

MSH segment shall be constructed as defined in the Appendix C.1.2 "Message Control".

1085   Field *MSH-9 Message Type* shall have at least two components. The first component shall have a value
of **ADT**; the second component shall have value of **A40**. The third component is optional; however, if
present, it shall have a value of **ADT_A39**.

3.8.4.2.2.2 EVN Segment

See Appendix C.1.4 for the list of all required and optional fields within the EVN segment.

1090   ### 3.8.4.2.2.3 PID Segment

The PID segment shall be constructed as defined in Section 3.8.4.1.2.3.

3.8.4.2.2.4 MRG Segment

The PID and PV1 segments contain the dominant patient information, including patient identifier and
the issuing assigning authority. The MRG segment identifies the "old" or secondary patient records to be
1095   de-referenced. HL7 does not require that the "old" record be deleted; it does require that the "old"
identifier shall not be referenced in future transactions following the merge.

The Patient Identity Source Actor shall send the "old" patient identifier (to be merged) in MRG-1, with
the identifier value in the component MRG-1.1 and the assigning authority in the component MRG-1.4.

The Patient Identity Source Actor shall populate the same value of the assigning authority in PID-3.4, in
1100   the component MRG-1.4.

IHE does not require that the Patient Identity Source Actor send any attributes within the MRG segment
beyond what is specified in the HL7 standard.

3.8.4.2.2.5 PV1 Segment

PV1 segment shall be constructed as defined in Section 3.8.4.1.2.4.

1105   **3.8.4.2.3 Expected Actions**

The Patient Identifier Cross-reference Manager shall be capable of accepting attributes in the MRG
segment as specified in Table 3.8-4.

Table 3.8-4 IHE Profile - MRG segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	250	CX	R		00211	Prior Patient Identifier List
2	250	CX	O		00212	Prior Alternate Patient ID
3	250	CX	O		00213	Prior Patient Account Number
4	250	CX	O		00214	Prior Patient ID
5	250	CX	O		01279	Prior Visit Number
6	250	CX	O		01280	Prior Alternate Visit ID
7	250	XPN	R2		01281	Prior Patient Name

Adapted from the HL7 Standard, Version 2.3.1

1110   In addition, the Patient Identifier Cross-reference Manager shall perform the Expected Actions as
specified in Section 3.8.4.1.3.

When the Patient Identifier Cross-reference Manager receives the ADT^A40 message type of the Patient
Identity Feed transaction, it shall cross-reference the patient identifiers provided in the PID-3 and MRG-
1 fields of the message by replacing any references it is maintaining internally to the patient ID provided
1115   in the MRG-1 field by the patient ID included in the PID-3 field. After the identifier references are
replaced, the Patient Identifier Cross-reference Manager shall reapply its internal cross-referencing
logic/ policies before providing the updated information via either the PIX Query or PIX Notification
Transactions.

3.8.4.2.4 Expected Actions – Document Registry

1120   The Document Registry shall be capable of accepting attributes in the MRG segment as specified in
Table 3.8-4. Other attributes may exist, but the Document Registry shall ignore them.

Table 3.8-4 IHE Profile - MRG segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	250	CX	R		00211	Prior Patient Identifier List
2	250	CX	O		00212	Prior Alternate Patient ID
3	250	CX	O		00213	Prior Patient Account Number
4	250	CX	R2		00214	Prior Patient ID
5	250	CX	O		01279	Prior Visit Number

| 6 | 250 | CX | O | | 01280 | Prior Alternate Visit ID |
| 7 | 250 | XPN | R2 | | 01281 | Prior Patient Name |

Adapted from the HL7 Standard, Version 2.3.1

In addition, the Document Registry shall perform the Expected Actions as specified in Section 3.8.4.1.4.

1125 When the Document Registry receives the ADT^A40 message type of the Patient Identity Feed transaction, it shall merge the patient identity specified in MRG-1 (secondary patient identity) into the patient identity specified in PID-3 (primary patient identity) in its registry. After the merge, all Document Submission Sets (including all Documents beneath them) under the secondary patient identity before the merge shall point to the primary patient identity. The secondary patient identity shall no

1130 longer be referenced in the future services provided by the Document Registry.

3.8.5 Security Considerations

3.8.5.1 Audit Record Considerations – Admit/Register or Update Patient

The Patient Admit/Register transactions (A01, A04, A05) and Update Patient Information (A08)

1135 transaction are to be audited as "Patient Record" events, as defined in table 3.20.6-1. The actors involved in the transaction shall create audit data in conformance with DICOM (Supp 95) "Patient Record". The following tables show items that are required to be part of the audit record for these specific PIX transactions.

3.8.5.1.1 Patient Identity Source Actor audit message:

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110110, DCM, "Patient Record")
	EventActionCode	M	"C" (create) for A01, A04, A05 "U" (update) for A08
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-8", "IHE Transactions", "Patient Identity Feed")
Source (Patient Identity Source Actor) (1)			
Human Requestor (0..n)			
Destination (Patient Identifier Cross-reference Manager or Document Registry) (1)			
Audit Source (Patient Identity Source Actor) (1)			
Patient (1)			

1140 Where:

Source **AuditMessage/ ActiveParticipant**	UserID	M	The identity of the Patient Identity Source Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human Requestor (if known) **AuditMessage/ ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

Destination **AuditMessage/ ActiveParticipant**	UserID	M	The identity of the Patient Identifier Cross-reference Manager or Document Registry facility and receiving application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	*M*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source **AuditMessage/ AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Patient **(AudittMessage/ ParticipantObjectIdentifi cation)**	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	the patient ID in HL7 CX format..
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*M*	MSH-10 - the message identifier

1145 **3.8.5.1.2 Patient Identifier Cross-reference Manager or Document Registry Actor audit message:**

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110110, DCM, "Patient Record")
	EventActionCode	M	"C" (create) for A01, A04, A05 "U" (update) for A08
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-8", "IHE Transactions", "Patient Identity Feed")

Source (Patient Identity Source Actor) (1)
Destination (Patient Identifier Cross-reference Manager or Document Registry) (1)
Audit Source (Patient Identifier Cross-reference Manager or Document Registry) (1)
Patient(1)

Where:

	Field Name	Opt	Value Constraints
Source **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Identity Source Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

	Field Name	Opt	Value Constraints
Destination **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Identifier Cross-reference Manager or Document Registry facility and receiving application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

	Field Name	Opt	Value Constraints
Audit Source **AuditMessage/** **AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

1150

	Field Name	Opt	Value Constraints
	ParticipantObjectTypeCode	M	"1" (person)

	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	the patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	M	MSH-10 - the message identifier

3.8.5.2 Audit Record Considerations – Patient Identity Merge (Merge Patient ID)

The Patient Identity Merge transaction (A40) is to be audited as a "Patient Record" event, as defined in table 3.20.6-1. The source of the transaction shall create audit data in conformance with DICOM (Supp 95) "Patient Record". The following tables show items that are required to be part of the audit record for the Patient Identity Merge transaction. Logically, a merge operation consists of a delete on one patient record, and an update of another patient record. Separate audit records shall be written for the delete operation and the update operation.

3.8.5.2.1 Patient Identity Source Actor audit message:

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110110, DCM, "Patient Record")
	EventActionCode	M	"D" (delete) for the Delete operation "U" (update) for the Update operation
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-8", "IHE Transactions", "Patient Identity Feed")
Source (Patient Identity Source Actor) (1)			
Human Requestor (0..n)			
Destination (Patient Identifier Cross-reference Manager or Document Registry) (1)			
Audit Source (Patient Identity Source Actor) (1)			
Patient(1)			

1160   Where:

	Field Name	Opt	Value Constraints
Source **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Identity Source Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human Requestor (if known) **AuditMessage/** **ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

	Field Name	Opt	Value Constraints
Destination **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Identifier Cross-reference Manager or Document Registry facility and receiving application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source	AuditSourceID	U	Not specialized.
AuditMessage/ AuditSourceIdentification	AuditEnterpriseSiteID	U	not specialized
	AuditSourceTypeCode	U	not specialized

Patient	ParticipantObjectTypeCode	M	"1" (person)
(AudittMessage/ ParticipantObjectIdentifi cation)	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	the patient ID in HL7 CX format.
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	M	MSH-10 - the message identifier

3.8.5.2.2 Patient Identifier Cross-reference Manager or Document Registry Actor audit message:

1165

	Field Name	Opt	Value Constraints
Event	EventID	M	EV(110110, DCM, "Patient Record")
AuditMessage/ EventIdentification	EventActionCode	M	"D" (delete) for the Delete audit record "U" (update) for the Update audit record
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	EV("ITI-8", "IHE Transactions", "Patient Identity Feed")

Source (Patient Identity Source Actor) (1)
Destination (Patient Identifier Cross-reference Manager or Document Registry) (1)
Audit Source (Patient Identifier Cross-reference Manager or Document Registry) (1)
Patient(1)
Where:

Source	UserID	M	The identity of the Patient Identity Source Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
AuditMessage/ ActiveParticipant	AlternativeUserID	M	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

	UserID	M	The identity of the Patient Identifier Cross-reference Manager or Document Registry facility and receiving application from the HL7 message; concatenated together, separated by the | character.

	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source	*AuditSourceID*	*U*	*Not specialized.*
AuditMessage/ AuditSourceIdentification	*AuditEnterpriseSiteID*	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Patient	ParticipantObjectTypeCode	M	"1" (person)
(AudittMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	the patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	M	MSH-10 - the message identifier

1170

3.9 PIX Query

This section corresponds to Transaction ITI-9 of the IHE IT Infrastructure Technical Framework. Transaction ITI-9 is used by the Patient Identifier Cross-reference Consumer and Patient Identifier Cross-reference Manager actors.

1175   ### 3.9.1 Scope

This transaction involves a request by the Patient Identifier Cross-reference Consumer Actor for a list of patient identifiers that correspond to a patient identifier known by the consumer. The request is received by the Patient Identifier Cross-reference Manager. The Patient Identifier Cross-reference Manager immediately processes the request and returns a response in the form of a list of corresponding patient

1180   identifiers, if any.

3.9.2 Use Case Roles
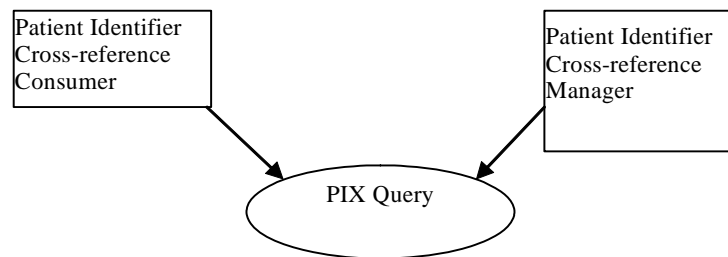
Actor: Patient Identifier Cross-reference Consumer

Role: Queries the Patient Identifier Cross-reference Manager for a list of corresponding patient

1185   identifiers, if any

Actor: Patient Identifier Cross-reference Manager

Role: Manages the cross-referencing of patient identifiers across Patient Identification Domains. Upon request it returns a list of corresponding patient identifiers, if any.

3.9.3 Referenced Standard

1190   HL7 2.5, Chapter 2 – Control, Chapter 3 – Patient Administration, Chapter 5 – Query

HL7 version 2.5 was selected for this transaction for the following reasons:

It was considered the most stable version that contained the functionality required by transactions ITI-9 and ITI-10.

3.9.4 Interaction Diagram
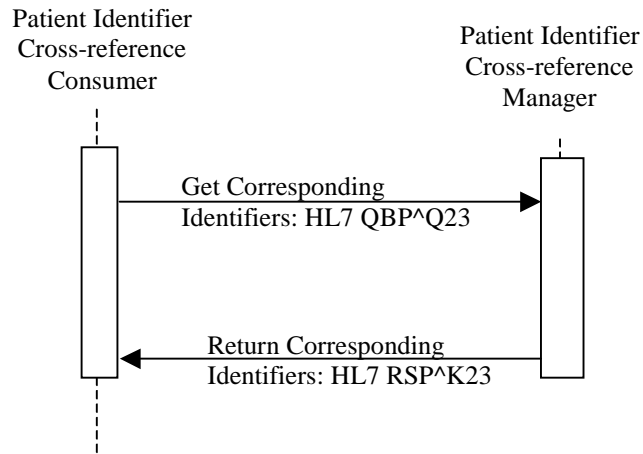
1195

Figure 3.9-1 Get Corresponding Identifiers Sequence

3.9.4.1 Get Corresponding Identifiers

3.9.4.1.1 Trigger Events

A Patient Identifier Cross-reference Consumer's need to get the patient identifier associated with a
1200 domain for which it needs patient related information will trigger the request for corresponding patient
identifiers message based on the following HL7 trigger event:

- Q23 – Get Corresponding Identifiers

3.9.4.1.2 Message Semantics

The Request for Corresponding Patient Identifiers transaction is conducted by the HL7 QBP^Q23
1205 message. The Patient Identifier Cross-reference Consumer Actor shall generate the query message
whenever it needs to obtain a corresponding patient identifier(s) from other Patient Identification
Domain(s). The segments of the message listed below are required, and their detailed descriptions are
provided in the following subsections.

Note: Conventions used in this section as well as additional qualifications to the level of specification and HL7 profiling are stated in
1210 Appendix C and C.1 in this Volume.

Table 3.9-1 QBP Query By Parameter

QBP	Query By Parameter	Chapter in HL7 2.5
MSH	Message Header	2
QPD	Query Parameter Definition	5
RCP	Response Control Parameter	5

The receiver shall respond to the query by sending the RSP^K23 response message. This satisfies the requirements of original mode acknowledgment; no intermediate ACK message is to be sent.

3.9.4.1.2.1 MSH Segment

The MSH segment shall be constructed as defined in Appendix C.1.2 "Message Control".

Field *MSH-9 Message Type* shall have at least two components. The first component shall have a value of QBP; the second component shall have the value of Q23. The third component is optional; however, if present, it shall have a value of QBP_Q21.

3.9.4.1.2.2 QPD Segment

The Patient Identifier Cross-reference Consumer Actor is required to send attributes within the QPD segment as described in Table 3.9-2.

Table 3.9-2 IHE Profile - QPD segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	250	CE	R	0471	01375	Message Query Name
2	32	ST	R+		00696	Query Tag
3	250**	CX	R			Person Identifier
4	250	CX	O			What Domains Returned

Adapted from the HL7 Standard, version 2.5

** Note: This value assumes completion of an HL7 erratum to correct an error identified in the standard.

This message shall use the field QPD-3 *Person Identifier* to convey a single Patient ID uniquely identifying the patient within a given Patient Identification Domain.

The Patient Identifier Cross-reference Consumer Actor shall provide the patient identifier in the ID component (first component) of the QPD-3 field (QPD-3.1).

The Patient Identifier Cross-reference Consumer Actor shall provide component QPD-3.4, Assigning Authority, by including either the first subcomponent (namespace ID) or the second and third subcomponents (universal ID and universal ID type) If all three subcomponents are populated, the first subcomponent shall reference the same entity as is referenced by the second and third components.

If the requesting system wishes to select the domains from which they wish to receive Patient IDs, it does so by populating *QPD-4-What Domains Returned* with as many repetitions as domains for which it wants to receive Patient IDs. Each repetition of QPD-4 shall contain an instance of data type CX in which only the fourth component (Assigning Authority) is populated; the remaining components shall be empty. The responding system shall return the Patient ID value for each requested domain if a value is known.

If QPD-4 is empty, the Patient Identifier Cross-reference Manager Actor shall return Patient IDs for all domains for which it possesses a corresponding Patient ID (subject to local publication restrictions).

The Consumer shall specify "IHE PIX Query" for QPD-1 Message Query Name.

3.9.4.1.2.3 RCP Segment

Although HL7 requires that the RCP Segment be sent in all QBP messages, IHE does not require that
1245 the Patient Identifier Cross-reference Consumer Actor send any attributes within the RCP segment, as is
specified in the HL7 standard.

3.9.4.1.2.3.1 Populating RCP-1-Query Priority

Field *RCP-1-Query Priority* shall always contain **I**, signifying that the response to the query is to be
returned in Immediate mode.

1250 ### 3.9.4.1.3 Expected Actions

The Patient Identifier Cross-reference Manager shall be capable of accepting attributes in the QPD
segment as specified in Table 3.9-2.

The Patient Identifier Cross-reference Manager Actor must be capable of receiving all valid
combinations of subcomponents that make up the Assigning Authority component (i.e., all valid
1255 combinations of QPD-3.4).

The Patient Identifier Cross-reference Manager Actor shall be capable of accepting multiple concurrent
PIX Query requests (Get Corresponding Identifiers messages) and responding correctly using the Return
Corresponding Identifiers message.

3.9.4.2 Return Corresponding Identifiers

1260 ### 3.9.4.2.1 Trigger Events

The Patient Identifier Cross-reference Manager's response to the Get Patient Identifiers message will
trigger the following message:
- K23 – Corresponding patient identifiers

3.9.4.2.2 Message Semantics

1265 The Return Corresponding Identifiers transaction is conducted by the HL7 RSP^K23 message. The
Patient Identifier Cross-reference Manager Actor shall generate this message in direct response to the
QBP^Q23 query message previously received. This message satisfies the Application Level, Original
Mode Acknowledgement for the HL7 QBP^Q23 message. The segments of the message listed without
enclosing square brackets in the Table below are required. Detailed descriptions of all segments listed in
1270 the table below are provided in the following subsections. Other segments of the message are optional.

Note: Conventions used in this section as well as additional qualifications to the level of specification and HL7 profiling are stated in
Appendix C and C.1 in this Volume.

Table 3.9-3 RSP Segment Pattern Response

RSP	Segment Pattern Response	Chapter in HL7 2.5
MSH	Message Header	2
MSA	Message Acknowledgement	2
[ERR]	Error segment	2
QAK	Query Acknowledgement	5

RSP	Segment Pattern Response	Chapter in HL7 2.5
QPD	Query Parameter Definition	5
[PID]	Patient Identification	3

3.9.4.2.2.1 MSH Segment

1275 The MSH segment shall be constructed as defined in Appendix C.1.2, "Message Control".

Field *MSH-9-Message Type* shall have at least two components. The first component shall have a value of RSP; the second component shall have the value of K23. The third component is optional; however, if present, it shall have a value of RSP_K23.

3.9.4.2.2.2 MSA Segment

1280 The Patient Identifier Cross-reference Manager Actor is not required to send any attributes within the MSA segment beyond what is specified in the HL7 standard. See Appendix C.1.3 for the list of all required and optional fields within the MSA segment.

3.9.4.2.2.3 QAK Segment

The Patient Identifier Cross-reference Manager Actor shall send attributes within the QAK segment as
1285 defined in Table 3.9-4. For the details on filling in QAK-2 (Query Response Status) refer to Section 3.9.4.2.2.6.

Table 3.9-4 IHE Profile - QAK segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	32	ST	R		00696	Query Tag
2	2	ID	R+	0208	00708	Query Response Status

Adapted from the HL7 standard, version 2.5

3.9.4.2.2.4 QPD Segment

1290 The Patient Identifier Cross-reference Manager Actor shall echo the QPD Segment value that was sent in the QBP^Q23 message.

3.9.4.2.2.5 PID Segment

The Patient Identifier Cross-reference Manager Actor shall return only those attributes within the PID segment that are required by the HL7 standard: *PID-3-Patient IdentifierList* and *PID-5-Patient Name*.

1295 The PID segment is returned only when the Patient Identifier Cross-reference Manager Actor recognizes the specified Patient Identification Domain and Patient ID and an identifier exists for the specified patient in at least one other domain. See Section 3.9.4.2.2.6, "Patient Identifier Cross-reference Manager Actor Query Response Behavior," for a detailed description of how the Patient Identifier Cross-reference Manager Actor responds to the query request under various circumstances.

1300 The Patient Identifier Cross-reference Manager Actor shall use the field PID-3 Patient Identifier List to convey the Patient ID uniquely identifying the patient within each Patient Identification Domain for which a Patient ID exists for the specified patient. Each resulting ID returned in PID-3 shall include a

fully qualified Assigning Authority component. In other words, the Assigning Authority component returned shall include ALL subcomponents (namespace ID, Universal ID, and Universal ID type).

1305 To eliminate the issue of conflicting name values between Patient Identifier Domains, the Patient Identifier Cross-reference Manager Actor shall return in an empty (not present) value in the first repetition of field PID-5-Patient Name, and shall return a second repetition of field *PID-5-Patient Name* in which the only populated component is Component 7 (Name Type Code). Component 7 of repetition 2 shall contain a value of S (Coded Pseudo-name to assure anonymity). All other components of
1310 repetition 2 shall be empty (not present).

3.9.4.2.2.6 Patient Identifier Cross-reference Manager Actor Query Response Behavior

It is wholly the responsibility of the Patient Identifier Cross-reference Manager Actor to perform the matching of patient identifiers based on the patient traits it receives. The information provided by the Patient Identifier Cross-reference Manager Actor to Patient Identifier Cross-reference Consumer Actors
1315 is a list of cross-referenced identifiers in two or more of the domains managed by the cross-referencing Actor. The list of cross-references is not made available until the set of policies and processes for managing the cross-reference function have been completed. The policies of administering identities adopted by the cooperating domains are completely internal to the Patient Identifier Cross-reference Manager Actor and are outside of the scope of this framework. Possible matches should not be
1320 communicated until the healthcare institution policies and processes embodied in the Patient Identifier Cross-reference Manager Actor reach a positive matching decision.

The Patient Identifier Cross-reference Manager Actor shall respond to the query request as described by the following 6 cases:

Case 1: The Patient Identifier Cross-reference Manager Actor recognizes the specified Patient
1325 Identification Domain and Patient ID sent by the Patient Identifier Cross-reference Consumer in QPD-3, and corresponding identifiers exist for the specified patient in at least one of the domains requested in QPD-4 (one identifier per domain). (See Case 6 below for the required behavior if there are multiple identifiers recognized within a given Identifier Domain by the Patient Identifier Cross-reference Manager Actor.)

1330 **AA** (application accept) is returned in MSA-1.

OK (data found, no errors) is returned in QAK-2.

A single PID segment is returned in which one repetition of *PID-3 Patient Identifier List* is populated for each of the domains, if any, that the Patient Identifier Cross-reference Manager Actor did recognize in which a single identifier exists for the requested patient, not including the queried-for patient
1335 identifier that is returned in QPD-3.

Case 2: The Patient Identifier Cross-reference Manager Actor recognizes the Patient Identification Domain and Patient ID sent in QPD-3, but no identifier exists for that patient in any of the domains sent in QPD-4.

AA (application accept) is returned in MSA-1.

1340 **NF** (no data found, no errors) is returned in QAK-2.

No PID segment is returned.

Case 3: The Patient Identifier Cross-reference Manager Actor recognizes the specified Patient Identification Domain sent in the fourth component of QPD-3, but does not recognize the Patient ID sent in the first component of QPD-3.

1345   **AE** (application error) is returned in MSA-1 and in QAK-2.

An ERR segment is returned in which the components of *ERR-1-Error Code* and Location are valued as follows.

COMP #	COMPONENT NAME	VALUE
1	Segment ID	QPD
2	Sequence	1
3	Field Position	3
4	Field Repetition	1
5	Component Number	1
6	Sub-Component Number	*(empty)*

As specified by HL7, *ERR-2.6-Sub-Component Number* is not valued because we are referring to the
1350   entire fourth component of field QPD-4.

ERR-3-HL7 Error Code is populated with the error condition code **204** (unknown key identifier). Together with the values in ERR-2, this signifies that the Patient Identifier Cross-reference Manager Actor did not recognize the value in the first component of QPD-3.

Case 4: The Patient Identifier Cross-reference Manager Actor does not recognize the Patient
1355   Identification Domain of the identifier sent in QPD-3.

AE (application error) is returned in MSA-1 and in QAK-2.

An ERR segment is returned in which the components of *ERR-2-Error Location* are valued as follows.

COMP #	COMPONENT NAME	VALUE
1	Segment ID	QPD
2	Sequence	1
3	Field Position	3
4	Field Repetition	1
5	Component Number	4
6	Sub-Component Number	*(empty)*

As specified by HL7, *ERR-2.6-Sub-Component Number* is not valued because we are referring to the
1360   entire fourth component of field QPD-3.

ERR-3-HL7 Error Code is populated with the error condition code **204** (unknown key identifier). Together with the values in ERR-2, this signifies that the Patient Identifier Cross-reference Manager Actor did not recognize the value in the fourth component of QPD-3.

Case 5: The Patient Identifier Cross-reference Manager Actor does not recognize one or more of the
1365   Patient Identification Domains for which an identifier has been requested.

AE (application error) is returned in MSA-1 and in QAK-2.

For each domain that was not recognized, an ERR segment is returned in which the components of *ERR-2-Error Location* are valued as follows.

COMP #	COMPONENT NAME	VALUE
1	Segment ID	QPD
2	Sequence	1
3	Field Position	4
4	Field Repetition	*(see below)*
5	Component Number	*(empty)*
6	Sub-Component Number	*(empty)*

1370   As specified by HL7, *ERR-2.5-Component Number* and *ERR-2.6-Sub-Component Number* are not valued because we are referring to the entire field QPD-4.

ERR-3-HL7 Error Code* is populated with the error condition code **204** (unknown key identifier). Together with the values in ERR-2, this signifies that the Patient Identifier Cross-reference Manager Actor did not recognize the domain for the occurrence of *QPD-4-What Domains Returned* whose

1375   ordinal number is returned as an integer in ERR-2.4.

Case 6: The Patient Identifier Cross-reference Manager Actor recognizes the specified Patient Identification Domain and Patient ID sent by the Patient Identifier Cross-reference Consumer in QPD-3, and corresponding identifiers exist for the specified patient in at least one of the domains requested in QPD-4, and there are multiple identifiers within at least one of the requested domains.

1380   **AA** (application accept) is returned in MSA-1.

OK (data found, no errors) is returned in QAK-2.

A single PID segment is returned in which one repetition of *PID-3-Patient Identifier List* is populated for each of the identifiers, not including the queried-for patient identifier that is returned in QPD-3. If the Patient Identifier Cross-reference Manager Actor chooses to return multiple identifiers associated

1385   with the same domain, it shall return these identifiers grouped in successive repetitions within the *PID-3-Patient Identifier List*.

3.9.4.2.3 Expected Actions

The Patient Identifier Cross-reference Consumer will use the list of patient identifier aliases provided by the Patient Identifier Cross-reference Manger to perform the functions for which it requested the list.

1390   In the case where the returned list of identifiers contains multiple identifiers for a single domain, the Patient Identifier Cross-reference Consumer shall either use ALL of the multiple identifiers from the given domain or it shall ignore ALL of the multiple identifiers from the given domain.

This allows Patient Identifier Cross-reference Consumer Actors capable of handling multiple identities for a single patient within a single domain (i.e., those that can correctly aggregate the information

1395   associated with the different identifiers) to do so. For those Patient Identifier Cross-reference Consumer Actors not capable of handling this situation, ignoring the entire list of different identifiers prevents the consumer from presenting incomplete data.

3.9.5 Security Considerations

3.9.5.1 Audit Record Considerations

1400 The PIX Query Transaction is a Query Information event as defined in table 3.20.6-1. The Actors involved in the transaction shall create audit data in conformance with DICOM (Supp 95) "Query", with the following exceptions:

3.9.5.1.1 Patient Identifier Cross-reference Consumer audit message:

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110112, DCM, "Query")
	EventActionCode	M	"E" (Execute)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-9", "IHE Transactions", "PIX Query")
Source (Patient Identifier Cross-reference Consumer) (1)			
Human Requestor (0..n)			
Destination (Patient Identifier Cross-reference Manager) (1)			
Audit Source (Patient Identity Cross-reference Consumer) (1)			
Patient (0..n)			
Query Parameters(1)			

Where:

	Field Name	Opt	Value Constraints
Source **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Identifer Cross-reference Consumer Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human **Requestor (if** **known)** **AuditMessage/** **ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

1405

	UserID	M	The identity of the Patient Identifier Cross-reference Manager facility and receiving application from the HL7 message; concatenated together, separated by the | character.

	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source **AuditMessage/ AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Patient **(AudittMessage/ ParticipantObjectIdentifi cation)**	ParticipantObjectTypeCode	M	"1" (Person)
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
Query Parameters **(AudittMessage/ ParticipantObjectIdentifi cation)**	ParticipantObjectTypeCode	M	"2" (system object)
	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ITI-9", "IHE Transactions", "PIX Query")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	*U*	*not specialized*
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	the QPD segment of the query - Base64 encoded
	ParticipantObjectDetail	M	MSH-10 - the message identifier

3.9.5.1.2 Patient Identifier Cross-reference Manager audit message:

	Field Name	**Opt**	**Value Constraints**
Event **AuditMessage/ EventIdentification**	EventID	M	EV(110112, DCM, "Query")
	EventActionCode	M	"E" (Execute)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-9", "IHE Transactions", "PIX Query")
Source (Patient Identifier Cross-reference Manager) (1)			
Destination (Patient Identifier Cross-reference Consumer) (1)			
Audit Source (Patient Identifier Cross-reference Manager) (1)			
Patient (0..n)			
Query Parameters(1)			

Where:

Source **AuditMessage/ ActiveParticipant**	UserID	M	The identity of the Patient Identifer Cross-reference Consumer Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

1410

Destination **AuditMessage/ ActiveParticipant**	UserID	M	The identity of the Patient Identifier Cross-reference Manager facility and receiving application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source **AuditMessage/ AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Patient **(AudittMessage/ ParticipantObjectIdentifi cation)**	ParticipantObjectTypeCode	M	"1" (Person)
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
Query Parameters **(AudittMessage/ ParticipantObjectIdentifi cation)**	ParticipantObjectTypeCode	M	"2" (system object)
	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*Not specialized*
	ParticipantObjectIDTypeCode	M	EV("ITI-9", "IHE Transactions", "PIX Query")
	ParticipantObjectSensitivity	*U*	*Not specialized*
	ParticipantObjectID	*U*	*not specialized*
	ParticipantObjectName	*U*	*Not specialized*
	ParticipantObjectQuery	M	the QPD segment of the query - Base64 encoded
	ParticipantObjectDetail	M	MSH-10 - the message identifier

3.10 PIX Update Notification

1415   This section corresponds to Transaction ITI-10 of the IHE IT Infrastructure Technical Framework. Transaction ITI-10 is used by the Patient Identifier Cross-reference Consumer and Patient Identifier Cross-reference Manager actors.

3.10.1 Scope

This transaction involves the Patient Identifier Cross-reference Manager Actor providing notification of
1420   updates to patient identifier cross-reference associations to Patient Identifier Cross-reference Consumers that have registered (by configuration on the Cross-reference Manager) their interest in receiving such notifications. This transaction uses HL7's generic 'Update Person Information' message to communicate this patient-centric information.

3.10.2 Use Case Roles
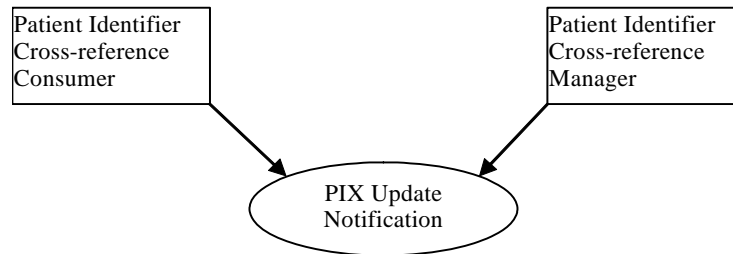
1425

Actor: Patient Identifier Cross-reference Manager

Role: It serves a well-defined set of Patient Identification Domains. The Patient Identifier Cross-reference Manager manages the cross-referencing of patient identifiers across Patient Identification Domains by providing a list of patient ID "aliases" via notification to a configured list of interested
1430   Patient Identifier Cross-reference Consumers.

Actor: Patient Identifier Cross-reference Consumer

Role: Receives notifications from the Patient Identifier Cross-reference Manager of changes to patient ID aliases. Typically the Patient Identifier Cross-reference Consumer Actor uses this information to maintain information links about patients in a different patient ID domain.

1435   ### 3.10.3 Referenced Standard

HL7 Version 2.5, Chapter 2 – Control, Chapter 3 – Patient Administration

HL7 version 2.5 was selected for this transaction for the following reason:

It was considered the most stable version that contained the functionality required by Transaction ITI-9 and ITI-10.

1440 **3.10.4 Interaction Diagram**
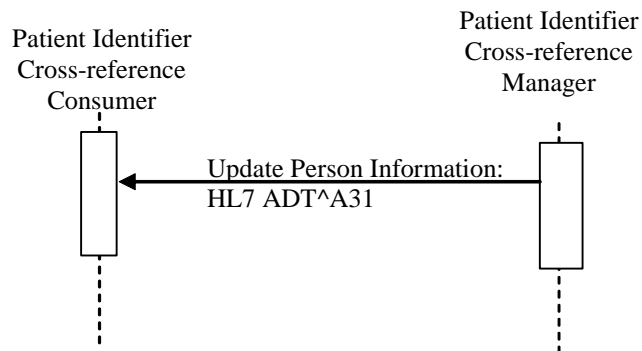
Figure 3.10-1 Update Person Information Sequence

3.10.4.1 Update Person Information

3.10.4.1.1   Trigger Events

1445 The Patient Identifier Cross-reference Manager shall notify a Patient Identifier Cross-reference Consumer when there is a change in a set of cross-referenced patient identifiers for any of the patient identifiers belonging to Patient Identifier Domains of interest to the consumer. The configuration of the domains of interest to a Patient Cross-reference Consumer is maintained by the Patient Cross-reference Manager Actor.

1450 Several notifications may have to be issued to communicate a single update to a set of cross-reference patient identifiers as required to reflect all the changes on the resulting sets of cross-reference patient Identifiers belonging to Patient Identifier Domains of interest to the Patient Identifier Cross-referencing Consumer.

The following HL7 trigger event will be used to update to the list of patient identifiers:

1455 • A31 – Update Person Information

3.10.4.1.2   Message Semantics

The PIX Update Notification transaction is conducted by the ADT^A31 message. The Patient Identifier Cross-reference Manager Actor initiates this transaction whenever identifier list information is updated for a patient.

1460 It is wholly the responsibility of the Patient Identifier Cross-reference Manager Actor to perform the matching of patient identifiers based on the patient traits it receives. The information provided by the Patient Identifier Cross-reference Manager Actor to Patient Identifier Cross-reference Consumer Actors shall only contain a list of cross-referenced identifiers for the domains of interest as configured with the Patient Identifier Cross-reference Manager actor in two or more of the domains managed by the cross-
1465 referencing Actor. Multiple notifications may need to be sent. For example:

Consumer CON_A is configured to receive update notifications for domains DOM_A and DOM_AD. Notifications are sent as follows:

- A PIX A01 feed is send for a patient for DOM_A. The update notification shall contain the patient identifier and assigning authority for DOM_A.

1470
- A PIX A01 feed is processed for DOM_AD. The Patient Identifier Cross-reference Manager cross references this patient with DOM_A. The update notification shall contain the patient identifier and assigning authority for DOM_A and DOM_AD.

- A PIX A08 feed is processed for DOM_AD changing the patient address. The Patient Identifier Cross-reference Manager cross references determines this patient is no longer the
1475 same patient as DOM_A. Two update notifications shall be sent. One containing the patient identifier and assigning authority for DOM_A. The other one containing the patient identifier and assigning authority for DOM_AD.

The list of cross-references is not made available until the set of policies and processes for managing the cross-reference function have been completed. The policies of administering identities adopted by the
1480 cooperating domains are completely internal to the Patient Identifier Cross-reference Manager Actor and are outside of the scope of this standard. Possible matches should not be communicated until the healthcare institution policies and processes embodied in the Patient Identifier Cross-reference Manager Actor reach a positive matching decision.

The Patient Identifier Cross-reference Manager Actor Configuration is expected to have configuration
1485 indicating which Identity Consumers are interested in receiving the PIX Update Notification Transactions. This configuration information shall include identification of the identity consumer systems interested in receiving notifications and, for each of those systems, a list of the patient identifier domains of interest. The Patient Identifier Cross-reference Manager Actor should account for consumers interested in all domains.

1490 The segments of the message listed in the Table below are required. Other segments are optional.

Table 3.10-1 ADT Patient Administration Message

ADT	Patient Administration Message	Chapter in HL7 2.5
MSH	Message Header	2
EVN	Event Type	3
PID	Patient Identification	3
PV1	Patient Visit	3

Each message shall be acknowledged by the HL7 ACK message sent by the receiver of ADT message to its sender. See Appendix C.1.3, "Acknowledgement Modes" for the definition and discussion of the ACK message.

1495 **3.10.4.1.2.1 MSH Segment**

The MSH segment shall be constructed as defined in Appendix C.1.2, "Message Control".

Field *MSH-9 Message Type* shall have at least two components. The first component shall have a value of ADT; the second component shall have the value of A31. The third component is optional; however, if present, it shall have a value of ADT_A05.

1500 ### 3.10.4.1.2.2 EVN Segment

See Appendix C.1.4 for the list of all required and optional fields within the EVN segment.

3.10.4.1.2.3 PID Segment

The Patient Identifier Cross-reference Manager Actor shall provide only those attributes within the PID segment that are required by the HL7 standard: *PID-3-Patient Identifier List* and *PID-5-Patient Name*.

1505 The Patient Identifier Cross-reference Manager Actor shall use the field *PID-3 Patient Identifier List* to convey the Patient IDs uniquely identifying the patient within each Patient Identification Domain for which a Patient ID exists for the specified patient. Each resulting ID returned in PID-3 shall include a fully qualified Assigning Authority component. In other words, the Assigning Authority component returned shall include ALL subcomponents (namespace ID, Universal ID, and Universal ID type).

1510 To eliminate the issue of multiple name values between Patient Identifier Domains, the Patient Identifier Cross-reference Manager Actor shall return a single space character in field *PID-5-Patient Name*.

A single PID segment is sent in which one repetition of *PID-3-Patient Identifier List* is populated for each of the identifiers in the notification. If the Patient Identifier Cross-reference Manager Actor chooses to send multiple identifiers associated with the same domain, it shall return these identifiers 1515 grouped in successive repetitions within the *PID-3-Patient Identifier List*.

3.10.4.1.2.4 PV1 Segment

As is specified by the HL7 Standard, Version 2.5, the PV1 Segment is required. The required field *PV1-2-patient class* shall contain **N** (not applicable) to indicate the transmission of patient information outside the context of a visit or encounter. Other fields shall be left blank.

1520

Table 3.10-2 IHE Profile – PV1 segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
2	1	IS	R	0004	00132	Patient Class

Adapted from the HL7 Standard, version 2.5

3.10.4.1.3 Expected Actions

The Patient Identifier Cross-reference Consumer, when it receives the ADT^A31 message, shall update 1525 its internal identifier information for the affected patient(s) in all domains in which it is interested whenever it receives updated identifier information that results in a change to the cross-referencing of a patient.

In the case where the returned list of identifiers contains multiple identifiers for a single domain, the Patient Identifier Cross-reference Consumer shall either use ALL of the multiple identifiers from the 1530 given domain or it shall ignore ALL of the multiple identifiers from the given domain.

This allows Patient Identifier Cross-reference Consumer Actors capable of handling multiple identities for a single patient within a single domain (i.e., those that can correctly aggregate the information associated with the different identifiers) to do so. For those Patient Identifier Cross-reference Consumer Actors not capable of handling this situation, ignoring the entire list of different identifiers prevents the 1535 consumer from presenting incomplete data.

3.10.5 Security Considerations

3.10.5.1 Audit Record Considerations

The PIX Update Notification Transaction is "Patient Record" event, as defined in table 3.20.6-1. The Actors involved in the transaction shall create audit data in conformance with DICOM (Supp 95) 1540 "Patient Record", with the following exceptions:

3.10.5.1.1 Patient Identifier Cross-reference Manager audit message:

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110110, DCM, "Patient Record")
	EventActionCode	M	"R" (Read)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-10", "IHE Transactions", "PIX Update Notification")
Source (Patient Identifier Cross-reference Manager) (1)			
Human Requestor (0..n)			
Destination (Patient Identifier Cross-reference Consumer) (1)			
Audit Source (Patient Identifier Cross-reference Manager) (1)			
Patient IDs(1..n) (represents the components of PID-3)			
Where:			
Source **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Identifer Cross-reference Manager Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*Not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human Requestor (if known) **AuditMessage/** **ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*Not specialized*
	UserName	*U*	*Not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

	UserID	M	The identity of the Patient Identifier Cross-reference Consumer facility and receiving application from the HL7 message; concatenated together, separated by the | character.

	AlternativeUserID	U	Not specialized
	UserName	U	Not specialized
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source **AuditMessage/ AuditSourceIdentification**	AuditSourceID	U	Not specialized.
	AuditEnterpriseSiteID	U	Not specialized
	AuditSourceTypeCode	U	Not specialized

1545

Patient IDs **(AudittMessage/ ParticipantObjectIdentifi cation)**	ParticipantObjectTypeCode	M	"1" (Person)
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	U	Not specialized
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	the patient ID in HL7 CX format.
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	M	MSH-10 - the message identifier

3.10.5.1.2 Patient Identifier Cross-reference Consumer audit message:

	Field Name	**Opt**	**Value Constraints**
Event **AuditMessage/ EventIdentification**	EventID	M	EV(110110, DCM, "Patient Record")
	EventActionCode	M	"U" (update)
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	EV("ITI-10", "IHE Transactions", "PIX Update Notification")
Source (Patient Identifier Cross-reference Manager) (1)			
Destination (Patient Identifier Cross-reference Consumer) (1)			
Audit Source (Patient Identifier Cross-reference Consumer) (1)			
Patient IDs(1..n) (represents the components of PID-3)			

Where:

Source **AuditMessage/ ActiveParticipant**	UserID	M	The identity of the Patient Identifer Cross-reference Manager Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

	UserID	M	The identity of the Patient Identifier Cross-reference Consumer facility and receiving application from the HL7 message; concatenated together, separated by the | character.

	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	U	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source	*AuditSourceID*	U	*Not specialized.*
AuditMessage/ AuditSourceIdentification	*AuditEnterpriseSiteID*	U	*not specialized*
	AuditSourceTypeCode	U	*not specialized*

1550

Patient IDs	ParticipantObjectTypeCode	M	"1" (Person)
(AudittMessage/ ParticipantObjectIdentifi cation)	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	U	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	U	*not specialized*
	ParticipantObjectID	M	the patient ID in HL7 CX format.
	ParticipantObjectName	U	*not specialized*
	ParticipantObjectQuery	U	*not specialized*
	ParticipantObjectDetail	M	MSH-10 - the message identifier

3.11 Retrieve Specific Information for Display

This section corresponds to Transaction ITI-11 of the IHE IT Infrastructure Technical Framework. Transaction ITI-11 is used by the Information Source and Display actors.

1555 **3.11.1 Scope**

This transaction involves the query of information for presentation purposes. This may occur when a user attempts to lookup information associated with certain patient that is stored on a different system. Note that the retrieved 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
1560 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.

To support a wide range of display capabilities, the information provided is formatted into well-formed XHTML. Such formatting shall be done using XHTML Basic and W3C HTML Compatibility Guidelines provided in the Appendix C of the W3C XHTML 1.0 Recommendation.

1565 **3.11.2 Use Case Roles**
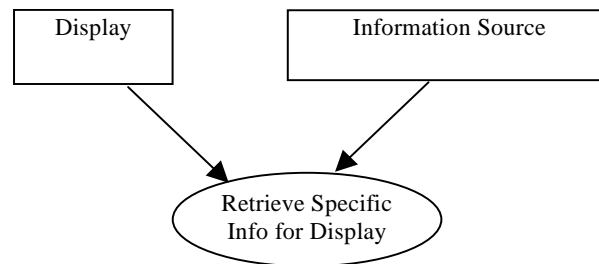
Actor: Display

Role: A system that requests specific information for display, and displays it.

1570 **Actor:** Information Source

Role: A system that provides specific information in response to the request from the Display Actor, in a presentation-ready format.

3.11.3 Referenced Standards

IETF RFC1738, Uniform Resource Locators (URL), December 1994,
1575   http://www.faqs.org/rfcs/rfc1738.html

IETF RFC2616 HyperText Transfer Protocol HTTP/1.1

Extensible Markup Language (XML) 1.0 (Second Edition). W3C Recommendation 6 October 2000. http://www.w3.org/TR/REC-xml.

Web Services Description Language (WSDL) 1.1. W3C Note 15 March 2001.
1580 http://www.w3.org/TR/wsdl.

XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition).A Reformulation of HTML 4 in XML 1.0. W3C Recommendation 26 January 2000, revised 1 August 2002. http://www.w3.org/TR/xhtml1.

XHTML™ Basic. W3C Recommendation 19 December 2000. http://www.w3.org/TR/xhtm-basic.

1585   http://www.w3.org/TR/xhtml-basicInteraction Diagram

Figure 3.11-1 Request For Specific Information – Summary sequence

3.11.3.1 Request For Specific Information - Summary

3.11.3.1.1   Trigger Events

1590   The following event will trigger a Request for Specific Information:

- User of the Display Actor needs to review a summary list of information/ reports that are part of a patient's clinical history (i.e., summary of lab reports, summary of radiology exam reports, etc.) with the intent of selecting a specific item off the list for subsequent retrieval as a persistent object via the Retrieve Document for Display Transaction

1595   **3.11.3.1.2   Message Semantics**

The Retrieve Specific Information for Display transaction is performed by the invocation of a web service. The Display Actor shall generate a web service request whenever a user needs to review the information stored as part of a patient's clinical history on the Information Source Actor.

To specify the type of information that needs to be returned, a web service request shall include the
1600   following parameters (keys) to filter the subset of information (See Table 3.11.4-1). All parameter names and values (see Table 3.11.4-2) are case-sensitive.

Table 3.11.4-1 Web Service Request Keys

Parameter Name	REQ	Description	Notes
requestType	R	requestType specifies what type of information shall be retrieved. This parameter shall always be valued.	See Table 3.11.4-2 for the list of possible values.
patientID	R	This attribute identifies the subject of the results being queried for. Its value shall include identification of assigning authority.	PatientID value shall be formatted as HL7 CX data type (including assigning authority) according to the requirements specified for the Patient Identity Feed transaction (see Section 3.8.4.1.2.3)
lowerDateTime	O	Used to constrain the earliest date/time of creation of information.	This value shall be encoded in the XML primitive dateTime format.
upperDateTime	O	Used to constrain the latest date/time of creation of information.	This value shall be encoded in the XML primitive dateTime format.
mostRecentResults	R	The numeric value that indicates the number of most recent results to be included into the response, *i.e.*, 1 indicates to provide the latest result.	Value of 0 indicates that all available results shall be returned.

1605   **Table 3.11.4-2 Web Service Request Types**

requestType value	Description
SUMMARY	Summary of all reports known to the Information Source
SUMMARY-RADIOLOGY	Summary of radiology reports
SUMMARY-CARDIOLOGY	Summary of cardiology reports
SUMMARY-LABORATORY	Summary of laboratory reports
SUMMARY-SURGERY	Summary of surgery reports
SUMMARY-EMERGENCY	Summary of emergency reports
SUMMARY-DISCHARGE	Summary of discharge reports
SUMMARY-ICU	Summary of intensive care reports
SUMMARY-RX	Summary of Prescriptions

Note: parameter values that contain reserved characters need to be encoded using %<hex><hex> notation. Reserved characters include slash (/, encode as %2f) and ampersand (&, encode as %26).

Formal definition of the web service in WSDL is provided in the Appendix A.

The only binding required for both the Display Actor and Information Source Actor is the binding to the
1610 HTTP-GET. In this binding the sample message will be formatted as follows:

http://<location>/IHERetrieveSummaryInfo?requestType=SUMMARY&patientID=99998410^^^%26w
ww.mlhlife.com%26DNS &lowerDateTime=2003-01-01T00:00:00&upperDateTime=2003-01-
01T23:59:59&mostRecentResults=1

The <location> part of the URL is configurable by the implementation, and must contain the host name,
1615 an optional port address, and may be followed by an optional path. The path if present may not contain
a '?' character. The remainder of the URL, including IHERetrieveSummaryInfo and the following
request parameters are specified by the WSDL and may not be changed.

More specifically, using the definitions from RFC 1738, the <location> part of the URL must match the production for location from the figure below:

```
1620   location        = hostport [ "/" hpath ]

       hostport        = host [ ":" port ]
       host            = hostname | hostnumber
       hostname        = *[ domainlabel "." ] toplabel
1625   domainlabel     = alphadigit | alphadigit *[ alphadigit | "-" ] alphadigit
       toplabel        = alpha | alpha *[ alphadigit | "-" ] alphadigit
       alphadigit      = alpha | digit
       hostnumber      = digits "." digits "." digits "." digits
       port            = digits
1630
       hpath           = hsegment *[ "/" hsegment ]
       hsegment        = *[ uchar | ";" | ":" | "@" | "&" | "=" ]
       lowalpha        = "a" | "b" | "c" | "d" | "e" | "f" | "g" | "h" |
                         "i" | "j" | "k" | "l" | "m" | "n" | "o" | "p" |
1635                     "q" | "r" | "s" | "t" | "u" | "v" | "w" | "x" |
                         "y" | "z"
       hialpha         = "A" | "B" | "C" | "D" | "E" | "F" | "G" | "H" | "I" |
                         "J" | "K" | "L" | "M" | "N" | "O" | "P" | "Q" | "R" |
                         "S" | "T" | "U" | "V" | "W" | "X" | "Y" | "Z"
1640
       alpha           = lowalpha | hialpha
       digit           = "0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" |
                         "8" | "9"
       safe            = "$" | "-" | "_" | "." | "+"
1645   extra           = "!" | "*" | "'" | "(" | ")" | ","

       hex             = digit | "A" | "B" | "C" | "D" | "E" | "F" |
                         "a" | "b" | "c" | "d" | "e" | "f"
       escape          = "%" hex hex
1650
       unreserved      = alpha | digit | safe | extra
       uchar           = unreserved | escape
```

The following location values are legal according to this specification:

<location> value	Resulting URL
Myhost	http://myhost/IHERetrieveSummaryInfo?…
myhost:8080	http://myhost:8080/IHERetrieveSummaryInfo?…
myhost/MyAspPageThatLooksLikeItCouldBeAFolder.aspx	http://myhost/MyAspPageThatLooksLikeItCouldBeAFolder.aspx/IHERetrieveSummaryInfo?…
myhost:8080/MyAspPageThatLooksLikeItCouldBeAFolder.aspx	http://myhost:8080/MyAspPageThatLooksLikeItCouldBeAFolder.aspx/IHERetrieveSummaryInfo?…
myhost/MyJspPage.jsp	http://myhost/MyJspPage.jsp/IHERetrieveSummaryInfo?…
myhost:8080/MyJspPageThatLooksLikeItCouldBeAFolder.jsp	http://myhost/MyJspPage.jsp/ IHERetrieveSummaryInfo?…

1655   The following location values are not legal:

<location> value	Resulting URL
My+Computer	'+' is not a legal character in a host name.

myhost:99999	99999 is not a valid port.
myhost/myPath.jsp?request=	'?' is not valid in a path.

In addition, the Display Actor shall support the following field of the HTTP request:

Table 3.11.4-3 HTTP Request and Response Fields

HTTP Field	REQ	Description	Values
Accept-Language	O	This field restricts the set of natural languages that are preferred as a response to the request.	Any valid value according to RFC2616

1660   The Information Source actor shall support the following field of the HTTP response.

Table 3.11.4-4 HTTP Response Fields

HTTP Field	REQ	Description	Values
Expires	R	This field gives the date/time after which the response is considered stale	Shall be 0. This is now deprecated usage, but it is the widely supported means of specifying no cacheing.
Cache-Control	R	This field indicates that this response should not be cached.	Shall be no-cache

If necessary, the Display Actor may perform the request to the web service utilizing HTTPS protocol.

Information Source Actors may return HTTP redirect responses (responses with values of 301, 302, 303 or 307) in response to a request. Display Actors can expect to receive an error response, or the data
1665   requested, or a request to look elsewhere for the data. A Display Actor must follow redirects, but if a loop is detected, it may report an error.

3.11.3.1.3   Expected Actions

Upon reception of the Request for Specific Information, the Information Source Actor shall parse the request and if there are no errors, return the Response with Specific Information as specified in Section
1670   3.11.4.2, and HTTP response code 200 - OK.

To specify the type of information that needs to be processed, an Information Source Actor shall support the following parameters (keys) to filter the subset of information (See Table 3.11.4-5).

Table 3.11.4-5 Web Service Request Keys

Parameter Name	REQ	Description	Notes
requestType	R	requestType specifies what type of information shall be retrieved. This parameter shall always be valued.	See Table 3.11.4-2 for the list of possible values.
patientID	R	This attribute identifies the subject of the results being queried for. Its value shall include identification of assigning authority.	PatientID value shall be formatted as HL7 CX data type (including assigning authority) according to the requirements specified for the Patient Identity Feed transaction (see Section 3.8.4.1.2.3)
lowerDateTime	R	Used to constrain the earliest date/time of creation of information.	This value shall be encoded in the XML primitive dateTime format.
upperDateTime	R	Used to constrain the latest date/time of creation of information.	This value shall be encoded in the XML primitive dateTime format.
mostRecentResults	R	The numeric value that indicates the number of most recent results to be included into the response, *i.e.*, 1 indicates to provide the latest result.	Value of 0 indicates that all available results shall be returned.

1675

If the requestType specified is not supported, the Information Source Actor shall return HTTP response-code 404 (not found) with the suggested reason-phrase "requestType not supported".. If the Information Source Actor is not able to format the document in any content types listed in the 'Accept' field, it shall return HTTP response code 406 – Not Acceptable.

1680 If the Patient ID specified by the Display Actor is not known to the Information Source Actor, it shall return HTTP response-code 404 (not found) with the suggested reason-phrase "Patient ID not found". If the Display Actor provides the Patient ID from a different domain than the one the Information Source Actor belongs to, and the Information Source Actor is grouped with the Patient ID Consumer Actor, it may attempt to obtain a mapping of the provided Patient ID into its domain before responding.

1685   Note: Other HTTP response codes may be returned by the Information Source Actor, indicating conditions outside of the scope of this profile, for example, 401 – Authentication Failed might be returned if Information Source Actor is grouped with the Kerberized Server Actor.

    Note: It is recommended that the Information Source Actor complement the returned error code with a human readable description of the error condition.

1690 If an error condition cannot be automatically recovered, at a minimum, the error should be displayed to the user by the Display Actor.

If lowerDateTime and/or upperDateTime parameters are specified, they shall define the lower and/or upper inclusive boundary of the temporal range in which returned information should have been created. The value of the mostRecentResults parameter shall be interpreted within such specified date/time
1695 range.

3.11.3.2 Response with Specific Information - Summary

3.11.3.2.1 Trigger Events

This message is sent by the Information Source Actor in response to the Request For Specific Information web service request.

1700 #### 3.11.3.2.2 Message Semantics

Information Source Actor shall support at least one of the values of the requestType parameter specified in Table 3.11.4-2.

The Information Source shall set an expiration of zero to ensure no caching. The message shall be formatted using XHTML Basic and W3C HTML Compatibility Guidelines provided in the Appendix C
1705 of the W3C XHTML 1.0 Recommendation.

The Display Actor may request the Information Source Actor to provide any specific information including a summary of reports of different types pertaining to a particular patient. The exact content of the summary is determined by the Information Source Actor and may be regulated by the institution policy. For example, it may contain the hyperlink to a persistent object so that it can be retrieved by
1710 using the Retrieve Document for Display Transaction. In the case of retrieving a summary of documents (requestType of SUMMARY[-xx]), it is strongly recommended to include a link to the relevant documents, for each item of the summary. If present, the link will have to be formatted as a web service request in accordance to the requirements in Section 3.12. It may also contain a hyperlink representing the invocation of the Request for Specific Information for display, as specified in this Section.

1715 #### 3.11.3.2.3 Expected Actions

The Display Actor shall render the received response for the user. It shall not assume that the content of the document may be meaningfully parsed beyond determination of XHTML tags necessary for accurate presentation of provided information.

When the summary responses include links to documents or other specific information, Information
1720 Source Actors are strongly encouraged to format them according to the requirements stated in Sections 3.11 and 3.12, to facilitate retrieval of information from other information sources.

3.11.3.3 Request For Specific Information - List

3.11.3.3.1 Trigger Events

The following event will trigger a Request for Specific Information:

1725 • User of the Display Actor needs to review a particular subset of information that is part of a patient's clinical history (i.e., lab report, radiology exam report, list of medications, etc.) that is stored on the Information Source system.

3.11.3.3.2 Message Semantics

The Retrieve Specific Information for Display transaction is performed by the invocation of a web
1730 service. The Display Actor shall generate a web service request whenever a user needs to review the information stored as part of a patient's clinical history on the Information Source Actor.

To specify the type of information to be returned, a web service request shall include the following parameters (keys) to filter the subset of information (See Table 3.11.4-7). All parameter names and values (see Table 3.11.4-7) are case-sensitive.

1735

Table 3.11.4-6 Web Service Request Keys

Parameter Name	REQ	Description	Notes
requestType	R	requestType specifies what type of information shall be retrieved. This parameter shall always be valued.	See Table 3.11.4-7 for the list of possible values.
patientID	R	This attribute identifies the subject of the results being queried for. Its value shall include identification of assigning authority.	PatientID value shall be formatted as HL7 CX data type (including assigning authority) according to the requirements specified for the Patient Identity Feed transaction (see Section 3.8.4.1.2.3)

Table 3.11.4-7 Web Service Request Types

requestType value	Description
LIST-ALLERGIES	List of allergies and adverse reactions for a patient known to the Information Source
LIST-MEDS	List of medications currently taken by or administered to a patient

Formal definition of the web service in WSDL is provided in the Appendix A.

1740   The only binding required for both Display Actor and Information Source Actor is the binding to the HTTP-GET. In this binding the sample message will be formatted as follows:

http://<location>/IHERetrieveListInfo?requestType=LIST-MEDS&patientID=99998410^^^%26www.mlhlife.com%26DNS

The <location> part of the URL is configurable by the implementation, and must contain the host name, an optional port address, and may be followed by an optional path. The path if present may not contain a '?' character. The remainder of the URL, including IHERetrieveListInfo and the following request parameters are specified by the WSDL and may not be changed. See the discussion about location in section 3.11.4.1.2 Message Semantics above.

In addition, the Display Actor shall support the following field of the HTTP request:

1750

Table 3.11.4-8 HTTP Request and Response Fields

HTTP Field	REQ	Description	Values
Accept-Language	O	This field restricts the set of natural languages that are preferred as a response to the request.	Any valid value according to RFC2616

The Information Source actor shall support the following field of the HTTP response.

Table 3.11.4-9 HTTP Request Fields

HTTP Field	REQ	Description	Values
Expires	R	This field gives the date/time after which the response is considered stale	Shall be 0. This is now deprecated usage, but it is the widely supported means of specifying no cacheing.

HTTP Field	REQ	Description	Values
Cache-Control	R	This field indicates that this response should not be cached.	Shall be no-cache

If necessary, the Display Actor may perform the request to the web service utilizing HTTPS protocol.

1755 Information Source Actors may return HTTP redirect responses (responses with values of 301, 302, 303 or 307) in response to a request. Display Actors can expect to receive an error response, or the data requested, or a request to look elsewhere for the data. A Display Actor must follow redirects, but if a loop is detected, it may report an error.

3.11.3.3.3   Expected Actions

1760 Upon reception of the Request for Specific Information, the Information Source Actor shall parse the request and if there are no errors, shall return the Response with Specific Information as specified in Section 3.11.4.2, and HTTP response code 200 - OK.

If the requestType specified is not supported, the Information Source Actor shall return HTTP response-code 404 (not found) with the suggested reason-phrase "requestType not supported". If the Information
1765 Source Actor is not able to format the document in any content types listed in the 'Accept' field, it shall return HTTP response code 406 – Not Acceptable.

If the Patient ID specified by the Display Actor is not known to the Information Source Actor, it shall return HTTP response-code 404 (not found) with the suggested reason-phrase "Patient ID not found". If the Display Actor provides the Patient ID from a different domain than the one the Information Source
1770 Actor belongs to, and the Information Source Actor is grouped with the Patient ID Consumer Actor, it may attempt to obtain a mapping of the provided Patient ID into its domain before responding.

> Note: Other HTTP response codes may be returned by the Information Source Actor, indicating conditions outside of the scope of this profile, for example, 401 – Authentication Failed might be returned if Information Source Actor is grouped with the Kerberized Server Actor.

1775   Note: It is recommended that the Information Source Actor complement returned error code with a human readable description of the error condition.

If an error condition cannot be automatically recovered, at a minimum, the error should be displayed to the user by the Display Actor.

3.11.3.4 Response with Specific Information - List

1780 #### 3.11.3.4.1   Trigger Events

This message is sent by the Information Source Actor in response to the Request For Specific Information web service request.

3.11.3.4.2   Message Semantics

Information Source Actor shall support at least one of the values of the requestType parameter specified
1785 in Table 3.11.4-7.

The Information Source shall set an expiration of zero to ensure no caching. The message shall be formatted using XHTML Basic and W3C HTML Compatibility Guidelines provided in the Appendix C of the W3C XHTML 1.0 Recommendation.

1790 The Display Actor may request the Information Source Actor to provide a list of information items (pertaining to a particular patient) that the Information Source has presently recorded. The exact content of the list is determined by the Information Source Actor.

The Display Actor shall not use the lowerDateTime, upperDateTime or mostRecentResults parameters in a query. The Information Source shall ignore them if they are specified.

3.11.3.4.3 Expected Actions

1795 The Display Actor shall render the received response for the user. It shall not assume that the content of the document may be meaningfully parsed beyond determination of XHTML tags necessary for accurate presentation of provided information.

3.12 Retrieve Document for Display

This section corresponds to Transaction ITI-12 of the IHE IT Infrastructure Technical Framework.
1800   Transaction ITI-12 is used by the Information Source and Display actors.

3.12.1 Scope

This transaction involves the retrieval of a document (persistent object) for presentation purposes. The uniquely identifiable persistent object means that retrieving the same document instance at a different point in time will provide the same semantics for its presented content. The information content of the
1805   document is immutable even if the presentation of such content is provided with the use of different formats, stylesheets, etc.

3.12.2 Use Case Roles
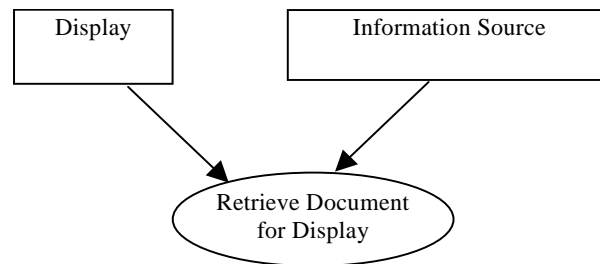
1810   **Actor:** Display

Role: A system that requests a document/object for display, and displays it.

Actor: Information Source

Role: A system that provides specific information in response to the request from the Display Actor, in a presentation-ready format.

1815   ### 3.12.3 Referenced Standards

IETF RFC2616 HyperText Transfer Protocol HTTP/1.1

Extensible Markup Language (XML) 1.0 (Second Edition). W3C Recommendation 6 October 2000.
http://www.w3.org/TR/REC-xml.

Web Services Description Language (WSDL) 1.1. W3C Note 15 March 2001.
1820   http://www.w3.org/TR/wsdl.

3.12.4 Interaction Diagram
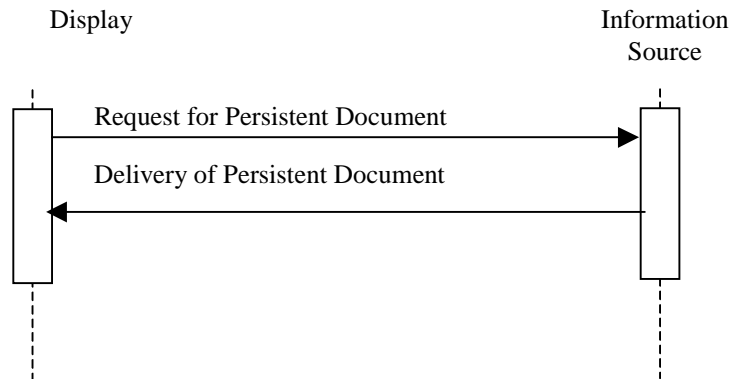
Figure 3.12-1 Request for Persistent Document Sequence

3.12.4.1 Request for Persistent Document

1825 **3.12.4.1.1   Trigger Events**

The request for a document is triggered when a user of the Display Actor needs to review a particular document that is stored by the Information Source Actor.

3.12.4.1.2   Message Semantics

The Retrieve Document for Display transaction is performed by the invocation of a web service. The
1830 Display Actor shall generate the web service request whenever a user needs to review the document stored as part of a patient's clinical history on the Information Source Actor.

The web service request shall include the following parameters (keys) to identify the document to be returned and its format See Table (3.12.4-1). All parameter names and values are case-sensitive.

Table 3.12.4-1 Query Keys

Parameter Name	REQ	Description	Values
requestType	R	This parameter is required to have a value of DOCUMENT.	DOCUMENT
documentUID	R	Identifies document's UID as known to both actors.	This value shall be a properly defined Object identifier (OID) as specified in Volume 2, Appendix B.
preferredContentType	R	This parameter is required to identify the preferred format the document is to be provided in (as MIME content type).	Display may specify one of the following formats: image/jpeg application/x-hl7-cda-level-one+xml (see note) application/pdf (see note)

1835   Note: see IANA registry for details about hl7-cda-level-one and PDF, such as version. Applications creating PDF may use this
MIME type for other versions of PDF up to 1.3. Receivers shall support document encoded in this version and previous
versions.

Note: see HL7 CDA framework release 1.0 for details about application/x-hl7-cda-level-one+xml.

1840   Formal definition of the web service in WSDL is provided in Appendix A.

The only binding required for both the Display Actor and Information Source Actor is the binding to the HTTP-GET. In this binding the sample message will be formatted as follows:

http://<location>/IHERetrieveDocument?requestType=DOCUMENT&documentUID=1.2.3&preferred ContentType=application%2fpdf

1845   The <location> part of the URL is configurable by the implementation, and must contain the host name, an optional port address, and may be followed by an optional path. The path if present may not contain a '?' character. The remainder of the URL, including IHERetrieveDocument and the following request parameters are specified by the WSDL and may not be changed. See the discussion about location in section 3.11.4.1.2 Message Semantics above.

1850   In addition, the Display Actor shall support the following fields of the HTTP request:

Table 3.12.4-3 HTTP Request and Response Fields

HTTP Field	REQ	Description	Values
Accept	O	This field may be used to specify certain media types which are acceptable for the response	At least one of the following values: image/jpeg application/x-hl7-cda-level-one+xml application/pdf */* Other values may be included as well
Accept-Language	O	This field is similar to Accept, but restricts the set of natural languages that are preferred as a response to the request.	Any valid value according to RFC2616
Expires	R	This field gives the date/time after which the response is considered stale	Any valid value according to RFC2616, or 0

The Information Source actor shall support the following field of the HTTP response.

Table 3.12.4-4 HTTP Response Fields

HTTP Field	REQ	Description	Values
Expires	R	This field gives the date/time after which the response is considered stale	Any valid value according to RFC2616, or 0

The Display Actor may provide list of content types it supports in the HTTP Accept field. If the HTTP
1855   Accept Field is absent, it means that any content type is acceptable by the Display Actor.

The preferredContentType parameter shall specify the content type desired by the Display Actor. The value of the preferredContentType parameter of the request shall be one of the values from the Table 3.12.4-1 and shall not contradict values specified in the HTTP Accept field.

The Information Source shall provide info in preferredContentType if capable, otherwise it shall only
1860   use a type specified in the Accept Field as appropriate given the information to be returned.

If necessary, the Display Actor may perform the request to the web service utilizing HTTPS protocol.

Information Source Actors may return HTTP redirect responses (responses with values of 301, 302, 303 or 307) in response to a request. Display Actors can expect to receive an error response, or the data requested, or a request to look elsewhere for the data. A Display Actor must follow redirects, but if
1865   a loop is detected, it may report an error.

3.12.4.1.3   Expected Actions

Upon reception of the Request for Specific Information, the Information Source Actor shall parse the request and shall return the retrieved document as specified in Section 3.12.4.2, and HTTP response code 200 - OK.

1870   If the requestType specified is a not a legal value according to this profile, the Information Source Actor shall return HTTP response-code 403 (forbidden) with the suggested reason-phrase "requestType not supported".

If the Information Source Actor is not able to format the document in any content types listed in the 'Accept' field, it shall return HTTP response code 406 – Not Acceptable.

1875   If the specified documentUID is not known to the Information Source Actor, it shall return HTTP response-code 404 (not found) with the suggested reason-phrase "Document UID not found".

If the documentUID, preferredContentType or requestType parameters are missing, the Information Source Actor shall return HTTP response code 400 - Bad Request.

If the documentUID or preferredContentType parameters are malformed, the Information Source Actor
1880   shall return HTTP response code 400 - Bad Request.

If the specified preferredContentType is not consistent with the setting of the HTTP Accept field, the Information Source Actor shall return HTTP response code 400 – Bad Request.

> Note: Other HTTP response codes may be returned by the Information Source Actor, indicating conditions outside of the scope of this profile, for example, 401 – Authentication Failed might be returned if Information Source Actor is grouped with the
1885   Kerberized Server Actor.

> Note: It is recommended that the Information Source Actor complement returned error code with a human readable description of the error condition.

If an error condition cannot be automatically recovered, at a minimum, the error should be displayed to the user by the Display Actor.

1890   ### 3.12.4.2 Delivery of Persistent Document

3.12.4.2.1   Trigger Events

The Delivery of Persistent Document message is the transmission of the requested document in specified format from the Information Source Actor to the Display Actor. This transmission will happen if such document, identified by the documentUID parameter in the request, has been successfully located by the
1895   Information Source Actor.

3.12.4.2.2   Message Semantics

In response to the request from the Display Actor, the Information Source Actor shall format the document according to the preferredContentType specified, and return it in the HTTP response. See Section 3.12.4.1.2 for a discussion of the rules related to preferredContentType.

1900   The Information Source Actor shall maintain global uniqueness of object identifiers.

The Information Source Actor shall set an expiration date compatible with the policies associated with the possible removal of instances of persistent documents (no more than a week).

3.12.4.2.3 Expected Actions

The Display Actor shall render the received document for the user.

1905

3.13 Follow Context

This section corresponds to Transaction ITI-13 of the IHE IT Infrastructure Technical Framework. Transaction ITI-13 is used by the Patient Context Participant, User Context Participant and Context Manager Actors.

1910 3.13.1 Scope

This transaction allows the Context Manager Actor to force other context participant actors to synchronize based on the new context values.

This transaction is composed of multiple methods as defined by the *HL7 Context Management "CCOW" Standard*. It has multiple phases consisting of surveying the participants, indication to them of final decision as to whether the context changed or not, and retrieval of the new context values by the context participants.

Each of the context participant actors follows a specific subject. The Patient Context Participant Actor follows the patient subject and does not expect the user subject to be set in context. The User Context Participant follows the user subject.

1920   The semantics of the methods used are defined in the documents HL7 Context Management "CCOW" Standard: Component Technology Mapping: ActiveX or HL7 Context Management "CCOW" Standard: Component Technology Mapping: Web, in conjunction with the HL7 Context Management "CCOW" Standard: Subject Data Definitions document. A Context Participant Actor can implement either technology. The Context Manager Actor shall support both technologies in order to interoperate with joining participants implementing the technology of their choice.

3.13.2 Use Case Roles
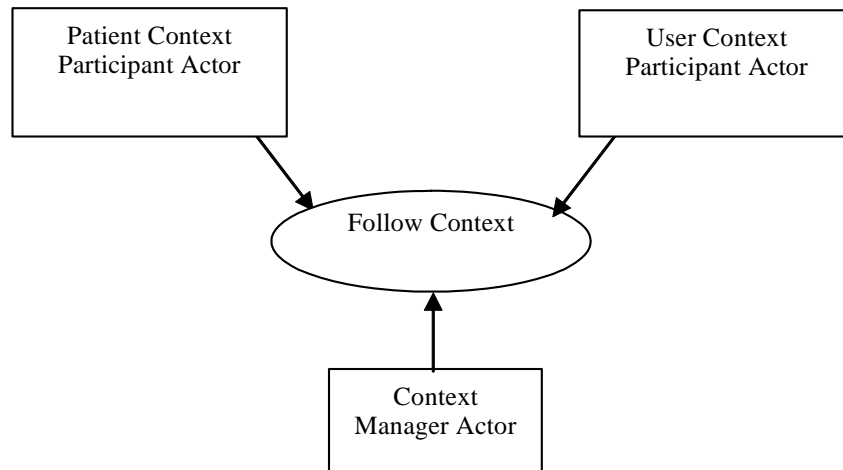
Actor: Patient Context Participant

Role: Responds to context survey. Synchronizes display to new value(s) in the patient subject of a context it follows.

Actor: User Context Participant

Role: Responds to context survey. Synchronizes display to new value(s) in the patient subject of a context it follows.

Actor: Context Manager

Role: Conducts context survey, notifies the context participants of acceptance or cancellation of a change, and provides context values.

3.13.3 Referenced Standard

HL7 Context Management "CCOW" Standard, Version 1.4

Technology and Subject Independent Architecture

Component Technology Mapping: ActiveX

Component Technology Mapping: Web

Subject Data Definitions

3.13.4 Interaction Diagram
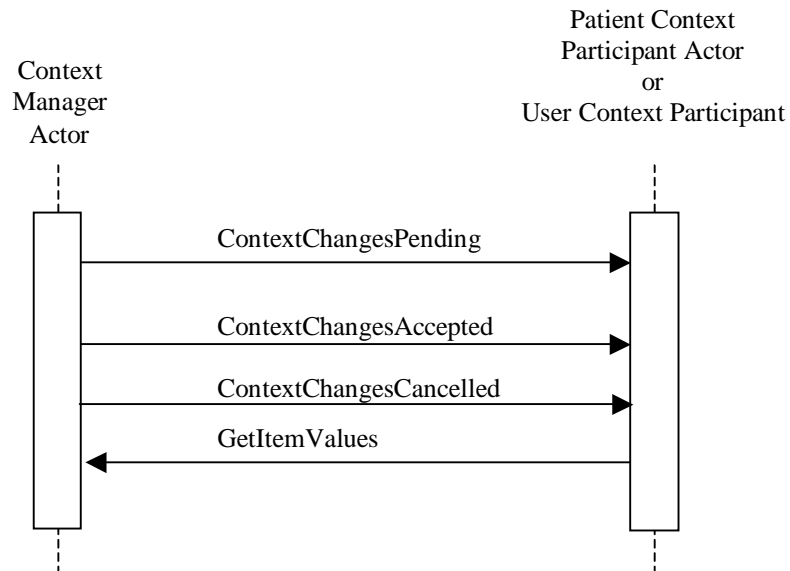
Figure 3.13-1 Follow Context – ContextChangesPending Method Sequeice

3.13.4.1 Follow Context – ContextChangesPending Method

The ContextChangesPending method is invoked by the Context Manager Actor to survey context participant actors with regard to acceptability of changes proposed by a Patient Context Participant or Client Authentication Agent Actors.

1950 **3.13.4.1.1   Trigger Events**

The ContextChangesPending method is triggered when the Context Manager receives invocation of the EndContextChanges method.

3.13.4.1.2   Message Semantics

ContextChangesPending is defined as a method on the ContextParticipant interface and allows the
1955 Context Manager to survey a context participant as to whether or not it is ready to follow the changes in the context.

In the invocation of this method, the Context Manager shall provide the pending context's coupon.

Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.7.2, for a description of the parameters associated with this
1960 method.

3.13.4.1.3   Expected Actions

Performing the ContextChangesPending method, the Patient Context Participant or User Context Participant Actor makes a decision whether or not it can accept change of context (for example due to operation being in progress). To reach this decision, it may invoke the GetItemValues method to inspect
1965 proposed new values in the context.

As a response, a Context Participant Actor will respond with an indication to Accept or Conditionally Accept the proposed change. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.7.2, for the specifics of the response formation.

1970 **3.13.4.2 Follow Context – ContextChangesAccepted Method**

The ContextChangesAccepted method is invoked by the Context Manager Actor to confirm to the context participants that instigator of change accepted proposed changes.

3.13.4.2.1   Trigger Events

The ContextChangesAccepted method is triggered when the Context Manager receives invocation of the
1975 PublishChangesDecision method indicating that the changes have been accepted.

3.13.4.2.2   Message Semantics

ContextChangesAccepted is defined as a method on the ContextParticipant interface and allows the Context Manager to inform a context participant that the context value(s) have been changed.

In the invocation of this method, the Context Manager provides the new context coupon.

1980 Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture,* Section 17.3.7.3 for a description of the parameters associated with this method.

3.13.4.2.3   Expected Actions

Performing the ContextChangesAccepted method, the Patient Context Participant or User Context Participant Actor accepts new context and can subsequently retrieve new values using the GetItemValues method.

It responds with confirmation of success or an exception. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.7.3, for the specifics of the response formation.

3.13.4.3 Follow Context – ContextChangesCancelled Method

The ContextChangesCancelled method is invoked by the Context Manager Actor to inform the context participants that instigator of change cancelled proposed changes.

3.13.4.3.1   Trigger Events

The ContextChangesCancelled method is triggered when the Context Manager receives invocation of the PublishChangesDecision method indicating that the changes have been cancelled.

3.13.4.3.2   Message Semantics

ContextChangesCancelled is defined as a method on the ContextParticipant interface and allows the Context Manager inform a context participant that the pending context change has been cancelled.

In the invocation of this method, the Context Manager provides the pending context's coupon.

Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture,* Section 17.3.7.4 for a description of the parameters associated with this method.

3.13.4.3.3   Expected Actions

Performing the ContextChangesCancelled method, the Patient Context Participant or User Context Participant Actor keeps its current context and destroys information about a pending context change that has been cancelled.

It responds with confirmation of success or an exception. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture* document, Section 17.3.7.4, for the specifics of the response formation.

3.13.4.4 Follow Context – GetItemValues Method

The GetItemValues method is invoked by a Context Participant Actor to retrieve value(s) from the context it follows.

3.13.4.4.1   Trigger Events

The GetItemValues method is triggered by a Context Participant Actor after it receives the context coupon as a result of the ContextChangesPending, ContextChangesAccepted or GetContextCoupon methods.

2015 **3.13.4.4.2   Message Semantics**

GetItemValues is defined as a method on the ContextData or SecureContextData interface. If the context is not secured when a participant actor has joined the context (i.e., Patient Context Participant that only follows patient context), then this method should be invoked on the ContextData interface. Otherwise, it shall be invoked on the SecureContextData interface.

2020   By invocation of this method without specification of the list of item names, a context participant retrieves values of all items presently set in context. It can also first invoke the GetItemNames method on the same interface (as specified in CCOW Standard) and use the list of items for selective retrieval of item values from the context via GetItemValues method. The Patient Context Participant needs to search through the resulting list of Patient.Id.IdList.<n> values until a recognized Patient Domain is found. The
2025   Patient Context Participant may choose to be grouped with a PIX Patient Identifier Cross-reference Consumer to handle the cases where no known Patient Domain is found in the resulting IdList.

Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture document*, Section 17.3.4.5, for the Patient Context Participant Actor, and Section 17.3.13.2, for the User Context Participant, for a description of parameters associated with this method.

2030 **3.13.4.4.3   Expected Actions**

Context Manager shall return the values of requested items or an exception. Refer to the *HL7 Context Management "CCOW" Standard: Technology and Subject-Independent Architecture document*, Section 17.3.4.5, for the Patient Context Participant Actor, and Section 17.3.13.2, for the User Context Participant, for a description of the response issued by the Context Manager Actor.

2035 ## 3.14 Register Document Set

This section corresponds to Transaction ITI-14 of the IHE IT Infrastructure Technical Framework. Transaction ITI-14 is used by the Document Repository Actor to register a set of documents with the Document Registry.

2040 Note: This transaction is used by the XDS.a Integration Profile. For a discussion on XDS.a and XDS.b Integration Profiles see IHE ITI TF-1 Section 10 and IHE XDS.b Supplement (www.IHE.net/Technical _Frameworks).

3.14.1 Scope

The Register Document Set transaction passes a Submission Request from a Document Repository Actor to a Document Registry Actor.

A Register Document Set transaction carries:

2045 Metadata describing zero or more documents

XDS Submission Set definition along with the linkage to new documents and references to existing documents

XDS Folder definitions along with linkage to new or existing documents

3.14.2 Use Case Roles

2050
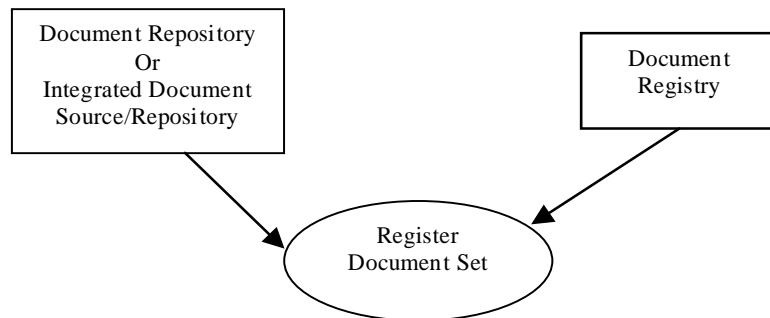
Actor: Document Repository or Integrated Document Source/Repository

Role: A document storage system that submits document metadata to a Document Registry.

Actor: Document Registry

2055 **Role:** A document indexing system that receives and stores document metadata.

Note: Within this transaction, the Document Repository and Integrated Document Source/Repository actors can be used interchangeably

3.14.3 Referenced Standards

ebRIM OASIS/ebXML Registry Information Model v2.1

2060 ebRS OASIS/ebXML Registry Services Specifications v2.1

HTTP HyperText Transfer Protocol HTTP/1.1 (IETF RFC2616)

CDA   HL7 Clinical Document Architecture (ANSI/HL7 CDA R1-2000)

HL7V2   HL7 Version 2.5

3.14.4 Interaction Diagram
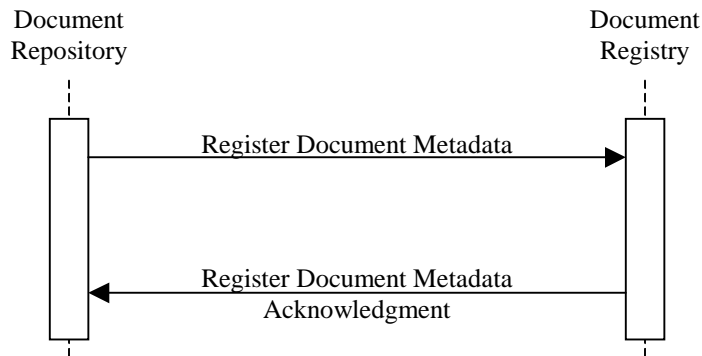
2065

3.14.4.1 Register Document Metadata

The Document Repository sends metadata for a set of documents to the Document Registry.

3.14.4.1.1   Trigger Events

The Register Document Metadata message is triggered when:

2070   1. A Document Repository wants to register metadata for a set of documents it holds.

2. A Document Repository receives a Provide and Register Document Set transaction (ITI-15)

3.14.4.1.2   Message Semantics

The sections in Chapter 4.1 specify the mapping of XDS concepts to ebRS and ebRIM semantics and document metadata.

2075   The Registry actor shall store and later include in metadata returned in a query response the XDSDocumentEntry.URI attribute along with the other metadata attributes received in the Register Document Set [ITI-14] transaction as determined by profile and transaction requirements. The Registry actor may store and later include in metadata returned in a query response the XDSDocumentEntry.repositoryUniqueId attribute if it is present in the Register Document Set [ITI-14]
2080   transaction.

3.14.4.1.2.1 Protocol Requirements

SOAP with Attachments shall be used as the protocol between the Document Repository and the Document Registry when these two actors are implemented separately. The protocol is specified in ITI
2085   TF-2 : 3.15.4.1.2.3.1 (On-line protocol binding).

3.14.4.1.2.2 Sequencing Requirements

The Repository actor shall:

1. Make a new document available for retrieval via the Retrieve Document transaction before it initiates the Register Document Metadata transaction with the Registry actor.

This is necessary because:

2. The Document Registry actor may choose to validate URIs contained in metadata before acknowledging the Register Document Metadata transaction.

3. The Document Consumer actor may retrieve the document before the Register Document Metadata Acknowledgement is received by the Repository actor.

3.14.4.1.2.3 Intentionally Left Blank

3.14.4.1.3   Expected Actions

Upon receipt of a Register Document Metadata message, the Document Registry with the aid of the Registry Adaptor shall do the following:

Accept all valid SubmitObjectsRequests.

Perform validations

Update the registry with the contained metadata

Return a RegistryResponse message given the status of the operation.

If the registry rejects the metadata, then, the following occurs:

An error is returned

The error status includes an error message

The request is rolled back

3.14.4.2 Register Document Metadata Acknowledgment

3.14.4.2.1   Trigger Events

The Document Registry finishes processing a Register Document Metadata request and shall respond with:

Register Document Metadata Acknowledgment

This message corresponds to the ebXML RequestResponse message.

3.14.4.2.2   Message Semantics

The ebXML RequestResponse message carries the status of the requested operation and an error
message if the requested operation failed. The conditions of failure and possible error messages are
given in the ebRS standard.

3.14.4.2.3   Expected Actions

The Document Repository now knows that the transaction succeeded/failed and can continue. The
metadata added to the registry as a result of this transaction is now available for discovery via query
transactions.

3.14.5 Security Considerations

3.14.5.1 XDS Affinity Domain Security Considerations

The XDS profile requires all actors be grouped with a Secure Node Actor as defined in the IHE Audit
Trail and Node Authentication Integration profile. This use of the ATNA profile in an XDS Affinity
Domain does not require a centralized XDS Affinity Domain Audit Repository Actor.

The use of ATNA along with XDS does require that each member of the XDS Affinity Domain does
have audit and security mechanisms in place. See ITI-TF-2: Appendix K.

The individual actors involved are often members of different secure domains, as illustrated in Figure
3.14.5.1-2. The data transfers between different secure domains need different protection than transfers
within a secure domain. The transactions used between different secure domains shall use the ATNA
Encryption Option.

Transfers within a single secure domain may choose to omit encryption if it is unnecessary, so it is
recommended that the online transfer security mechanisms be configurable. Certificate management
and exchange is defined as part of the XDS Affinity Domain business relationships and no IHE
Integration Profile is specified at this time, see ITI TF-1: Appendix L.

Each transaction will result in audit records describing the transaction. Each secure domain has its own
audit server to capture the records for the actors that are within that domain. Access to audit records by
other enterprises within the XDS Affinity Domain is managed and controlled by the business
relationship terms of the XDS Affinity Domain. There is no automatic IHE transaction for such access.

The audit records that shall be generated (references IHE ATNA Integration Profile) by normal XDS
activities are defined in the appropriate Security Considerations section of each transaction:

Figure 3.14.5-2 - Example Security Domain Relationships
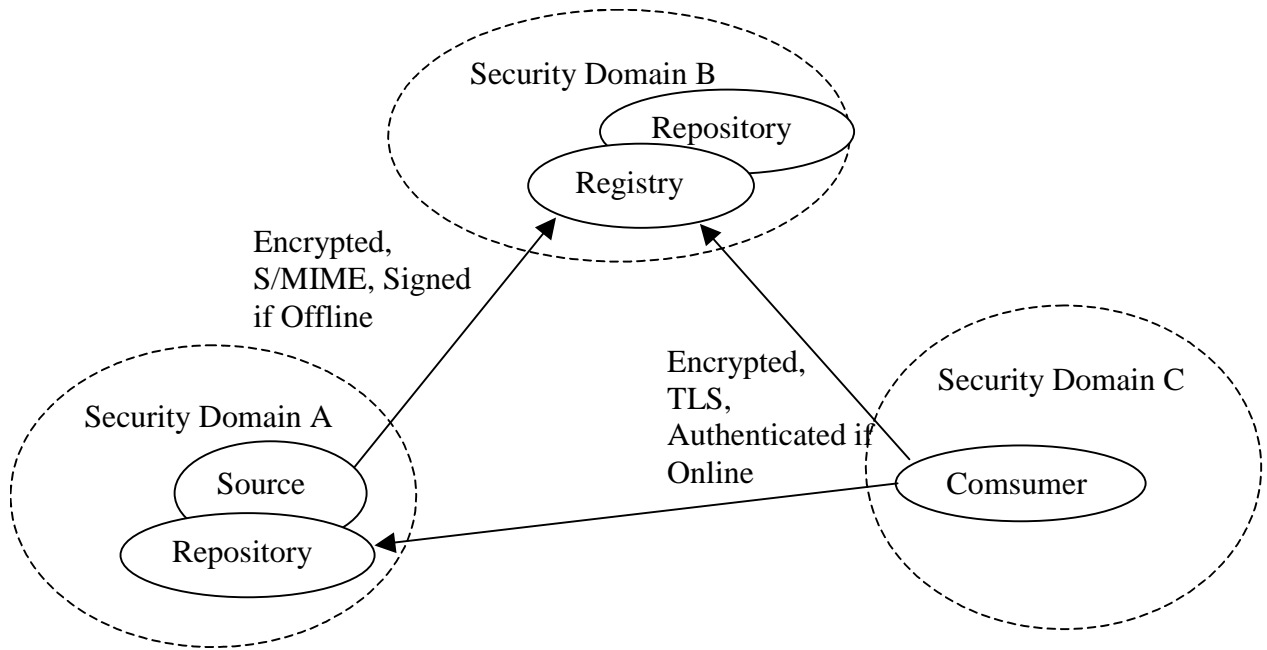
2150   All Actors are part of the same Clinical Affinity Domain

3.14.5.2 Audit Record Considerations

The Register Document Set Transaction is PHI-Export event, as defined in table 3.20.6-1. The Actors involved in the transaction shall create audit data in conformance with DICOM (Supp 95) "Data Export", with the following exceptions.

2155

3.14.5.2.1 Document Repository or Integrated Document Source/Repository audit message:

	Field Name	Opt	Value Constraints
Event **AuditMessage/ EventIdentification**	EventID	M	EV(110106, DCM, "Export")
	EventActionCode	M	"R" (Read)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-14", "IHE Transactions", "Register Document Set")
Source (Document Repository or Integrated Document Source/Repository) (1)			
Human Requestor (0..n)			
Destination (Document Registry) (1)			
Audit Source (Document Repository or Integrated Document Source/Repository) (1)			
Patient (1)			
SubmissionSet (1)			

Where:

	Field Name	Opt	Value Constraints
Source **AuditMessage/ ActiveParticipant**	UserID	U	not specialized
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human Requestor (if known) **AuditMessage/ ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

	Field Name	Opt	Value Constraints
Destination **AuditMessage/ ActiveParticipant**	UserID	M	SOAP endpoint URI.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

2160

	Field Name	Opt	Value Constraints
Audit Source **AuditMessage/ AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

	Field Name	Opt	Value Constraints
Patient (AudittMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	the patient ID in HL7 CX format..
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
Submission Set (AudittMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCode	M	"2" (System)
	ParticipantObjectTypeCodeRole	M	"20" (job)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd", "IHE XDS Metadata", "submission set classificationNode")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The submissionSet unique ID
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

3.14.5.2.2   Document Registry audit message:

	Field Name	Opt	Value Constraints
Event AuditMessage/ EventIdentification	EventID	M	EV(110107, DCM, "Import")
	EventActionCode	M	"C" (Create)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-14", "IHE Transactions", "Register Document Set")
Source (Document Repository or Integrated Document Source/Repository) (1)			
Destination (Document Registry) (1)			
Audit Source (Document Registry) (1)			
Patient (1)			
SubmissionSet (1)			

Where:

	Field Name	Opt	Value Constraints
Source AuditMessage/ ActiveParticipant	UserID	*U*	*not specialized*
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

2165

	UserID	M	SOAP endpoint URI

	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	U	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source	*AuditSourceID*	U	*Not specialized.*
AuditMessage/ AuditSourceIdentification	*AuditEnterpriseSiteID*	U	*not specialized*
	AuditSourceTypeCode	U	*not specialized*

Patient	ParticipantObjectTypeCode	M	"1" (person)
(AudittMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	U	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	U	*not specialized*
	ParticipantObjectID	M	the patient ID in HL7 CX format..
	ParticipantObjectName	U	*not specialized*
	ParticipantObjectQuery	U	*not specialized*
	ParticipantObjectDetail	U	*not specialized*
Submission Set	ParticipantObjectTypeCode	M	"2" (System)
(AudittMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCodeRole	M	"20" (job)
	ParticipantObjectDataLifeCycle	U	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd", "IHE XDS Metadata", "submission set classificationNode")
	ParticipantObjectSensitivity	U	*not specialized*
	ParticipantObjectID	M	The submissionSet unique ID
	ParticipantObjectName	U	*not specialized*
	ParticipantObjectQuery	U	*not specialized*
	ParticipantObjectDetail	U	*not specialized*

2170

3.15 Provide and Register Document Set

This section corresponds to Transaction ITI-15 of the IHE Technical Framework. Provide and Register Document Set is used by the Document Source to provide a set of documents to the Document Repository, and to request that the repository store these documents and then register them with the
2175   Document Registry.

> Note: This transaction is used by the XDS.a Integration Profile. For a discussion on XDS.a and XDS.b Integration Profiles see IHE
> ITI TF-1 Section 10 and IHE XDS.b Supplement (www.IHE.net/Technical _Frameworks).

The Provide and Register Document Set transaction describes only the interaction between the Document Source and Document Repository actors. The interaction between the Document Repository
2180   and the Document Registry is described separately in the Register Document Set Transaction (ITI-14).

This transaction aligns with the Registry Services standard (ebRS). The ebRS standard covers the interaction with a service that includes a registry with integrated repository. From the point of view of the Document Source, the separate nature of the XDS Document Registry and Repository actors is hidden. This transaction exactly matches the registry service for submitting registry/repository content
2185   found in ebRS.

By specifying separate registry and repository actors, XDS offers additional flexibility of having a single registry index content for multiple repositories. The ebRIM portion of the registry standard supports this possibility though the ExternalLink object type.

The documents and metadata go to the repository actor and then the metadata is forwarded on to the
2190   registry actor. They move in this direction for several reasons:

- Allows best reuse of ebXML Registry specified protocols
- Document Source only needs to know the identity of the Document Repository. Repository knows the identity of the registry. If Provide and Register Document Set transaction were sent to the registry then routing decisions for documents would be more complex.
2195 - Resulting protocols are simpler
- Simplifies the common case where the Document Source and the Document Repository are grouped.

3.15.1 Scope

The Provide Register Document Set transaction passes a Repository Submission Request (see ITI TF-2: 4.1.3.2) from a Document Source to a Document Registry.

2200   A Provider and Register Document Set transaction carries:

Metadata describing zero or more new documents

Submission Set definition along with the linkage to new documents and references to existing documents

Zero or more XDS Folder definitions along with linkage to new or existing documents

2205   Zero or more documents

3.15.2 Use Case Roles
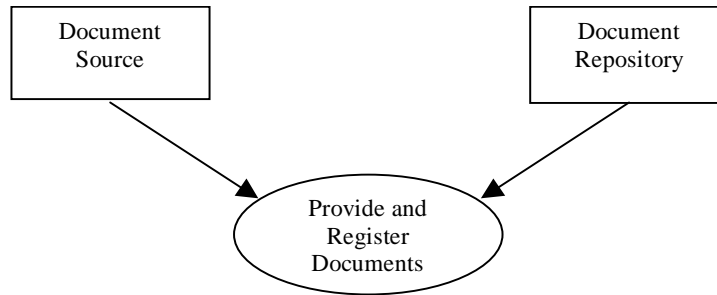
Actor: Document Source

Role: A system that submits documents and associated metadata to a Document Repository. Detail
2210 requirements for this actor are discussed in section 3.15.5.1.

Actor: Document Repository

Role: A document storage system that receives documents and associated metadata and:

Stores the documents

Enhances submitted metadata with repository information to enable later retrieval of documents

2215 Forwards the enhanced metadata to the Document Registry.

3.15.3 Referenced Standards

ebMS   OASIS/ebXML Messaging Services Specifications v2.1

ebRIM OASIS/ebXML Registry Information Model v2.1

ebRS   OASIS/ebXML Registry Services Specifications v2.1

2220 HTTP   HyperText Transfer Protocol HTTP/1.1 (IETF RFC2616)

MIME Multipurpose Internet Message Extensions (RFC 2045 to RFC 2049)

SMTP Simple Mail Transfer Protocol (RFC2821)

multipart/related The MIME Multipart/Related Content-type (RFC2387)

3.15.4 Interaction Diagram
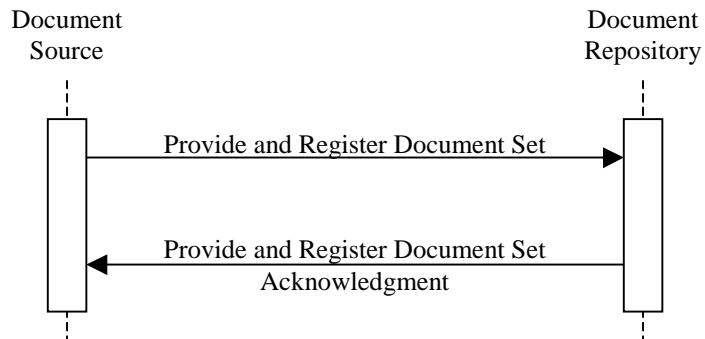
2225

3.15.4.1 Provide and Register Document Set Message

A Document Source sends documents and associated metadata to a Document Repository that has an associated Document Registry. This message corresponds to an ebRS SubmitObjectsRequest with associated documents.

2230   The Document Repository shall, upon receipt of a Provide and Register Document Set [ITI-15] transaction send a corresponding Register Document Set [ITI-14] transaction to the Document Registry actor.

- The Document Repository actor shall create and insert the XDSDocumentEntry.URI, XDSDocumentEntry.size, and XDSDocumentEntry.hash attributes for each document received
2235   from the Provide and Register Document Set [ITI-15] transaction into the Register Document Set [ITI-14] transaction metadata. If any of these attributes are present in the Provide and Register Document Set [ITI-15] transaction they shall be replaced. The XDSDocumentEntry.URI attribute value shall later be accepted in a Retrieve Document transaction [ITI-17] for that document and the document shall be returned.

2240 **3.15.4.1.1   Trigger Events**

The Document Source, based on a human decision or the application of a certain rule of automatic operation, wants to submit

- A set of one or more documents to the Document Repository and

- The associated metadata to the Document Registry.

2245 **3.15.4.1.2   Message Semantics**

Message semantics are discussed as follows:

1. Metadata

2. Security Requirements

3. Protocol Selection (On-Line Protocol binding and Off-Line Protocol binding)

2250 **3.15.4.1.2.1   Metadata**

The Register Document Set message shall include the metadata attributes (as defined in section 4.1.7 through 4.1.9) that will be forwarded by the Document Repository to the Document Registry using the Register Document Set Transaction [ITI-14].

The Document Source supplies all necessary registry object attributes with the exception of the URI
2255   attribute of an XDSDocumentEntry that must be assigned by the Document Repository. Therefore, the Document Repository must add this attribute to the metadata before initiating the Register Document Set transaction to the registry.

3.15.4.1.2.2   Intentionally Left Blank

3.15.4.1.2.3   Protocol Selection

2260   There are two types of network relationships between the Document Source and Document Repository:

On-line – the Document Source constructs a direct connection (i.e, socket) to the Document Repository.

Off-line – the Document Source connects to the Document Repository via SMTP.

3.15.4.1.2.3.1   On-Line Protocol Binding

3.15.4.1.2.3.1.1   General structure and header

2265   This is a MIME multipart/related message. The first attachment inside the payload of the SOAP request bears the registry metadata in an XML file containing the SubmitObjectsRequest.
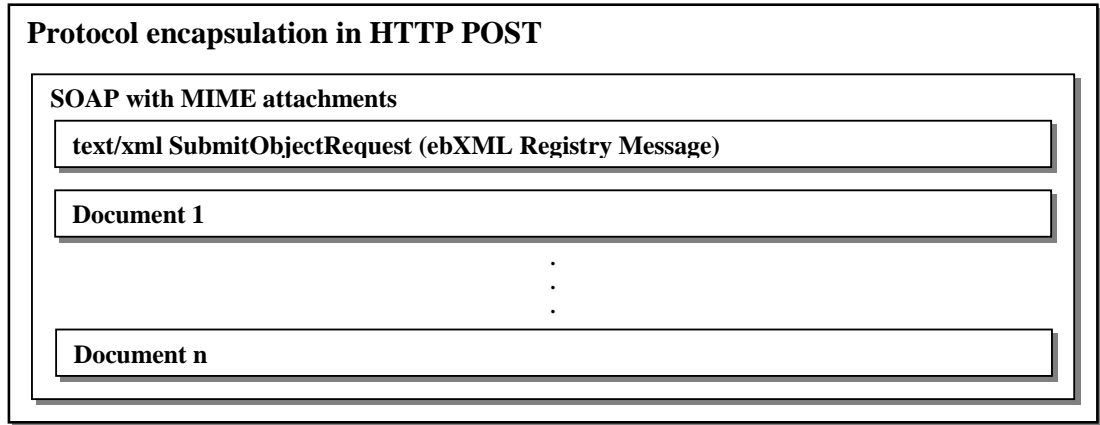
Figure 3.15.4.1-1 General Diagram of the Main message composing the On-Line Provide and Register Document Set Transaction

2270   ### 3.15.4.1.2.3.1.2   Associated Documents

The next attachments will contain the document(s) to be provided and registered, as MIME parts. There are one or more parts that contain byte streams representing documents1.

The multipart packaging transmits the MIME-type of each part. The metadata part shall be of type text/xml. Parts containing documents destined for the Document Repository can have any MIME type,
2275   either single part or multipart. Each part containing a document has associated with it a document ID that is unique within the scope of this message. The Registry Metadata contained within one part of this message uses these document IDs to bind pieces of metadata to documents.

The registry metadata will be valid according to ebRIM and will contain the definition of one or more ebXML ExtrinsicObjects. An ExtrinsicObject is a registry object that represents a repository document
2280   within the registry. Each ExtrinsicObject will contain an **id** attribute. The format of this **id** follows the ebXML Registry definition. It is either a valid UUID or a symbolic name. The value of this **id** attribute is used to link an ExtrinsicObject (XDSDocumentEntry) to a single part of the multipart that contains the attachments to the message. The header of the relevant part of the multipart will have a Content-Id header whose value is this **id** attribute surrounded by angle brackets as in the following example.
2285   The metadata includes:
```
<ExtrinsicObject id="myDocument" ...
```

---

1   This section is written independent of which protocol binding is used to package this multipart message. The protocol choice is documented elsewhere in this profile.

---

which links to the following MIME multipart part:

```
--------Boundary
Content-Type: text/xml
Content-Id: <myDocument>

This sentence is the value of the document.
--------Boundary
```

3.15.4.1.2.3.2   Off-Line Protocol Binding

3.15.4.1.2.3.2.1   General structure and header

As shown on Figure 3.15.4.1-2, the Off-Line transaction will be based on the ebXML Message Service Binding, as defined in the ebXML Registry Service (ebRS), with an Asynchronous Message and responses as defined in ebXML Messaging Services (ebMS). The re-use of ebXML enables implementers to integrate the Provide and Register Document Set transaction into a server which supports more comprehensive services, including some using Collaboration-Protocol Profiles (CPP) and Collaboration-Protocol Agreement (CPA) as supported by ebXML. Because IHE is aiming to specify such as plug-and-play mechanisms, the Off-Line Protocol Binding is entirely defined into the present document. This specification does not mandate the use of a CPA between the Document Repository acting as "ebRS Registry" and the Document Source acting as "ebRS Registry Client". Such protocol agreement aspects are beyond the scope of the XDS Profile. The Document Source has only to know the Document Repository e-mail address to be able to provide and register a document set.

```
┌─────────────────────────────────────────────────────────────────────────┐
│ Protocol encapsulation in SMTP/ESMTP                                      │
│ ┌───────────────────────────────────────────────────────────────────┐   │
│ │ SOAP with MIME attachments                                         │   │
│ │ ┌───────────────────────────────────────────────────────────────┐ │   │
│ │ │ text/xml SOAP:Envelope                                         │ │   │
│ │ │   ┌─────────────────────────────────────────────────────────┐ │ │   │
│ │ │   │ SOAP:Header, with Service=LifeCycleManager and          │ │ │   │
│ │ │   │ Action=submitObjects                                    │ │ │   │
│ │ │   └─────────────────────────────────────────────────────────┘ │ │   │
│ │ │   ┌─────────────────────────────────────────────────────────┐ │ │   │
│ │ │   │ SOAP:Body, with Manifest=list of attachments            │ │ │   │
│ │ │   │ (e.g. ebXML Reg. Msg + Documents)                       │ │ │   │
│ │ │   └─────────────────────────────────────────────────────────┘ │ │   │
│ │ └───────────────────────────────────────────────────────────────┘ │   │
│ │ ┌───────────────────────────────────────────────────────────────┐ │   │
│ │ │ text/xml SubmitObjectRequest (ebXML Registry Message)          │ │   │
│ │ └───────────────────────────────────────────────────────────────┘ │   │
│ │ ┌───────────────────────────────────────────────────────────────┐ │   │
│ │ │ Document 1                                                     │ │   │
│ │ └───────────────────────────────────────────────────────────────┘ │   │
│ │                              .                                      │   │
│ │                              .                                      │   │
│ │                              .                                      │   │
│ │ ┌───────────────────────────────────────────────────────────────┐ │   │
│ │ │ Document n                                                     │ │   │
│ │ └───────────────────────────────────────────────────────────────┘ │   │
│ └───────────────────────────────────────────────────────────────────┘   │
└─────────────────────────────────────────────────────────────────────────┘
```
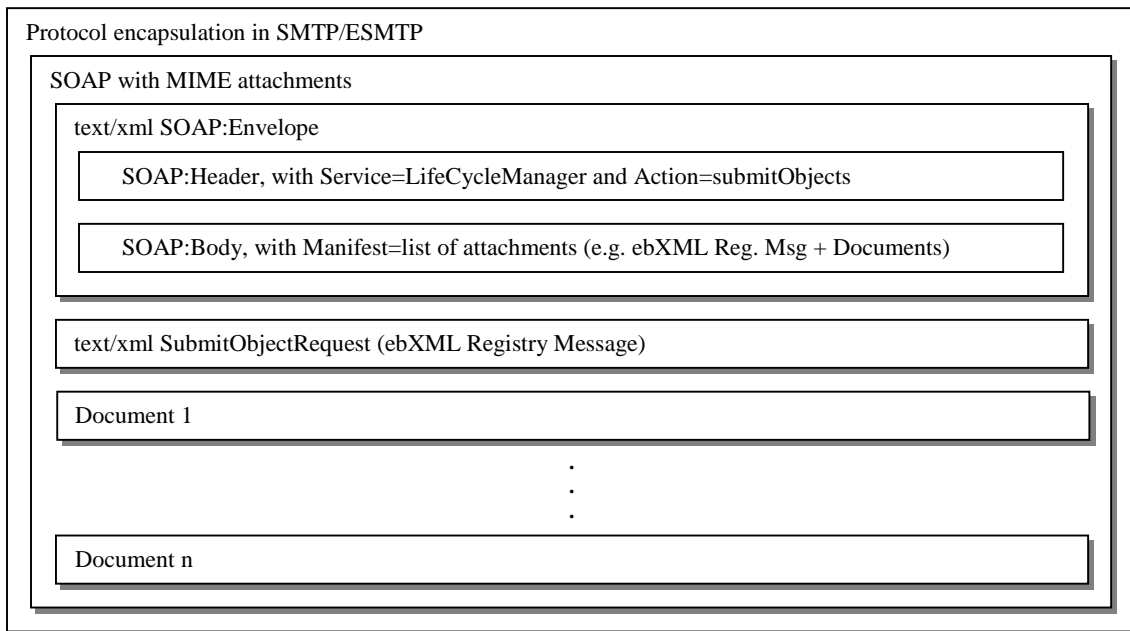
Figure 3.15.4.1-2 General Diagram of the Main message composing the Off-Line Provide and Register Document Set Transaction

The message is an e-mail message (which the ebXML Messaging Services can split into several messages if a single message would be too big) containing the following fields:

• The **From:** e-mail address of the sender (Document Source).

- Optionally, a **Reply-to:** address if the Document Source wants the response messages to be sent to another e-mail address.

2315
- The **To:** e-mail address of the recipient (Document Repository). In case the Document Repository is able to register a document set to more than one Document Registry, it will have a different e-mail address for each one of the Repository-Registry peer.

- **Date:** is the date and time of the Provide and Register Document Set Transaction.

- **Subject: XDS/1.0/PnR/** (followed optionally by indication of XDS "subprofile" name. It SHALL
2320   NOT contain any Patient related information)

- **MIME-Version: 1.0**.

- **SOAPAction: "ebXML"**.

   This is a MIME multipart/related message. The first attachment is the text/xml SOAP:Envelope part containing the ebMS header. The character set
2325   of the ebMS header is UTF-8.

The Header is described in the ebMS standard. It contains the following ebRS tag values:

- The header of the message, in /SOAP:Envelope/ SOAP:Header/eb:MessageHeader/ as shown in the table below.

Table 3.15.4.1-1 ebXML Message Header

Location ("@" for attributes)	Description
eb:From/eb:PartyId	Identification of the message sender (its email address, preceded by mailto:)
eb:From/eb:Role	String indicating the authorized role of the sender formatted as a URI per ebXML messaging specification: http://www.ihe.net/roles/iti/xds/DocumentSource
eb:To/eb:PartyId	Identification of intended recipient of the message (its email address, preceded by mailto:)
eb:To/eb:Role	String indicating the authorized role of the sender formatted as a URI per ebXML messaging specification: http://www.ihe.net/roles/iti/xds/DocumentRepository
eb:CPAId	Identification of a Collaboration Protocol Agreement between the sender and receiver. This shall contain the trading partner agreed CPA text reference, if it exists (e.g., the URI of the XML file describing the partnership agreement). If there is no CPA, this element shall be the concatenation of eb:From/eb:PartyId and the eb:To/eb:PartyId, separated by the hyphen character (-).
eb:ConversationId	In the absence of a local trading partner agreement, shall be CCYYMMDD-HHMMSS-mmmmm based upon the sending ebXML message generation. When generating responses the eb:ConversationID is taken from the original message.
eb:Service	Shall be LifeCycleManager
eb:Action	Shall be submitObjects
eb:MessageData/eb:MessageId	A unique message identifier generated by the sender: either a concatenation of message elements to create a globally unique identifier, or a single message element if that element is globally unique.
eb:MessageData/eb:Timestamp	UTC Time that the message header was created in XMLSchema dateTime format. Example: 2004-12-25T23:50:50
eb:DuplicateElimination	If present, duplicate messages should be eliminated.

eb:Description	Description of the Submission Set (equivalent to the XDSSubmissionSet.comments attribute).
eb:AckRequested	Optional in ebMS, required here to indicate that the repository shall acknowledge the message. This element has the following attributes: SOAP:mustUnderstand="1" eb:version="2.1" eb:signed="false"

2330
- List of references to document, in /SOAP:Envelope/ SOAP:Body/eb:Manifest/eb:Reference as shown in the table below.

Table 3.15.4.1-2 ebXML Message References

Location ("@" for attributes)	Description
@eb:id	Identification of the document, which is the OID of the XDSDocument. However, the first reference shall be to the SubmitObjectsRequest XML file, with id set to SubmitObjectsRequest.
@xlink:href	The relative URI of the document in the payload of the ebMS message, cid: followed by the OID. Used only for a newly submitted XDS Document.
@xlink:role	Shall be present only for the first reference, and be set to **http://www.ihe.net/roles/iti/xds/SubmitObjectsRequest**
eb:Schema	Shall be present only for the first reference, and has following attributes: eb:location=http://www.ihe.net/schemas/iti/xds/SubmitObjectsRequest eb:version=1.0
eb:Description	To be set to the XDSDocumentEntry.title. However, for the first reference, shall be set to the meaning of SubmitObjectsRequest in the local language (i.e. lang="en-US", "Provide and Register Document Set Metadata").

The following attachment inside the payload of the SOAP request bears the registry metadata in an
2335 XML file containing the SubmitObjectsRequest.

3.15.4.1.2.3.2.2 Associated Documents

See the subsection "Associated Documents" in the On-Line Binding section (ITI TF-2: 3.15.4.1.2.3.1.1). Any document that has a reference xlink:href and contains a URI that is a content id (URI scheme "cid") shall be included in the payload.

2340 **3.15.4.1.3 Expected Actions**

The Document Repository will receive this message. Each document within the message will be stored into the repository as an octet stream with an associated MIME type. A detected failure will result in an error result message being returned to the Document Source thus terminating this transaction.

2345 The Document Repository will modify the received registry metadata adding:
- A URI identifier (xdsDocumentEntry.URI) must be created that can be used by a Document Consumer to reference the document.
- A hash value (xdsDocumentEntry.hash)
- A size (xdsDocumentEntry.size).

2350

If hash and/or size slots are present in the submission, the repository shall verify the value(s) with the actual value(s) of the submitted document and return an error on mismatch.

2355   A Register Document Set transaction with this modified metadata will be issued to the XDS Document Registry.

The repository will ensure that any Document Retrieve Transaction received including the URI identifying the XDS Document, this document shall be provided to the Document Consumer unchanged from the octet stream that was submitted (full fidelity repository).

2360

3.15.4.1.3.1 Basic Patient Privacy Enforcement Option

If the Basic Patient Privacy Enforcement Option is implemented:

1. The Document Source actor shall populate the confidentialityCode in the document metadata with the list of OID values that identify the Patient Privacy Consent Policies that apply to the associated document. The confidentiality codes for different documents in the same submission may be different.

2. The Document Source actor shall be able to be configured with the Patient Privacy Consent Policies, Patient Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the XDS Affinity Domain Policy. The details of this are product specific and not specified by IHE.

3. The Document Source actor may have user interface or business rule capabilities to determine the appropriate confidentiality codes for each document. The details of this are product specific and not specified by IHE. However, the information about how confidentiality codes are assigned must be part of the published policy for the XDS Affinity Domain. For example, when publishing a document, the Document Source, might show a list of checkboxes where a user can select which of the available consents a document is to be published.

4. The Document Recipient actor shall be able to be configured with the Patient Privacy Consent Policies, Patient Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the policies. The meanings of the codes on the media must be provided out of band, e.g., by telephone, fax, or email. The detail of how this is done is product specific and not specified by IHE. If the documents are transferred internally within the organization or to other members of the recipient's affinity domain, appropriate internal confidentiality codes shall be applied.

5. The Document Recipient actor shall have the ability to coerce the confidentiality code in the metadata associated with the document from the codes used by the Document Source to the codes used by the Document Recipient.

6. The Document Recipient actor shall abide by the XDS Affinity Domain Policies represented by the confidentialityCode in the metadata associated with the document. The Document Recipient actor likely will have user access controls or business rule capabilities to determine the details of how confidentiality codes apply to query results. The details of this are product specific and not specified by IHE. These rules shall reduce the query results to only those that are appropriate to the current situation for that actor and user.

2395 ### 3.15.4.2 Provide and Register Document Set Acknowledgment

The Document Repository sends a Provide and Register Document Set Acknowledgment when the processing of a Provide and Register Document Set is complete. This message is identical to the RegistryResponse message specified in ebRS. It shall be conveyed in the same protocol as the request.

2400 **3.15.4.2.1   Trigger Events**

The following events can trigger this message:

Documents stored to repository successfully and metadata stored to registry successfully (The registry part is carried out as part of a Register Document Set transaction)

Documents stored to repository successfully but an error occurred in storing the metadata to the registry

2405   Documents were not successfully stored to the repository

3.15.4.2.2   Message Semantics

An ebRS RegistryResponse message is returned containing status and an error message if necessary.

Additional relevant semantics for both the repository and registry are described in the Register Document Set transaction.

2410 **3.15.4.2.3   Expected Actions**

The Document Source now knows that the transaction succeeded/failed and continue. The metadata added to the registry as a result of this transaction is now available for discovery via query transactions. The document(s) added to the repository are now available for retrieval.

3.15.5 Actor Requirements

2415   This section summarizes the capabilities of one or more actors relevant to this transaction. The details regarding how to perform these operations are documented elsewhere in this transaction or possibly in other transactions.

3.15.5.1 Document Source

An implementation of the Document Source Actor shall be capable of the following operations:

2420   1.   Submit one or more documents. Whether a submission contains a single or multiple documents depends on workflows, policies, and other external factors which are outside of the scope of this profile.

An implementation of the Document Source Actor may support one or more of the following XDS Options.

2425   1.   **Document Replacement Option:** In this option the Document Source offers the ability to submit a document as a replacement for another document already in the registry/repository.

        2.   **Document Addendum Option:** In this option the Document Source shall offer the ability to submit a document as an addendum to another document already in the registry/repository.

        3.   **Document Transformation Option:** In this option the Document Source shall offer the ability
2430   to 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)

4. **Folder Management Option:** In this option the Document Source offers the ability to perform
2435 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).

2440 •

These operations are discussed in section 4.1.3.4 Other Properties of Submission Requests.

3.15.5.2 Document Repository

A Document Repository shall be capable of accepting submissions containing multiple documents.

Note: The Document Source may submit single documents or multiple documents depending on its needs.

2445 A Document Repository may validate the following metadata elements received as part of a Provide and Register transaction:

XDSDocumentEntry.uniqueId – a submission may be rejected if not unique within the repository.

XDSSubmissionSet.sourceId – a repository may choose to accept submissions only from certain sources and use this field to perform the filtering.

2450

3.15.6 Security Considerations

Relevant XDS Affinity Domain Security background is discussed in the Register Document transaction (see ITI TF-2: 3.14.5.1).

3.15.6.1 Audit Record Considerations

2455 The Provide and Register Document Set Transaction is PHI-Export event, as defined in table 3.20.6-1. The Actors involved in the transaction shall create audit data in conformance with DICOM (Supp 95) "Data Export"/"Data Import", with the following exceptions.

3.15.6.1.1 Document Source audit message:

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110106, DCM, "Export")
	EventActionCode	M	"R" (Read)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-15", "IHE Transactions", "Provide and Register Document Set")
Source (Document Source) (1)			
Human Requestor (0..n)			
Destination (Document Repository) (1)			
Audit Source (Document Source) (1)			
Patient (1)			
SubmissionSet (1)			

Where:

Source	UserID	U	not specialized
AuditMessage/ ActiveParticipant	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human Requestor (if known)	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
AuditMessage/ ActiveParticipant	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

2460

Destination	UserID	M	SOAP endpoint URI.
AuditMessage/ ActiveParticipant	*AlternativeUserID*	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source	*AuditSourceID*	*U*	*Not specialized.*
AuditMessage/ AuditSourceIdentification	*AuditEnterpriseSiteID*	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Patient	ParticipantObjectTypeCode	M	"1" (Person)
(AudittMessage/ ParticipantObjectIdentifi cation)	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
	ParticipantObjectTypeCode	M	"2" (System)
	ParticipantObjectTypeCodeRole	M	"20" (job)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd", "IHE XDS Metadata", "submission set classificationNode")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The submissionSet unique ID

	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

2465 **3.15.6.1.2 Document Repository audit message:**

	Field Name	Opt	Value Constraints
Event **AuditMessage/ EventIdentification**	EventID	M	EV(110107, DCM, "Import")
	EventActionCode	M	"C" (Create)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-15", "IHE Transactions", "Provide & Register Document Set")
Source (Document Source) (1)			
Destination (Document Repository) (1)			
Audit Source (Document Repository) (1)			
Patient (1)			
SubmissionSet (1)			
Where:			
Source **AuditMessage/ ActiveParticipant**	UserID	*U*	*not specialized*
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Destination **AuditMessage/ ActiveParticipant**	UserID	M	SOAP endpoint URI
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source **AuditMessage/ AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

	ParticipantObjectTypeCode	M	"1" (Person)
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*

	ParticipantObjectDetail	*U*	*not specialized*
Submission Set **(AuditMessage/ ParticipantObjectIdentifi cation)**	ParticipantObjectTypeCode	M	"2" (System)
	ParticipantObjectTypeCodeRole	M	"20" (job)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd", "IHE XDS Metadata", "submission set classificationNode")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The submissionSet unique ID
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

2470

3.16 Query Registry

This section corresponds to Transaction ITI-16 of the IHE Technical Framework. Transaction ITI-16 is used by the Document Consumer to query the Document Registry for information about documents indexed in the registry.

2475

      Note: This is a very general query mechanism that allows very broad use. Future extensions to XDS may introduce restrictions or specified the use of canned queries. Proposals for restricting the search mechanism are requested.

3.16.1 Scope

The Query Registry Transaction supports a variety of types of queries. Examples include the following:

Query by patient (Id) for a time interval, by document type(s), by practice setting(s), by author person

2480   Query by Document Source

Query for XDS Folders updated during a time interval

Query for all documents in a Folder or Submission Set

Query by time of submission

The list of XDS registry entries attributes that can be the target of a query are defined in Section 4.1.7

2485   through 4.1.9. This transaction will document the basic syntax and semantics of XDS Document Registry queries.

All queries return:

- Metadata for one or more registry objects, or
- Object references for one or more registry objects (registry UUIDs).

2490   **3.16.2 Use Case Roles**
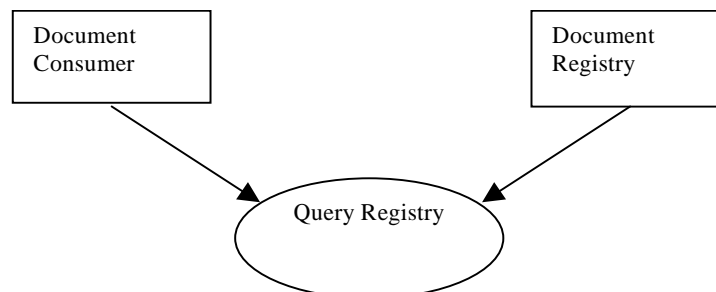
Actor: Document Consumer

2495   **Role:** Generates Query Registry messages and sends them to the Document Registry.

Actor: Document Registry

Role: Receives Query Registry messages and executes a query against registry metadata to select and return matching data to the Document Consumer.

3.16.3 Referenced Standard

2500   ebRS   OASIS/ebXML Registry Services Specifications v2.1

        SQL   ISO/IEC 9075 Database Language SQL

3.16.4 Interaction Diagram
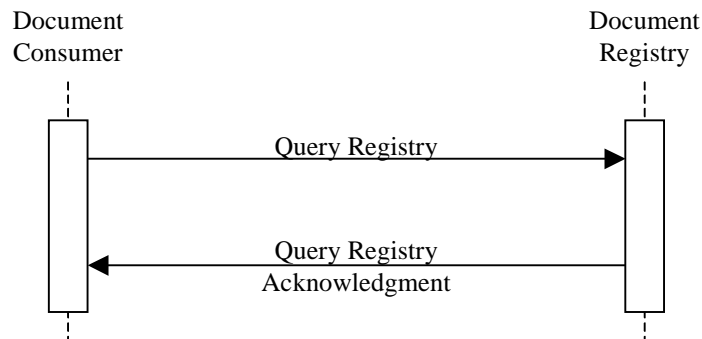
3.16.4.1 Query Registry

2505   This is the query request to the registry from a Document Consumer.

3.16.4.1.1   Trigger Events

This message is initiated when the Document consumer wants to retrieve document metadata.

3.16.4.1.2   Message Semantics

XDS specifies the use of SQL as a query language to the registry. There are 2 significant parameters to
2510   an AdHocQueryRequest (HTTP-SOAP):

- returnType
- SQL query text

3.16.4.1.2.1   Parameter returnType

XDS supports the following values for the parameter returnType:

2515   •   ObjectRef – a list of object UUIDs (references)

        •   LeafClass – list of XML elements representing the leaf class of the object returned

The 'LeafClass' returnType is meant for returning a small amount of fully specified ebXML objects
(such as a list of ExtrinsicObject (XDSDocumentEntry) elements with full contents: slots, external
2520   identifiers, classifications etc.). This type of query result is self-contained, everything known about the
object(s) is returned. The specific query documented in this section describes which object types will be
included. ObjectRef elements are also returned. These represent objects not included in the returned
object list that are referenced by objects in the returned object list. These ObjectRefs are required by the
registry standard.

2525   The 'ObjectRef' returnType returns references to the registry objects that match the query. This type query is recommended when the returned object list could be large. An initial query returning ObjectRefs for all objects of interest followed by secondary queries requesting full metadata (query type LeafClass) is an efficient way to query for large bodies of metadata. This strategy is particularly easy to use when querying for a single object type (XDSDocumentEntry or XDSSubmissionSet are examples) 2530   since only a single object type is involved.

An ObjectRef looks like:

```
<ObjectRef id="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"/>
```

3.16.4.1.2.2 SQL query text

2535   SQL queries submitted to an XDS Document Registry shall conform to the ebRS Registry Services specification, which maps elements of the information model (ebRIM) into a collection of SQL views.

The next sections show the details of several useful queries. This is not an exhaustive list. Any valid SQL query written against the registry information model (ebRIM+XDS specialization) may be used. The specific SQL subset used by registry is specified in Appendix D of ebRS.

2540   **3.16.4.1.2.2.1   SQL Select Statement**

All SELECT statements shall explicitly code the SELECT variable. So,

     SELECT eo.id FROM ExtrinsicObject eo …

Is valid, and

     SELECT * FROM ExtrinsicObject eo …

2545   is not.

Note: This requirement is stated in ebRS verson 2.1 in section 8.3.2 Semantic Constraints on Query Syntax.

3.16.4.1.2.3 Security Requirements

2550   Relevant security requirements are discussed in the Register Document transaction (see ITI TF-2: 3.14.4.1.2.3) and in Security Considerations Sections 3.16.4.1.5 and 3.16.4.2.4.

3.16.4.1.3 Expected Actions

The registry returns a Query Registry Acknowledgment message.

3.16.4.1.4 Minimum Query Catalog

2555   The queries documented in this section form a minimal set of queries needed by Document Consumers to discover documents in XDS.

It is the responsibility of the Document Consumer to package the SQL from any of these Minimum Queries listed below into a Query transaction.

2560

All implementations of the Registry actor shall support all queries, including parts labeled optional, that are documented in this section. Document Consumer actors shall be able to depend on these queries to be supported by XDS Registry actors. XDS Registry actors may reject queries not in this query catalog. For example, XDS Registry actors may reject queries using the SQL keyword 'LIKE' except where noted in the following queries.

2565

Queries whose names start with 'Find' are broad, keyword-based searches focused on a single patient ID. Queries whose names start with 'Get' are simpler retrieval-style searches.

Query Parameters

2570

Each query is represented as a function with parameters. The parameters are numbered and the *Parm* column in each query definition table indicates which parameter a particular row of the table supports. Additionally, each query parameter is supported by one or more detail parameters. For example, the query parameter *fromDateTime* is supported by detail parameters *$timeSlot, $lowerTime,* and *$uppertime* where *$timeSlot* indicates the name of the slot (there are 3) that is being tested and *$lowerTime* and *$upperTime* give the time range of interest. If a query parameter like *fromDateTime* is used then all of its detail parameters must be filled in. If this query parameter is not used, then all rows

2575

with a *Parm* showing that query's number are to be removed from the query.

All DateTime values are formatted as YYYYMMDDHHMMSS (each degree of accuracy is optional, see definition of the DTM XDS Data Type in Table 3.14.2.1-3). All time comparisons are:

LowerDateTime <= DateTime < UpperDateTime

Some parameters are labeled as being in 'value list' format. A value list has the format:

2580

('value1', 'value2')

The single quotes around the list items are required. The list format, parentheses and comma separation are required.

All values (constants) are set into single quotes, for example a dateTime value of '200412252359'.

When using the LIKE clause, the wildcard character is '%'.

2585

Single values are coded as

123 - without quotes for numbers

'Approved' - in single quotes for strings.

'Children''s Hospital' – a single quote is inserted in a string by specifying two single quotes

Within the LIKE predicate

2590

Underscore ('_') matches an arbitrary character

Percent ('%') matches an arbitrary string

Format for multiple values is

(value, value, value, …) OR

(value) if only one value is to be sepecified.

2595   where each value is coded as described above for single values. Parameters labeled as accepting multiple values shall be coded using this format.

In the query parameter tables below, each row represents a query parameter. Optional parameters which are not included in the query invocation have no affect on the query. Queries return registry objects that match all the supplied parameters. When multiple values are included for a parameter, objects are
2600   returned that match any included value (within the context of the larger query).

In the following tables, coding schemes are represented by a pair of parameters, one representing the code value and the second representing the coding scheme name from which the code value is taken. For example, in the FindDocuments query, are found parameters

        $XDSDocumentEntryClassCode – classCode values of interest

2605 $XDSDocumentEntryClassCodeScheme – coding scheme for each class code value

While the 'codes' can be specified without the 'code schemes', if any code schemes are specified (if the code schemes parameter is specified) then the code schemes for all codes listed shall be present and in the same order as the codes.

The 'Opt' column of each query parameter table below specifies whether the parameter is required ('R')
2610   or optional ('O'). Document Registry actor implementations shall reject queries missing required parameters and shall accept but not require all optional parameters.. The 'Mult' column labels each query parameter as accepting multiple values ('M') or not accepting multiple values ('—').

The 'status' attribute (XDSDocumentEntryStatus, XDSSubmissionSetStatus, XDSFolderStatus) shall take on values in the set ('Approved', 'Deprecated'). Formatting of the Patient ID field requires special
2615   attention. The Registry actor shall perform string matching on the Patient ID field per SQL specifications and will provide no pre-processing of Patient ID values. That is, Document Registry actors do not process the Patient ID, remove unwanted components, and then process the query. Document Consumer actors are required to specify the proper format for Patient ID values (IDNumber^^^&OIDofAA&ISO) and shall include no further values in the Patient ID. Should the
2620   Document Consumer add extra values (e.g., a value in component 5 of the HL7 view of the data), the response of the Registry actor is undefined.

3.16.4.1.4.1 FindDocuments

Find documents (XDSDocumentEntry objects) in the registry for a given patientID with a matching 'status' attribute. The other parameters can be used to restrict the set of XDSDocumentEntry objects
2625   returned.

Returns: XDSDocumentEntry objects matching the query parameters

Parameter Name	Attribute	Opt	Mult
$XDSDocumentEntryPatientId	XDSDocumentEntry. patientId	R	--
$XDSDocumentEntryClassCode	XDSDocumentEntry. classCode	O	M
$XDSDocumentEntryClassCodeScheme	XDSDocumentEntry. classCode[1]	O[2]	M[2]
$XDSDocumentEntryPracticeSettingCode	XDSDocumentEntry. practiceSettingCode	O	M
$XDSDocumentEntryPracticeSettingCodeScheme	XDSDocumentEntry. practiceSettingCode[1]	O[2]	M[2]
$XDSDocumentEntryCreationTimeFrom	Lower value of XDSDocumentEntry. creationTime	O	--
$XDSDocumentEntryCreationTimeTo	Upper value of XDSDocumentEntry.	O	--

Parameter Name	Attribute	Opt	Mult
	creationTime		
$XDSDocumentEntryServiceStartTimeFrom	Lower value of XDSDocumentEntry. serviceStartTime	O	--
$XDSDocumentEntryServiceStartTimeTo	Upper value of XDSDocumentEntry. serviceStartTime	O	--
$XDSDocumentEntryServiceStopTimeFrom	Lower value of XDSDocumentEntry. serviceStopTime	O	--
$XDSDocumentEntryServiceStopTimeTo	Upper value of XDSDocumentEntry. serviceStopTime	O	--
$XDSDocumentEntryHealthcareFacilityTypeCode	XDSDocumentEntry. healthcareFacilityTypeCode	O	M
$XDSDocumentEntryHealthcareFacilityTypeCodeScheme	XDSDocumentEntry. healthcareFacilityTypeCode[1]	O[2]	M[2]
$XDSDocumentEntryEventCodeList	XDSDocumentEntry. eventCodeList	O	M
$XDSDocumentEntryEventCodeListScheme	XDSDocumentEntry. eventCodeList[1]	O[2]	M[2]
$XDSDocumentEntryConfidentialityCode	XDSDocumentEntry. confidentialityCode	O	M
$XDSDocumentEntryFormatCode	XDSDocumentEntry. formatCode	O	M
$XDSDocumentEntryStatus	XDSDocumentEntry. status	R	M

[1]This attribute is not listed by name in table 4.1-5 Document Metadata Attribute Definition. It is included in the documentation of the attribute that bears the same name without the 'Scheme' suffix. As an example, XDSDocumentEntry.ClassCodeScheme is not an attribute listed in attribute table for 2630 XDSDocumenEntry. It is documented as part of XDSDocumentEntry.classCode, specifically as the 'codingScheme' Slot.

[2]This parameter is optional but if included shall 1) have the same number of values as the corresponding 'code' attribute, 2) the ith value of the 'code' attribute (e.g. XDSDocumentEntryClassCode) shall correspond to the ith value of the 'codeScheme' attribute (e.g. XDSDocumentEntryClassCodeScheme).

2635 **Example SQL**

```
SELECT doc.id
FROM ExtrinsicObject doc, ExternalIdentifier patId
, Classification clCode      # $XDSDocumentEntryClassCode
, Classification psc         # $XDSDocumentEntryPracticeSettingCode
, Classification hftc        # $XDSDocumentEntryhealthcareFacilityTypeCode
, Classification ecl         # $XDSDocumentEntryEventCodeList
, Slot clCodeScheme          # $XDSDocumentEntryClassCodeScheme
, Slot psCodeScheme          # $XDSDocumentEntryPracticeSettingCodeScheme
, Slot crTimef               # $XDSDocumentEntryCreationTimeFrom
, Slot crTimet               # $XDSDocumentEntryCreationTimeTo
, Slot serStartTimef         # $XDSDocumentEntryServiceStartTimeFrom
, Slot serStartTimet         # $XDSDocumentEntryServiceStartTimeTo
, Slot serStopTimef          # $XDSDocumentEntryServiceStopTimeFrom
, Slot serStopTimet          # $XDSDocumentEntryServiceStopTimeTo
, Slot hftcScheme            # $XDSDocumentEntryHealthcareFacilityTypeCodeScheme
, Slot eclScheme             # $XDSDocumentEntryEventCodeListScheme
, Classification conf        # $XDSDocumentEntryConfidentialityCode
, Classfication fmtCode      # $XDSDocumentEntryFormatCode
 WHERE
  doc.objectType = 'urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1'
# patientID
  AND (doc.id = patId.registryobject AND
      patId.identificationScheme='urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427' AND
      patId.value = $XDSDocumentEntryPatientId )
# classCode
  AND (clCode.classifiedobject = doc.id AND                                           # $XDSDocumentEntryClassCode
      clCode.classificationScheme = 'urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a' AND # $XDSDocumentEntryClassCode
      clCode.nodeRepresentation IN $XDSDocumentEntryClassCode )                        # $XDSDocumentEntryClassCode
# classCode Scheme
#   This coding depends on the above clause being included.
  AND (clCodeScheme.parent = clCode.id AND                                            # $XDSDocumentEntryClassCodeScheme
```

```
                 clCodeScheme.name = 'codingScheme' AND                                        # $XDSDocumentEntryClassCodeScheme
                 clCodeScheme.value IN $XDSDocumentEntryClassCodeScheme)                       # $XDSDocumentEntryClassCodeScheme
2670    # practice setting code
         AND (psc.classifiedObject = doc.id AND                                                # $XDSDocumentEntryPracticeSettingCode
                 psc.classificationScheme='urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead' AND  # $XDSDocumentEntryPracticeSettingCode
                 psc.nodeRepresentation IN $XDSDocumentEntryPracticeSettingCode )              # $XDSDocumentEntryPracticeSettingCode
        # practiceSetting Scheme
2675    #   This coding depends on the above clause being included.
         AND (psCodeScheme.parent = psc.id AND                                                 # $XDSDocumentEntryPracticeSettingCodeScheme
                 psCodeScheme.name = 'codingScheme' AND                                        # $XDSDocumentEntryPracticeSettingCodeScheme
                 psCodeScheme.value IN $XDSDocumentEntryPracticeSettingCodeScheme)             # $XDSDocumentEntryPracticeSettingCodeScheme
        # creationTime from
2680     AND (crTimef.parent = doc.id AND                                                      # $XDSDocumentEntryCreationTimeFrom
                 crTimef.name = 'creationTime' AND                                             # $XDSDocumentEntryCreationTimeFrom
                 $XDSDocumentEntryCreationTimeFrom &lt;= crTimef.value )                       # $XDSDocumentEntryCreationTimeFrom
          # creationTime to
         AND (crTimet.parent = doc.id AND                                                      # $XDSDocumentEntryCreationTimeTo
2685             crTimet.name = 'creationTime' AND                                             # $XDSDocumentEntryCreationTimeTo
                 crTimet.value &lt; $XDSDocumentEntryCreationTimeTo)                           # $XDSDocumentEntryCreationTimeTo
        # serviceStartTime from
         AND (serStartTimef.parent = doc.id AND                                                # $XDSDocumentEntryServiceStartTimeFrom
                 serStartTimef.name = 'serviceStartTime' AND                                   # $XDSDocumentEntryServiceStartTimeFrom
2690             $XDSDocumentEntryServiceStartTimeFrom &lt;= serStartTimef.value )             # $XDSDocumentEntryServiceStartTimeFrom
        # serviceStartTime to
         AND (serStartTimet.parent = doc.id AND                                                # $XDSDocumentEntryServiceStartTimeTo
                 serStartTimet.name = 'serviceStartTime' AND                                   # $XDSDocumentEntryServiceStartTimeTo
                 serStartTimet.value &lt; $XDSDocumentEntryServiceStartTimeTo)                 # $XDSDocumentEntryServiceStartTimeTo
2695    # serviceStopTime from
         AND (serStopTimef.parent = doc.id AND                                                 # $XDSDocumentEntryServiceStopTimeFrom
                 serStopTimef.name = 'serviceStopTime' AND                                     # $XDSDocumentEntryServiceStopTimeFrom
                 $XDSDocumentEntryServiceStopTimeFrom &lt;= serStopTimef.value )               # $XDSDocumentEntryServiceStopTimeFrom
        # serviceStopTime to
2700     AND (serStopTimet.parent = doc.id AND                                                 # $XDSDocumentEntryServiceStopTimeTo
                 serStopTimet.name = 'serviceStopTime' AND                                     # $XDSDocumentEntryServiceStopTimeTo
                 serStopTimet.value &lt; $XDSDocumentEntryServiceStopTimeTo)                   # $XDSDocumentEntryServiceStopTimeTo
        # healthcare facility type code
         AND (hftc.classifiedObject = doc.id AND                                               # $XDSDocumentEntryhealthcareFacilityTypeCode
2705             hftc.classificationScheme='urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1' AND # $XDSDocumentEntryhealthcareFacilityTypeCode
                 hftc.nodeRepresentation IN $XDSDocumentEntryhealthcareFacilityTypeCode )      # $XDSDocumentEntryhealthcareFacilityTypeCode
        # healthcareFacilityTypeCode Scheme
        #   This coding depends on the above clause being included.
         AND (hftcScheme.parent = hftc.id AND                                                  # $XDSDocumentEntryHealthcareFacilityTypeCodeScheme
2710             hftcScheme.name = 'codingScheme' AND                                          # $XDSDocumentEntryHealthcareFacilityTypeCodeScheme
                 hftcScheme.value IN $XDSDocumentEntryHealthcareFacilityTypeCodeScheme)        # $XDSDocumentEntryHealthcareFacilityTypeCodeScheme
        # event code list
         AND (ecl.classifiedObject = doc.id AND                                                # $XDSDocumentEntryEventCodeList
2715             ecl.classificationScheme = 'urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4' AND # $XDSDocumentEntryEventCodeList
                 ecl.nodeRepresentation IN $XDSDocumentEntryEventCodeList )                    # $XDSDocumentEntryEventCodeList
        # eventCodeList Scheme
        #   This coding depends on the above clause being included.
         AND (eclScheme.parent = ecl.id AND                                                    # $XDSDocumentEntryEventCodeListScheme
2720             eclScheme.name = 'codingScheme' AND                                           # $XDSDocumentEntryEventCodeListScheme
                 eclScheme.value IN $XDSDocumentEntryEventCodeListScheme)                      # $XDSDocumentEntryEventCodeListScheme
        # confidentialityCode
         AND (conf.classifiedObject = doc.id AND                                               # $XDSDocumentEntryConfidentialityCode
                 conf.classificationScheme = 'urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f' AND # $XDSDocumentEntryConfidentialityCode
2725             conf.nodeRepresentation IN $XDSDocumentEntryConfidentialityCode )             # $XDSDocumentEntryConfidentialityCode
        # format code
         AND (fmtCode.classifiedObject = doc.id AND                                            # $XDSDocumentEntryFormatCode
                 fmtCode.classificationScheme = 'urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d' AND # $XDSDocumentEntryFormatCode
                 fmtCode.nodeRepresentation IN $XDSDocumentEntryFormatCode)                    # $XDSDocumentEntryFormatCode
         # status
2730     AND doc.status IN $XDSDocumentEntryStatus
```

3.16.4.1.4.2 FindSubmissionSets

Find submission sets (XDSSubmissionSet objects) in the registry for a given patientID with matching 'status' attribute. The other parameters can be used to restrict the collection of XDSSubmissionSet objects returned.

Returns: XDSSubmissionSet objects matching the query parameters

Parameter Name	Attribute	Opt	Mult
$XDSSubmissionSetPatientId	XDSSubmissionSet. patientId	R	--
$XDSSubmissionSetSourceId	XDSSubmissionSet. sourceId	O	M
$XDSSubmissionSetSubmissionTimeFrom	XDSSubmissionSet. submissionTime Lower value	O	--
$XDSSubmissionSetSubmissionTimeTo	XDSSubmissionSet. submissionTime Upper value	O	--
$XDSSubmissionSetAuthorPerson[1]	XDSSubmissionSet. authorPerson	O	--

Parameter Name	Attribute	Opt	Mult
$XDSSubmissionSetContentType	XDSSubmissionSet. contentTypeCode	O	M
$XDSSubmissionSetStatus	XDSSubmissionSet. status	R	M

[1]The value for this parameter is a pattern compatible with the SQL keyword LIKE.

Example SQL

2740

```
SELECT ss.id
FROM RegistryPackage ss, ExternalIdentifier patId
 , Slot subTimeFrom       # $XDSSubmissionSetSubmissionTimeFrom
 , Slot subTimeTo         # $XDSSubmissionSetSubmissionTimeTo
 , Slot ap                # $XDSSubmissionSetAuthorPerson
 , ExternalIdentifier sid # $XDSSubmissionSetSourceId
 , Classification ctc     # $XDSSubmissionSetContentType
WHERE
# patient ID
      ( ss.id = patId.registryobject AND
      patId.identificationScheme= 'urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446' AND
      patId.value = $XDSSubmissionSetPatientId )
# source ID
  AND ( sid.registryobject = ss.id AND                                      # $XDSSubmissionSetSourceId
      sid.identificationScheme = 'urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832' AND    # $XDSSubmissionSetSourceId
      sid.value IN $XDSSubmissionSetSourceId )                              # $XDSSubmissionSetSourceId
# submission set time from
  AND ( subTimeFrom.parent = ss.id AND                                      # $XDSSubmissionSetSubmissionTimeFrom
      subTimeFrom.name = 'submissionTime' AND                              # $XDSSubmissionSetSubmissionTimeFrom
      subTimeFrom.value >= $XDSSubmissionSetSubmissionTimeFrom )           # $XDSSubmissionSetSubmissionTimeFrom
# submission set time to
  AND ( subTimeTo.parent = ss.id AND                                       # $XDSSubmissionSetSubmissionTimeTo
      subTimeTo.name = 'submissionTime' AND                               # $XDSSubmissionSetSubmissionTimeTo
      subTimeTo.value &lt; $XDSSubmissionSetSubmissionTimeTo )            # $XDSSubmissionSetSubmissionTimeTo
# author person
  AND ( ap.parent = ss.id AND                                              # $XDSSubmissionSetAuthorPerson
      ap.name = 'authorPerson' AND                                        # $XDSSubmissionSetAuthorPerson
      ap.value LIKE $XDSSubmissionSetAuthorPerson )                       # $XDSSubmissionSetAuthorPerson
# content type codes
  AND ( ctc.classifiedObject = ss.id AND                                   # $XDSSubmissionSetContentType
      ctc.classificationScheme = 'urn:uuid:aa543740-bdda-424e-8c96-df4873be8500' AND   # $XDSSubmissionSetContentType
      ctc.nodeRepresentation IN $XDSSubmissionSetContentType  )           # $XDSSubmissionSetContentType
# status
  AND ss.status = 'Approved'
```

3.16.4.1.4.3 FindFolders

2775   Find folders (XDSFolder objects) in the registry for a given patientID with matching 'status' attribute. The other parameters can be used to restrict the collection of XDSFolder objects returned.

Returns: XDSFolder objects matching the query parameters

Parameter Name	Attribute	Opt	Mult
$XDSFolderPatientId	XDSFolder.patientId	R	--
$XDSFolderLastUpdateTimeFrom	XDSFolder. lastUpdateTime lower value	O	--
$XDSFolderLastUpdateTimeTo	XDSFolder. lastUpdateTime upper bound	O	--
$XDSFolderCodeList	XDSFolder. codeList	O	M
$XDSFolderCodeListScheme	XDSFolder. codeList1	O2	M2
$XDSFolderStatus	XDSFolder.status	R	M

[1]This attribute is not listed by name in table 3.14.4.1-5 Document Metadata Attribute Definition. It is

2780   included in the documentation of the attribute that bears the same name without the 'Scheme' suffix. As an example, XDSDocumentEntry.ClassCodeScheme is not an attribute listed in attribute table for XDSDocumenEntry. It is documented as part of XDSDocumentEntry.classCode, specifically as the 'codingScheme' Slot.

2785

[2]This parameter is optional but if included shall 1) have the same number of values as the corresponding 'code' attribute, 2) the ith value of the 'code' attribute (e.g. XDSDocumentEntryClassCode) shall correspond to the ith value of the 'codeScheme' attribute (e.g. XDSDocumentEntryClassCodeScheme).

Example SQL

```
SELECT fol.id
FROM RegistryPackage fol, ExternalIdentifier patId
, Slot lupdateTimef      # $XDSFolderLastUpdateTimeFrom
, Slot lupdateTimet      # $XDSFolderLastUpdateTimeTo
, Classification cl      # $XDSFolderCodeList
, Slot clScheme          # $XDSFolderCodeListScheme
    WHERE
# patientID
    ( patId.registryobject = fol.id  AND
    patId.identificationScheme = 'urn:uuid:f64ffdf0-4b97-4e06-b79f-a52b38ec2f8a' AND
    patId.value = $XDSFolderPatientId )
# last update time from
 AND ( lupdateTimef.parent = fol.id AND                                        # $XDSFolderLastUpdateTimeFrom
    lupdateTimef.name = 'lastUpdateTime' AND                                   # $XDSFolderLastUpdateTimeFrom
    lupdateTimef.value >= $XDSFolderLastUpdateTimeFrom )                       # $XDSFolderLastUpdateTimeFrom
# last update time to
 AND ( lupdateTimet.parent = fol.id AND                                        # $XDSFolderLastUpdateTimeTo
    lupdateTimet.name = 'lastUpdateTime' AND                                   # $XDSFolderLastUpdateTimeTo
    lupdateTimet.value &lt; $XDSFolderLastUpdateTimeTo )                       # $XDSFolderLastUpdateTimeTo
# code list
 AND ( cl.classifiedObject = fol.id AND                                        # $XDSFolderCodeList
    cl.classificationScheme = 'urn:uuid:1ba97051-7806-41a8-a48b-8fce7af683c5' AND  # $XDSFolderCodeList
    cl.nodeRepresentation IN $XDSFolderCodeList )                             # $XDSFolderCodeList
# code list Scheme
#   This coding depends on the above clause being included.
  AND (clScheme.parent = cl.id AND                                            # $XDSFolderCodeListScheme
    clScheme.name = 'codingScheme' AND                                        # $XDSFolderCodeListScheme
    clScheme.value IN $XDSFolderCodeListScheme )                              # $XDSFolderCodeListScheme
# status
AND fol.status = 'Approved'
```

3.16.4.1.4.4 GetAll

2820

Get all registry content for a patient given the indicated status, format codes, and confidentiality codes.

Returns:

- XDSSubmissionSet, XDSDocumentEntry, and XDSFolder objects with patientId attribute matching $patientId parameter

- Association objects with sourceObject or targetObject attribute matching one of the above

2825

objects

Parameter Name	Attribute	Opt	Mult
$patientId	XDSFolder. patientId, XDSSubmissionSet. patientId, XDSDocumentEntry. patientId	R	--
$XDSDocumentEntryStatus	XDSDocumentEntry. status	R	M
$XDSSubmissionSetStatus	XDSSubmissionSet. status	R	M
$XDSFolderStatus	XDSFolder. status	R	M
$XDSDocumentEntryFormatCode	XDSDocumentEntry. formatCode	O	M
$XDSDocumentEntryConfidentialityCode	XDSDocumentEntry. confidentialityCode	O	M

Because of the limits placed on the usage of the SQL query language by ebXML Registry version 2.1, this query cannot be reasonably implemented as a single query. The following piece-wise queries return

XDSDocumentEntry objects

XDSSubmissionSet and XDSFolder objects

2830

Association objects

Example SQL Part 1

```
SELECT eo.id
FROM ExtrinsicObject eo, ExternalIdentifier patId
 , Classification cCode         # $XDSDocumentEntryConfidentialityCode
 , Classfication fmtCode        # $XDSDocumentEntryFormatCode
WHERE
  eo.status IN $XDSDocumentEntryStatus AND
  eo.objectType = 'urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1' AND
  patId.registryObject = eo.id AND
  patId.identificationScheme = 'urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427' AND
  patId.value = $patientId
 AND ( cCode.classifiedObject = eo.id AND                                       #
$XDSDocumentEntryConfidentialityCode
      cCode.classificationScheme = 'urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f' AND   #
$XDSDocumentEntryConfidentialityCode
      cCode.nodeRepresentation IN $XDSDocumentEntryConfidentialityCode  )             #
$XDSDocumentEntryConfidentialityCode
# format code
  AND (fmtCode.classifiedObject = doc.id AND                                    #
$XDSDocumentEntryFormatCode
      fmtCode.classificationScheme = 'urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d' AND  #
$XDSDocumentEntryFormatCode
      fmtCode.nodeRepresentation IN $XDSDocumentEntryFormatCode)                 #
$XDSDocumentEntryFormatCode
```

2835

2840

2845

2850

2855

Example SQL Part 2

```
SELECT rp.id FROM RegistryPackage rp, Classification cl, ExternalIdentifier patId
WHERE
 (
  rp.status IN $XDSSubmissionSetStatus AND
  cl.classifiedObject = rp.id AND
  cl.classificationNode = 'urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd' AND
  patId.registryObject = rp.id AND
  patId.identificationScheme = 'urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446' AND
  patId.value = $patientId
 )
OR
 (
  rp.status IN $XDSFolderStatus AND
  cl.classifiedObject = rp.id AND
  cl.classificationNode = 'urn:uuid:d9d542f3-6cc4-48b6-8870-ea235fbc94c2' AND
  patId.registryObject = rp.id AND
  patId.identificationScheme = 'urn:uuid:f64ffdf0-4b97-4e06-b79f-a52b38ec2f8a' AND
  patId.value = $patientId
 )
```

2860

2865

2870

2875

Example SQL Part 3

```
SELECT DISTINCT ass.id FROM Association ass, ExtrinsicObject eo, RegistryPackage ss, RegistryPackage fol
WHERE
 (
        (ass.sourceObject = ss.id AND ass.targetObject = fol.id) OR
        (ass.sourceObject = ss.id AND ass.targetObject = eo.id) OR
        (ass.sourceObject = fol.id AND ass.targetObject = eo.id)

 ) AND
  eo.id IN
        (SELECT eo.id FROM ExtrinsicObject eo, ExternalIdentifier patId
                WHERE
                  eo.status IN $XDSDocumentEntryStatus AND
                 patId.registryObject = eo.id AND
                 patId.identificationScheme = 'urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427' AND
                 patId.value = $patientId) AND

   ss.id IN
```

2880

2885

2890

2895

```
       (SELECT ss.id FROM RegistryPackage ss, ExternalIdentifier patId
         WHERE
           ss.status IN $XDSSubmissionSetStatus AND
           patId.registryObject = ss.id AND
           patId.identificationScheme = 'urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446' AND
           patId.value = $patientId
       ) AND
   fol.id IN
       (SELECT fol.id FROM RegistryPackage fol, ExternalIdentifier patId
         WHERE
           fol.status IN $XDSFolderStatus AND
           patId.registryObject = fol.id AND
           patId.identificationScheme = 'urn:uuid:f64ffdf0-4b97-4e06-b79f-a52b38ec2f8a' AND
           patId.value = $patientId
       )
```

3.16.4.1.4.5 GetDocument

Retrieve a collection of XDSDocumentEntry objects. XDSDocumentEntry objects are selected either by their entryUUID or uniqueId attribute.

Returns: XDSDocumentEntry objects requested

Parameter Name	Attribute	Opt	Mult
$XDSDocumentEntryEntryUUID	XDSDocumentEntry. entryUUID	O[1]	M
$XDSDocumentEntryUniqueId	XDSDocumentEntry. uniqueId	O[1]	M

1 - Either $XDSDocumentEntryEntryUUID or $XDSDocumentEntryUniqueId shall be specified. This transaction shall return an error if both parameters are specified.

Example SQL

```
# UUID param
SELECT doc.id                                                              #
$XDSDocumentEntryEntryUUID
FROM ExtrinsicObject doc                                                   #
$XDSDocumentEntryEntryUUID
WHERE  doc.id IN $XDSDocumentEntryEntryUUID                                #
$XDSDocumentEntryEntryUUID
# uniquid param
   SELECT doc.id FROM ExtrinsicObject doc, ExternalIdentifier uniqId       #
$XDSDocumentEntryUniqueId
     WHERE                                                                 #
$XDSDocumentEntryUniqueId
       uniqId.registryobject = doc.id AND                                  #
$XDSDocumentEntryUniqueId
       uniqId.identificationScheme = 'urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab' AND   #
$XDSDocumentEntryUniqueId
       uniqId.value IN $XDSDocumentEntryUniqueId                           #
$XDSDocumentEntryUniqueId
```

3.16.4.1.4.6 GetSubmissionSetContentsAndContents

Retrieve an XDSSubmissionSet object along with its contents. XDSSubmissionSet objects are selected either by their entryUUID or uniqueId attribute. The XDSDocumentEntry objects returned shall match one of the confidentiality

2945 codes listed if that parameter is included.

Returns:

- XDSSubmissionSet object specified in the query
- Association objects with type HasMember whose sourceObject attribute references the above XDSSubmissionSet object

2950 - XDSDocumentEntry and XDSFolder objects referenced by the targetObject attribute of one of the above Associations

Parameter Name	Attribute	Opt	Mult
$XDSSubmissionSetEntryUUID	XDSSubmissionSet. entryUUID	O[1]	--
$XDSSubmissionSetUniqueId	XDSSubmissionSet. uniqueId	O[1]	--
$XDSDocumentEntryFormatCode	XDSDocumentEntry. formatCode	O	M
$XDSDocumentEntryConfidentialityCode	XDSDocumentEntry. confidentialityCode	O	M

1 - Either $XDSSubmissionSetEntryUUID or $XDSSubmissionSetUniqueId shall be specified. This transaction shall return an error if both parameters are specified.

2955 This query is specified as 4 component queries: submission set, documents in the submission set, folders, and associations. The following special instructions apply:

- The variable $ssuuid in parts 2 and 3 and 4 must be replaced with the UUID of the registry package returned in part 1.
- The variable $docuuids in part 4 must be replaced with the UUIDs, in list format, of the
2960 documents returned in part 2
- The variable $foluuids in part 4 must be replaced with the UUIDs, in list format, of the folders returned in part 3

Example SQL Part 1

2965
```
# get submission set by uuid
SELECT ss.id FROM RegistryPackage ss                               #
$XDSSubmissionSetEntryUUID
WHERE                                                               #
$XDSSubmissionSetEntryUUID
2970      ss.id = $XDSSubmissionSetEntryUUID                        #
$XDSSubmissionSetEntryUUID
# get submission set by uniqueId
SELECT ss.id FROM RegistryPackage ss, ExternalIdentifier uniq      #
$XDSSubmissionSetUniqueId
2975 WHERE                                                          #
$XDSSubmissionSetUniqueId
  uniq.registryObject = ss.id AND                                  #
$XDSSubmissionSetUniqueId
  uniq.identificationScheme = 'urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8' AND  #
2980 $XDSSubmissionSetUniqueId
  uniq.value = $XDSSubmissionSetUniqueId                           #
$XDSSubmissionSetUniqueId
```

Example SQL Part 2

2985

```
# get docs based on submission set uuid
SELECT doc.id FROM ExtrinsicObject doc, Association a
, Classification conf        # $XDSDocumentEntryConfidentialityCode
, Classfication fmtCode       # $XDSDocumentEntryFormatCode
WHERE
  a.sourceObject = $ssuuid AND
  a.associationType = 'HasMember' AND
  a.targetObject = doc.id
 AND (
  conf.classificationScheme = 'urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f' AND       #
$XDSDocumentEntryConfidentialityCode
  conf.classifiedObject = doc.id AND                                                    #
$XDSDocumentEntryConfidentialityCode
  conf.nodeRepresentation IN $XDSDocumentEntryConfidentialityCode)                      #
$XDSDocumentEntryConfidentialityCode
  AND (fmtCode.classifiedObject = doc.id AND                                            #
$XDSDocumentEntryFormatCode
      fmtCode.classificationScheme = 'urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d' AND #
$XDSDocumentEntryFormatCode
      fmtCode.nodeRepresentation IN $XDSDocumentEntryFormatCode)                        #
$XDSDocumentEntryFormatCode
```

2990

2995

3000

3005

Example SQL Part 3

3010

```
SELECT fol.id FROM RegistryPackage fol, Association a
WHERE
  a.associationType = 'HasMember' AND
  a.sourceObject = $ssuuid AND
  a.targetObject = fol.id
```

3015

Example SQL Part 4

3020

```
SELECT ass.id FROM Association ass
WHERE
  ass.associationType = 'HasMember' AND
  ass.sourceObject = $ssuuid AND
  (
    ass.targetObject IN $docuuids OR
    ass.targetObject IN $foluuids
  )
```

3025

3.16.4.1.4.7 GetFolderAndContents

Retrieve an XDSFolder object and its contents. XDSFolder objects are selected either by their entryUUID or uniqueId attribute. The XDSDocumentEntry objects returned shall match one of the
3030 confidentiality codes listed if that parameter is included.

Returns:

* XDSFolder object specified in the query

- Association objects of type HasMember that have a sourceObject attribute referencing the XDSFolder object specified in the query

3035 XDSDocumentEntry objects referenced by the targetObject attribute of one of the Association objects specified above

Parameter Name	Attribute	Opt	Mult
$XDSFolderEntryUUID	XDSFolder. entryUUID	O[1]	--
$XDSFolderUniqueId	XDSFolder. uniqueId	O[1]	--
$XDSDocumentEntryFormatCode	XDSDocumentEntry. formatCode	O	M
$XDSDocumentEntryConfidentialityCode	XDSDocumentEntry. confidentialityCode	O	M

1 - Either $XDSFolderEntryUUID or $XDSFolderUniqueId shall be specified. This transaction shall return an error if both parameters are specified.

3040 This query is specified as 3 component queries: folder, documents in the folder, and associations linking the folder and documents. The following special instructions apply:

- The variable $foluuid in parts 2 and 3 must be replaced with the UUID of the registry package returned in part 1.
- The variable $docuuids in part 3 must be replaced with the UUIDs, in list format, of the
3045 documents returned in part 2

Example SQL Part 1

3050

```
# get folder by uuid
SELECT fol.id FROM RegistryPackage fol                                          #
$XDSFolderEntryUUID
WHERE                                                                           #
$XDSFolderEntryUUID
        fol.id = $XDSFolderEntryUUID                                            #
$XDSFolderEntryUUID
# get folder by uniqueId
SELECT fol.id FROM RegistryPackage fol, ExternalIdentifier uniq                 #
$XDSFolderUniqueId
WHERE                                                                           #
$XDSFolderUniqueId
  uniq.registryObject = fol.id AND                                             #
$XDSFolderUniqueId
  uniq.identificationScheme = 'urn:uuid:75df8f67-9973-4fbe-a900-df66cefecc5a' AND    #
$XDSFolderUniqueId
  uniq.value = $XDSFolderUniqueId                                              #
$XDSFolderUniqueId
```

3070 **Example SQL Part 2**

```
# get docs based on folder uuid
SELECT doc.id FROM ExtrinsicObject doc, Association a
, Classification conf        # $XDSDocumentEntryConfidentialityCode
```

```
3075    , Classfication fmtCode      # $XDSDocumentEntryFormatCode
        WHERE
          a.sourceObject = $foluuid AND
          a.associationType = 'HasMember' AND
          a.targetObject = doc.id
3080     AND (                                                                            #
        $XDSDocumentEntryConfidentialityCode
          conf.classificationScheme = 'urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f' AND      #
        $XDSDocumentEntryConfidentialityCode
          conf.classifiedObject = doc.id AND                                              #
3085    $XDSDocumentEntryConfidentialityCode
          conf.nodeRepresentation IN $XDSDocumentEntryConfidentialityCode)                #
        $XDSDocumentEntryConfidentialityCode
        # format code
          AND (fmtCode.classifiedObject = doc.id AND                                      #
3090    $XDSDocumentEntryFormatCode
               fmtCode.classificationScheme = 'urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d' AND #
        $XDSDocumentEntryFormatCode
               fmtCode.nodeRepresentation IN $XDSDocumentEntryFormatCode)                 #
        $XDSDocumentEntryFormatCode
```

3095

Example SQL Part 3

```
        SELECT ass.id FROM Association ass
        WHERE
3100      ass.associationType = 'HasMember' AND
          ass.sourceObject = $foluuid AND
          ass.targetObject IN $docuuids
```

3.16.4.1.4.8 GetFoldersForDocument

3105 Retrieve XDSFolder objects that contain the XDSDocumentEntry object provided with the query. XDSDocumentEntry objects are selected either by their entryUUID or uniqueId attribute.

Returns: XDSFolder objects that contain specified XDSDocumentEntry object. More specifically, for each Association object of type HasMember that has a targetObject attribute referencing the target XDSDocumentEntry object, return the object referenced by its sourceObject if it is of type XDSFolder.

3110

Parameter Name	Attribute	Opt	Mult
$XDSDocumentEntryEntryUUID	XDSDocumentEntry. entryUUID	O[1]	--
$XDSDocumentEntryUniqueId	XDSDocumentEntry. uniqueId	O[1]	--

1 - Either $XDSDocumentEntryEntryUUID or $XDSDocumentEntryUniqueId shall be specified. This transaction shall return an error if both parameters are specified.

Example SQL

```
3115    SELECT fol.id FROM RegistryPackage fol, Association a, ExtrinsicObject doc, Classification c
        WHERE
          doc.id IN
         (
        # UUID param
3120    SELECT doc.id                                                                     #
        $XDSDocumentEntryEntryUUID
        FROM ExtrinsicObject doc                                                          #
        $XDSDocumentEntryEntryUUID
```

```
WHERE   doc.id = $XDSDocumentEntryEntryUUID                                        #
$XDSDocumentEntryEntryUUID
# uniquid param
    SELECT doc.id FROM ExtrinsicObject doc, ExternalIdentifier uniqId             #
$XDSDocumentEntryUniqueId
    WHERE                                                                         #
$XDSDocumentEntryUniqueId
        uniqId.registryobject = doc.id AND                                       #
$XDSDocumentEntryUniqueId
        uniqId.identificationScheme = 'urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab' AND  #
$XDSDocumentEntryUniqueId
        uniqId.value = $XDSDocumentEntryUniqueId                                  #
$XDSDocumentEntryUniqueId
  ) AND
  a.targetObject = doc.id AND
  a.associationType = 'HasMember' AND
  a.sourceObject = fol.id AND
  c.classifiedObject = fol.id AND
  c.classificationNode = 'urn:uuid:d9d542f3-6cc4-48b6-8870-ea235fbc94c2'
```

3.16.4.1.4.9 GetRelatedDocuments

Retrieve XDSDocumentEntry objects that are related to the specified document via an Association object. The specified document is designated by UUID or uniqueId. The query shall return

- Association objects in which the sourceObject attribute OR the targetObject attribute references the specified document and the associationType attribute matches a value included in the $AssociationTypes parameter

- XDSDocumentEntry objects referenced by the targetObject attribute OR the sourceObject attribute of an Association object matched above

  Note: A side effect of the query is that the specified document is returned in the results.

See section 3.14.4.1.2.6 Document Relationships and Associations for background.

Returns: XDSDocumentEntry objects and related Association objects

Given : An XDSDocumentEntry object and a collection of association types.

Parameter Name	Attribute	Opt	Mult
$XDSDocumentEntryEntryUUID	XDSDocumentEntry. entryUUID	O[1]	--
$XDSDocumentEntryUniqueId	XDSDocumentEntry. uniqueId	O[1]	--
$AssociationTypes	Not a named attribute	R	M

1 - Either $XDSDocumentEntryEntryUUID or $XDSDocumentEntryUniqueId shall be specified. This transaction shall return an error if both parameters are specified.

This query is specified as 2 component queries: associations and documents linked by the associations. The following special instructions apply:

- The variable $assuuids in part 2 must be replaced with the UUIDs, in list format, of the association objects returned in part 1.

Example SQL Part 1

3165

```
SELECT a.id FROM Association a, ExtrinsicObject doc
WHERE
  doc.id IN
  (
# UUID param
SELECT doc.id                                                              #
$XDSDocumentEntryEntryUUID
FROM ExtrinsicObject doc                                                   #
$XDSDocumentEntryEntryUUID
WHERE  doc.id = $XDSDocumentEntryEntryUUID                                 #
$XDSDocumentEntryEntryUUID
# uniquid param
    SELECT doc.id FROM ExtrinsicObject doc, ExternalIdentifier uniqId      #
$XDSDocumentEntryUniqueId
    WHERE                                                                  #
$XDSDocumentEntryUniqueId
        uniqId.registryobject = doc.id AND                                #
$XDSDocumentEntryUniqueId
        uniqId.identificationScheme = 'urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab' AND   #
$XDSDocumentEntryUniqueId
        uniqId.value = $XDSDocumentEntryUniqueId                          #
$XDSDocumentEntryUniqueId
  ) AND
  a.associationType IN $AssociationTypes AND
  (
  a.sourceObject = doc.id OR
  a.targetObject = doc.id
  )
```

3170

3175

3180

3185

3190

Example SQL Part 2

3195

3200

```
SELECT doc.id FROM ExtrinsicObject doc, Association a
WHERE
  a.id IN $assuuids AND
  (
  doc.id = a.sourceObject OR
  doc.id = a.targetObject
  )
```

3.16.4.1.4.10 GetFolders

3205 Retrieve a collection of XDSFolder objects. XDSFolder objects are selected either by their entryUUID or uniqueId attribute.

Returns: XDSFolder objects requested.

Parameter Name	Attribute	Opt	Mult
$XDSFolderEntryUUID	XDSFolder. entryUUID	O[1]	M
$XDSFolderUniqueId	XDSFolder. uniqueId	O[1]	M

1 - Either $XDSFolderEntryUUID or $XDSFolderUniqueId shall be specified. This transaction shall return an error if both parameters are specified.

3210 **Example SQL**

```
# by UUID
SELECT fol.id FROM RegistryPackage fol  # $XDSFolderEntryUUID
WHERE                                   # $XDSFolderEntryUUID
  fol.id IN $XDSFolderEntryUUID         # $XDSFolderEntryUUID
# by uniqueID
```

3215

```
       SELECT fol.id from RegistryPackage fol, ExternalIdentifier uniq                    #
       $XDSFolderUniqueId
       WHERE                                                                              #
3220   $XDSFolderUniqueId
         uniq.registryObject = fol.id AND                                                 #
       $XDSFolderUniqueId
         uniq.identificationScheme = 'urn:uuid:75df8f67-9973-4fbe-a900-df66cefecc5a' AND  #
3225   $XDSFolderUniqueId
         uniq.value IN $XDSFolderUniqueId                                                 #
       $XDSFolderUniqueId
```

Insert this new section. This section documents a new query.

3.16.4.1.4.11 GetAssociations

Retrieve Association objects whose sourceObject or targetObject attribute match $uuid.

3230 **Returns:** Association objects

Parameter Name	Attribute	Opt	Mult
$uuid	None	O	M

Example SQL

```
       SELECT DISTINCT ass.id FROM Association ass
       WHERE
3235     ass.sourceObject IN $uuid OR
         ass.targetObject IN $uuid
```

3.16.4.1.4.12 GetDocumentsAndAssociations

Retrieve a collection of XDSDocumentEntry objects and the Association objects surrounding them.
3240 XDSDocumentEntry objects are selected either by their entryUUID or uniqueId attribute. This is the
GetDocuments query and GetAssociations query combined into a single query.

Returns:

- XDSDocumentEntry objects
- Association objects whose sourceObject or targetObject attribute matches one of the above
3245 objects

Parameter Name	Attribute	Opt	Mult
$XDSDocumentEntryEntryUUID	XDSDocumentEntry. entryUUID	O[1]	M
$XDSDocumentEntryUniqueId	XDSDocumentEntry. uniqueId	O[1]	M

1 - Either $XDSDocumentEntryEntryUUID or $XDSDocumentEntryUniqueId shall be specified. This
transaction shall return an error if both parameters are specified.

This query is specified in two parts: a query of XDSDocumentEntry objects and a separate query of
Association objects.

3250

Example SQL Part 1

```
# UUID param
SELECT doc.id                                                              #
$XDSDocumentEntryEntryUUID
FROM ExtrinsicObject doc                                                   #
$XDSDocumentEntryEntryUUID
WHERE  doc.id IN $XDSDocumentEntryEntryUUID                                #
$XDSDocumentEntryEntryUUID
# uniquid param
    SELECT doc.id FROM ExtrinsicObject doc, ExternalIdentifier uniqId      #
$XDSDocumentEntryUniqueId
    WHERE                                                                  #
$XDSDocumentEntryUniqueId
        uniqId.registryobject = doc.id AND                                #
$XDSDocumentEntryUniqueId
        uniqId.identificationScheme = 'urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab' AND   #
$XDSDocumentEntryUniqueId
        uniqId.value IN $XDSDocumentEntryUniqueId                         #
$XDSDocumentEntryUniqueId
```

Example SQL Part 2

```
SELECT DISTINCT ass.id FROM Association ass                                           #
$XDSDocumentEntryEntryUUID
WHERE                                                                                 #
$XDSDocumentEntryEntryUUID
  ass.sourceObject IN $XDSDocumentEntryEntryUUID OR                                   #
$XDSDocumentEntryEntryUUID
  ass.targetObject IN $XDSDocumentEntryEntryUUID                                      #
$XDSDocumentEntryEntryUUID

SELECT DISTINCT ass.id FROM Association ass, ExtrinsicObject doc, ExternalIdentifier uniqId   #
$XDSDocumentEntryUniqueId
WHERE                                                                                 #
$XDSDocumentEntryUniqueId
  uniqId.registryobject = doc.id AND                                                  #
$XDSDocumentEntryUniqueId
  uniqId.identificationScheme = 'urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab' AND   #
$XDSDocumentEntryUniqueId
  uniqId.value IN $XDSDocumentEntryUniqueId AND                                       #
$XDSDocumentEntryUniqueId
  (ass.sourceObject = doc.id OR                                                       #
$XDSDocumentEntryUniqueId
    ass.targetObject = doc.id)                                                        #
$XDSDocumentEntryUniqueId
```

3.16.4.1.4.13 GetSubmissionSets

Retrieve the XDSSubmissionSet objects used to submit a collection of XDSDocumentEntry and XDSFolder objects. The XDSDocumentEntry and XDSFolder objects of interest are identified by their UUIDs in the $uuid parameter.

Selection: XDSSubmissionSet objects are selected because Association objects exist that have:

- Type HasMember
- targetObject attribute containing one of the UUIDs provided in the $uuid parameter
- sourceObject attribute referencing an XDSSubmissionSet object

Returns:

- XDSSubmissionSet objects described above

Association objects described in the Selection section above

Parameter Name	Attribute	Opt	Mult
$uuid	XDSDocumentEntry. entryUUID and XDSFolder. entryUUID	R	M

3310

Example SQL

3315
```
SELECT ss.id FROM RegistryPackage ss, Classification c, Association a
WHERE
  c.classifiedObject = ss.id AND
  c.classificationNode = 'urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd' AND
  a.sourceObject = ss.id AND
  a.associationType = 'HasMember' AND
  a.targetObject IN $uuid
```

3320

3.16.4.1.5 Security considerations

The transaction shall be audited by the Document Consumer as follows

	Field Name	Opt.	Value Constraints
Event AuditMessage/ EventIdentification	EventID	M	EV (110112, DCM, "Query")
	EventActionCode	M	EV "E" (Execute)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	*M*	*EV("ITI-16", "IHE Transactions", "Registry SQL Query") or EV("ITI-18", "IHE Transactions", "Registry Stored Query")*
Audit Source (Document Consumer) (1)			
Source (Document Consumer) (1)			
Destination (Document Registry) (1)			
Human Requestor (0..1)			
Patient (1)			
Query (1) (AudittMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCode	M	EV 2 (system object)
	ParticipantObjectTypeCodeRole	M	EV 24 (query)
	ParticipantObjectDataLifeCycle	*NA*	
	ParticipantObjectIDTypeCode	M	*EV("ITI-16", "IHE Transactions", "Registry SQL Query")*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	(empty)
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	Shall hold the AdhocQueryRequest of the query, base64 encoded.
	ParticipantObjectDetail	*NA*	
	ParticipantObjectDescription	*U*	*not further specialized*

Note The ParticipantObjectQuery is encoded in base64 to simplify generic library processing of these audit records. Some other
query sources generate queries in binary form. Defective query sources could generate queries that contain improper XML
3325   that would cause processing problems for this audit message. By encoding the contents, the generic audit libraries do not
need to worry about correctness or format of the query request. Any request can be encoded as base64 without causing
problems for the audit capture library.

It is furthermore expected that the analysis processing of audit records use the ParticipantObjectIDTypeCode to determine how to analyze the encoded query.

3330

Using the following common blocks

Audit Source AuditMessage/ AuditSourceIdentification	AuditSourceID	M	The identity of the process issuing the audit message.
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Source AuditMessage/ ActiveParticipant	UserID	M	The identity of the Source. If the source logs, suggested format <process id>@<machine name>. If the destination logs, leave empty.
	AlternateUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	EV TRUE
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	MC	This field shall be present with values selected from those specified in RFC 3881 where applicable.
	NetworkAccessPointID	MC	Shall be present if Net Access Point Type Code is present. Shall use fields as specified in RFC 3881.

Destination AuditMessage/ ActiveParticipant	UserID	M	The identity of the Destination process. For SOAP-based services, this is the SOAP endpoint URI.
	AlternateUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	EV FALSE
	RoleIDCode	M	EV (110152, DCM, "Destination")
	NetworkAccessPointTypeCode	MC	This field shall be present with values selected from those specified in RFC 3881 where applicable.
	NetworkAccessPointID	MC	Shall be present if Net Access Point Type Code is present. Shall use fields as specified in RFC 3881.

Human Requestor AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the transaction.
	AlternateUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	EV TRUE
	RoleIDCode	*U*	*not specialized*
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

3335   Source and destination shall always be specified and refer to the systems executing the transaction. If known, human requestor must be used to additionally identify the human that initiated the transaction.

	ParticipantObjectTypeCode	M	EV 1 (person)

ParticipantObjectTypeCodeRole	M	EV 1 (patient)
ParticipantObjectDataLifeCycle	*NA*	
ParticipantObjectIDTypeCode	M	EV 2 (patient number)
ParticipantObjectSensitivity	*U*	*not specialized*
ParticipantObjectID	M	XDS patientId, in CX format as constrained by XDS
ParticipantObjectName	*U*	*The patient's name. Discouraged for privacy reasons.*
ParticipantObjectQuery	*NA*	
ParticipantObjectDetail	NA	
ParticipantObjectDescription	*U*	*not further specialized*

3340 **3.16.4.2 Query Registry Acknowledgement**

This is the response to the Query Registry message.

3.16.4.2.1 Trigger Events

Completion of query initiated by a Query Registry message.

3.16.4.2.2 Message Semantics

3345 The Query Registry Acknowledgement (AdhocQueryResponse) is returned in one of three forms:

1. List of ObjectRefs
2. Registry metadata describing objects found by query
3. Error message

3.16.4.2.3 Expected Actions

3350 The Document Consumer may process the returned registry data, retrieve documents based on the metadata if the necessary metadata was returned, or handle returned errors

3.16.4.2.4 Security considerations

The transaction shall be audited by the Document Registry as follows

	Field Name	**Opt.**	**Value Constraints**
Event	EventID	M	EV (110112, DCM, "Query")
AuditMessage/ EventIdentification			

	EventActionCode	M	EV "E" (Execute)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	*M*	*EV("ITI-16", "IHE Transactions", "Registry SQL Query") or* *EV("ITI-18", "IHE Transactions", "Registry Stored Query")*

Audit Source (Document Registry) (1)			
Source (Document Source) (1)			
Destination (Document Registry) (1)			
Human Requestor (0..1)			
Patient (1)			

Query (1) **(AuditMessage/ ParticipantObjectIdenti fication)**	ParticipantObjectTypeCode	M	EV 2 (system object)
	ParticipantObjectTypeCodeRole	M	EV 24 (query)
	ParticipantObjectDataLifeCycle	*NA*	
	ParticipantObjectIDTypeCode	M	*EV("ITI-16", "IHE Transactions", "Registry SQL Query")*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	(empty)
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	Shall hold the AdhocQueryRequest of the query, base64 encoded.
	ParticipantObjectDetail	*NA*	
	ParticipantObjectDescription	*U*	*not further specialized*

3355   For queries that do not specify the patient ID in the query request, this ID must be filled from the query response.

Using the following common blocks

Audit Source **AuditMessage/ AuditSourceIdentification**	AuditSourceID	M	The identity of the process issuing the audit message.
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Source **AuditMessage/ ActiveParticipant**	UserID	M	The identity of the Source. If the source logs, suggested format \<process id\>@\<machine name\>. If the destination logs, leave empty.
	AlternateUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	EV TRUE
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	MC	This field shall be present with values selected from those specified in RFC 3881 where applicable.
	NetworkAccessPointID	MC	Shall be present if Net Access Point Type Code is present. Shall use fields as specified in RFC 3881.

	UserID	M	The identity of the Destination process. For SOAP-based services, this is the SOAP endpoint URI.

	AlternateUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	EV FALSE
	RoleIDCode	M	EV (110152, DCM, "Destination")
	NetworkAccessPointTypeCode	MC	This field shall be present with values selected from those specified in RFC 3881 where applicable.
	NetworkAccessPointID	MC	Shall be present if Net Access Point Type Code is present. Shall use fields as specified in RFC 3881.

3360

Human Requestor **AuditMessage/ ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternateUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	EV TRUE
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	

Source and destination shall always be specified and refer to the systems executing the transaction. If known, human requestor must be used to additionally identify the human that initiated the transaction.

3365

Patient **(AudittMessage/ ParticipantObjectIdenti fication)**	ParticipantObjectTypeCode	M	EV 1 (person)
	ParticipantObjectTypeCodeRole	M	EV 1 (patient)
	ParticipantObjectDataLifeCycle	NA	
	ParticipantObjectIDTypeCode	M	EV 2 (patient number)
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	XDS patientId, in CX format as constrained by XDS
	ParticipantObjectName	U	The patient's name. Discouraged for privacy reasons.
	ParticipantObjectQuery	NA	
	ParticipantObjectDetail	NA	
	ParticipantObjectDescription	U	not further specialized

3.17 Retrieve Document

This section corresponds to Transaction ITI-17 of the IHE Technical Framework. The Document Consumer and Document Repository actors use transaction ITI-17.

3370

Note: This transaction is used by the XDS.a Integration Profile. For a discussion on XDS.a and XDS.b Integration Profiles see IHE ITI TF-1 Section 10 and IHE XDS.b Supplement (www.IHE.net/Technical _Frameworks).

3.17.1 Scope

This transaction is used by the Document Consumer to retrieve a document from the Document Repository. The Document Consumer has already obtained the URI information from the Document Registry by means of the Query Registry transaction.

3375

3.17.2 Use Case Roles
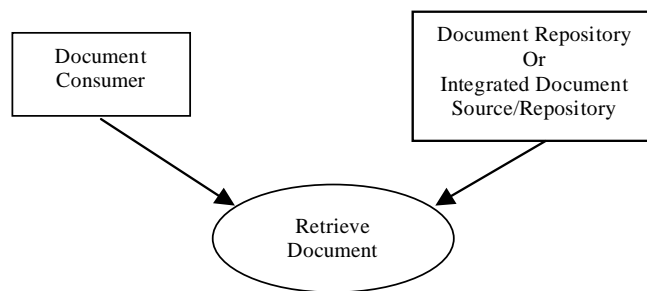
Actor: Document Consumer

Role: Obtains document.

3380

Actor: Document Repository or Integrated Document Source/Repository

Role: Provides documents.

Note: Within this transaction, the Document Repository and Integrated Document Source/Repository actors can be used interchangeably.

3.17.3 Referenced Standard

HTTP	Hyper Text Transfer Protocol HTTP 1.1 (RFC 2616)
MIME	Multipurpose Internet Message Extensions (RFC 2045 to RFC 2049)
SMTP	Simple Mail Transfer Protocol (RFC 2821)
Multipart/Related	The MIME Multipart/Related Content-type (RFC 2387)

3385

3.17.4 Interaction Diagram
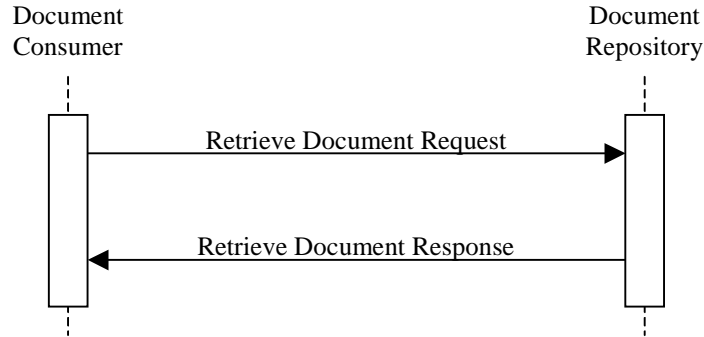
3.17.4.1 Retrieve Document Request

3.17.4.1.1 Trigger Events

3390   The Document Consumer obtains document URIs via the

Query Registry transaction.

3.17.4.1.2 Message Semantics

The URI specifies the protocol and protocol parameters that are to be used to retrieve the document. The Document Repository shall support the following parameters for protocol in the URI:

3395   HTTP

The details of URI handling are specified in the HTTP standard (RFC 2616).

The Document Repository shall fully implement support for any protocol parameters that are required by the HTTP standard.

3.17.4.1.2.1 Request Headers

3400   The HTTP Protocol specifies a variety of request headers that can affect the result returned by the server. Document Consumers may use any request header allowed by the HTTP Protocol2. However, XDS Repositories are not required to acknowledge or support of these headers not required by the protocol, and may be required in certain cases to ignore certain headers. See the table below for details.

Request Header	Repository Support	Comments
Accept Accept-Charset Accept-Language	Always Ignored	These headers, if used by the Repository could in fact alter the content returned from the repository, and so must be ignored by the repository. [inconsistent with RID].
Accept-Encoding	O	This header requests that an encoded form the data be

---

2   Ed Note: To allow common web browsers to be used without restriction.

		returned [e.g., gzip or compress]. Repositories may support this header, but are not required to. Document Consumers must support responses that ignore this content header.
Authorization	O	This header may be sent in environments where EUA is used with XDS. See the EUA profile for more details.
If-Modified-Since	O	Since Repositories are not expected to change documents once stored, they are free to ignore this header or respond as appropriate.

3405

3.17.4.1.3   Expected Actions

A Retrieve Document Response will be generated in return. Details are specified in the HTTP standard.

3.17.4.1.3.1 Basic Patient Privacy Enforcement Option

3410   If the Basic Patient Privacy Enforcement Option is implemented:

1. The Document Consumer actor shall abide by the XDS Affinity Domain Policies represented by the confidentialityCode in the metadata associated with the document. The Document Consumer actor likely will have user access controls or business rule capabilities to determine the details of how confidentiality codes apply to query results. The details of this are product specific and not
3415   specified by IHE. These rules shall reduce the query results to only those that are appropriate to the current situation for that actor and user.

2. The Document Consumer actor shall be able to be configured with Patient Privacy Consent Policies, Patient Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the XDS Affinity Domain Policy. The details of this are product
3420   specific and not specified by IHE.

3.17.4.2 Retrieve Document Response

3.17.4.2.1   Trigger Events

3425   This message is triggered by the:

Retrieve Document Request.

3.17.4.2.2   Message Semantics

XDS Repositories are required to return the following values:

Response Code	When to Return	Support

200 – OK	If the request is valid and data is available.	R
304 – Not Modified	If the request is a valid conditional GET [see HTTP specification], and the document has not been modified since the requested modification date.	O
400 – Bad Request	If the request is not valid.	R
401 – Authorization Required	If the request requires authentication, and an Authorization header is not present, or is not valid. Used in conjunction with EUA.	O
403 – Forbidden	If access needs to be denied for reasons other than authentication failure [e.g., because the request comes from a Node that is not allowed access to the document].	R
404 – Not Found	If the request is syntactically valid, but the document cannot be located, or does not otherwise exist [see RID].	R
410 – Gone	If the request is valid, and the document once existed, but is no longer available [e.g., the document may have been removed at the patients request].	O
5XX – Server Error	The server may return any error code beginning with the digit 5 to indicate a server error.	O

3430

3.17.4.2.2.1 Response Headers

The HTTP Protocol specifies a variety of response headers that provide more information about the response. The use of these headers is described in the table below:

Response Header	Repository Support	Comments
Expires	R	Any valid value according to RFC2616, or 0 [c.f. RID volume]
Content-Encoding	O	If the Document consumer requested encoding of the response, and the repository is able to fulfill that request, it must return the appropriate value in this header.
Content-Type	R	These headers correspond to the mimeType, languageCode, and size attributes of the XDSDocumentEntry. Content-Type is required in the response3. The other two are optional, but if present, must be the same as the values provided to the registry.
Content-Language Content-Length	O	
Last-Modified	R	This header should correspond to the date the document was first stored in the repository [if known], or the date of document creation [XDSDocumentEntry.creationTime].
WWW-Authenticate	O	If the XDS Repository requires authentication and the request did not contain valid credentials, this header must be returned in the 401 response.

3435

---

3   This is to allow browser-based document consumers to activate the appropriate viewer based on the type of data present, without requiring that information to be known in advance before the request is made.

3.17.4.2.3   Expected Actions

The Document Consumer now has the content of the document to process.

3440 **3.17.5 Security Considerations**

Relevant XDS Affinity Domain Security background is discussed in the Register Document transaction (see ITI TF-2: 3.14.5.1).

3.17.5.1 Audit Record Considerations

The Retrieve Document Transaction is PHI-Export event, as defined in table 3.20.6-1.   The Actors
3445 involved in the transaction shall create audit data in conformance with DICOM (Supp 95) "Data Export"/"Data Import", with the following exceptions.

The Repository Actor shall generate an "Export" event. This may be an event for each Retrieve Document Transaction, or multiple transactions for the same patient may be heuristically combined. The heuristics for this combination are not specified by IHE. It is intended to reduce the volume of audit
3450 records. Combination is permitted when the active participants and patient are the same, and the time difference is considered insignificant.

The Document Consumer Actor shall generate an "Import" event. This may be one event per transaction, or multiple transactions may be reported as a single event using a heuristic for combining transactions. Combination is permitted when the active participants and patient are the same, and the
3455 time difference is considered insignificant.

3.17.5.1.1   Document Consumer audit message:

	Field Name	Opt	Value Constraints
Event AuditMessage/ EventIdentification	EventID	M	EV(110107, DCM, "Import")
	EventActionCode	M	"C" (Create)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-17", "IHE Transactions", "Retrieve Document")
Source (Document Repository) (1)			
Destination (Document Consumer) (1)			
Human Requestor (0..n)			
Audit Source (Document Consumer) (1)			
Patient (0..1)			
Document URI (1)			

Where:

Source **AuditMessage/ ActiveParticipant**	UserID	*U*	*not specialized*
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Destination **AuditMessage/ ActiveParticipant**	UserID	*U*	*not specialized*
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human Requestor (if known) **AuditMessage/ ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

Audit Source **AuditMessage/ AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

3460

Patient (if-known) **(AudittMessage/ ParticipantObjectIdentifi cation)**	ParticipantObjectTypeCode	M	"1" (Person)
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
	ParticipantObjectTypeCode	M	"2" (System)
	ParticipantObjectTypeCodeRole	M	"3" (report)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(12, RFC-3881, "URI")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	Document URI
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*

	ParticipantObjectDetail	MC	Document Unique ID

3.17.5.1.2 Document Repository audit message:

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110106, DCM, "Export")
	EventActionCode	M	"R" (Read)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-17", "IHE Transactions", "Retrieve Document")
Source (Document Repository) (1)			
Destination (Document Consumer) (1)			
Audit Source (Document Repository) (1)			
Document URI(1)			

Where:

Source **AuditMessage/** **ActiveParticipant**	UserID	*U*	*not specialized*
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Destination **AuditMessage/** **ActiveParticipant**	UserID	*U*	*not specialized*
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

3465

Audit Source **AuditMessage/** **AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

	ParticipantObjectTypeCode	M	"2" (System)
	ParticipantObjectTypeCodeRole	M	"3" (report)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(12, RFC-3881, "URI")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	Document URI
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*

	ParticipantObjectDetail	MC	Document Unique ID

3.18 Registry Stored Query

3470 This section corresponds to Transaction 18 of the IHE Technical Framework. Transaction 18 is used by the Document Registry and Document Consumer actors.

Note: This transaction is used by the XDS.a and the XDS.b Integration Profile. For a discussion on XDS.a and XDS.b Integration Profiles see IHE ITI TF-1 Section 10 and IHE XDS.b Supplement (www.IHE.net/Technical _Frameworks).

3.18.1 Scope

3475 The Registry Stored Query transaction supports a variety of types of queries. Examples include the following:

Query by patient (Id) for a time interval, by document type(s), by practice setting(s), by author person

Query by Document Source

Query for XDS Folders updated during a time interval

3480 Query for all documents in a Folder or Submission Set

Query by time of submission

The list of XDS registry entries attributes that can be the target of a query are defined in Section 4.1.7 through 4.1.9. This transaction will document the basic syntax and semantics of XDS Document Registry queries.

3485 All queries return:

- Metadata for one or more registry objects, or
- Object references for one or more registry objects (registry UUIDs).

3.18.2 Use Case Roles
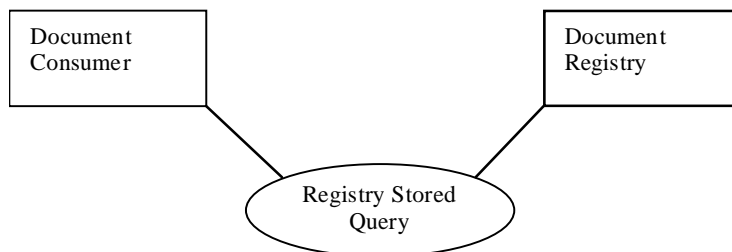
3490 **Actor:** Document Consumer

Role: Requests a query by identifier (UUID), and passes parameters to the query. A parameter controlling the format of the returned data is passed, it selects either object references or full objects.

Actor: Document Registry

Role: Services the query using its stored definitions of the queries defined for XDS.

3495   3.18.3 Referenced Standards

Implementors of this transaction shall comply with all requirements described in ITI TF-2:Appendix V: Web Services for IHE Transactions except for the level of SOAP supported. The SOAP level support depends on the profile conformance of the implementing actor. The following table specifies the level of conformance to SOAP:

3500

Profile implemented by actor	SOAP level required of actor
XDS.a	SOAP 1.1
XDS.b	SOAP 1.2
XDS.a & XDS.b	SOAP 1.1 and SOAP 1.2 for all Registry Stored Query requests without reconfiguration or restart

ebRIM   OASIS/ebXML Registry Information Model v3.0

ebRS   OASIS/ebXML Registry Services Specifications v3.0

3505   Note: The ebRIM and ebRS standards referenced here are version 3.0. Other transactions of XDS.a reference version 2.1.

3.18.4 Interaction Diagram
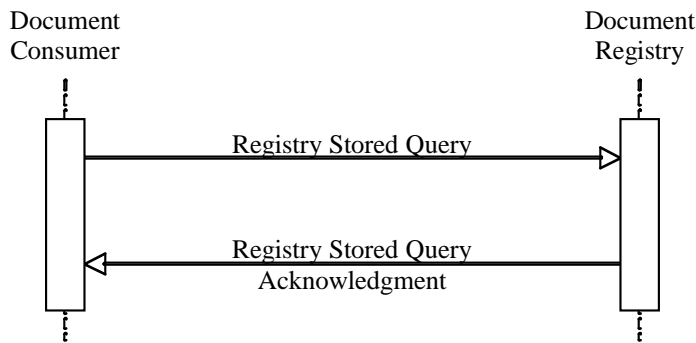
3.18.4.1 Registry Stored Query

This is a query request to the Document Registry from a Document Consumer. The query request
3510   contains:

- A reference to a pre-defined query stored on the Document Registry actor.
- Parameters to the query. The query parameters are matched up with the query variables defined in the query definition on the Document Registry actor.

3.18.4.1.1 Trigger Events

3515   This message is initiated when the Document Consumer wants to query/retrieve document metadata.

3.18.4.1.2 Message Semantics

The semantics of Stored Query are defined in section 6.3. *Stored Query Support* of ebRS version 3.0. This transaction corresponds to section 6.3.2 *Invoking a Stored Query* and 6.3.3 *Response to a Stored Query Invocation.* This profile does not specify how the queries come to be stored in the Registry actor nor how they are to be translated for other database architectures.

3.18.4.1.2.1 Version 3.0 ebXML Registry Standard

This transaction uses ebXML Registry version 3.0. The Invoke Stored Query message and the Invoke Stored Query Acknowledgement message shall be in version 3.0 format and be consistent with version 3.0 ebRIM and ebRS standards.

Version 3.0 ebXML Registry XML Schemas shall be used to validate the messages of this transaction. The major differences between version 2.1 and 3.0 of the Schema are:

- Different XML namespaces
- LeafRegistryObjectList element becomes RegistryObjectList
- ObjectType attribute changes format, changing from a text name to a UUID. For example, RegistryPackage becomes urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:RegistryPackage
- Status attribute value format changes from Approved to urn:oasis:names:tc:ebxml-regrep:StatusType:Approved
- Order of elements changes – Name, Description, Slot, Classification, ExternalIdentifier ordering becomes Slot, Name, Description, Classification, ExternalIdentifier.
- Id attribute is required for Classification, ExternalIdentifier, and Association
- The registryObject attribute is required on the ExternalIdentifier element.
- Association Types must be namespace qualified. For details see section 4.1.6.3 Association type formatting.

It is the responsibility of the Document Registry actor to translate between version 2.1 and version 3.0 formats when returning v2.1 objects in v3.0 query responses.

3.18.4.1.2.2 Sample Query Request

The sample query is included under the section 3.18.4.1.3 Expected Actions.

3.18.4.1.2.3 Query Request Parameters – Coding Style

The ebXML Registry stored query facility (Invoke Stored Query transaction) accepts the following parameters:

- returnType – 'LeafClass' or 'ObjectRef'
- Query ID – a UUID from the Stored Query IDs section (3.18.4.1.2.4) below
- Query Parameters – as defined in the Query Parameters section (3.18.4.1.2.3.7) below

3.18.4.1.2.3.1 Parameter returnType

Registry Stored Query supports the following values for the parameter returnType:

- ObjectRef – a list of object UUIDs (references)
- LeafClass – list of XML elements representing the leaf class of the object returned

The 'LeafClass' returnType is meant for returning a small amount of fully specified ebXML objects (such as a list of ExtrinsicObject (XDSDocumentEntry) elements with full contents: slots, external identifiers, classifications etc.). This type of query result is self-contained, everything known about the object(s) is returned. The specific query documented in this section describes which object types will be included. ObjectRef elements are also returned. These represent objects not included in the returned object list that are referenced by objects in the returned object list. These ObjectRefs are optional by the registry standard version 3.0.

The 'ObjectRef' returnType returns references to the registry objects that match the query. This type query is recommended when the returned object list could be large. An initial query returning ObjectRefs for all objects of interest followed by secondary queries requesting full metadata (query type LeafClass) is an efficient way to query for large bodies of metadata. This strategy is particularly easy to use when querying for a single object type (XDSDocumentEntry or XDSSubmissionSet are examples) since only a single object type is involved.

An ObjectRef looks like:

```
<ObjectRef id="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"/>
```

3.18.4.1.2.3.2 Parameter Query ID

This parameter holds the UUID assigned to the query to be invoked. UUIDs are assigned by this profile (see section 3.18.4.1.2.4) to each of the queries defined in section 3.18.4.1.2.3.7.

3.18.4.1.2.3.3 Date/Time Coding

All Date/time values are to be inclusive, interpreted as:

$XDSDocumentEntryCreationTimeFrom <= XDSDocumentEntry.creationTime < $XDSDocumentEntryCreationTimeTo

for example. The 'From' time or the 'To' time may be omitted.

3.18.4.1.2.3.4 Intentionally Left Blank

3.18.4.1.2.3.5 Coding of Single/Multiple Values

Single values are coded as

- 123 - without quotes for numbers
- 'urn:oasis:names:tc:ebxml-regrep:StatusType:Approved' - in single quotes for strings.
- 'Children's Hospital' – a single quote is inserted in a string by specifying two single quotes

Within the LIKE predicate

- Underscore ('_') matches an arbitrary character
- Percent ('%') matches an arbitrary string

Format for multiple values is

- (value, value, value, …) OR
- (value) if only one value is to be specified.

3590 where each value is coded as described above for single values.

When coding multiple values there is a potential conflict between needing to code a long list of values and the length restriction imposed by Schema on the size of the value of the <Value/> element. Slot values shall never exceed the Schema-enforced limit. Therefore, the use of multiple Value elements within the Slot shall be acceptable. Splits may occur only between values, where each Value element is
3595 surrounded by parentheses. The following example shows multiple values, split across multiple Value elements:

<Slot name="$uuid">

   <ValueList>

     <Value>('urn:uuid:a96d7361-6617-488a-891c-ee3f37d1f218','urn:uuid: 5655a680-1b6a-11dd-
3600 bd0b-0800200c9a66')</Value>

     <Value>('urn:uuid:ae315e81-2056-4829-a5b4-cf9531941f96')</Value>

   </ValueList>

</Slot>

This example shall be treated as equivalent to:

3605 <Slot name="$uuid">

   <ValueList>

     <Value>('urn:uuid:a96d7361-6617-488a-891c-ee3f37d1f218','urn:uuid: 5655a680-1b6a-11dd-
bd0b-0800200c9a66','urn:uuid:ae315e81-2056-4829-a5b4-cf9531941f96')</Value>

   </ValueList>

3610 </Slot>

Character comparisons shall be performed in accordance with the rules in 4.2.

And/or semantics for the coding of parameters shall be available only on parameters for multi-valued metadata elements (such as $XDSDocumentEntryEventCodeList). . Multi-valued parameters shall be coded in two ways with different interpretations.

3615 A parameter specified as a Slot with multiple values shall be interpreted as disjunction (OR semantics). For example:

```
<rim:Slot name="$XDSDocumentEntryEventCodeList">
  <rim:ValueList>
    <rim:Value>('a')</rim:Value>
    <rim:Value>('b')</rim:Value>
  </rim:ValueList>
</rim:Slot>
```

shall match an XDSDocumentEntry object with an eventCodeList attribute containing either 'a' or 'b'. The following coding of the parameter shall yield the same results:

3625
```
<rim:Slot name="$XDSDocumentEntryEventCodeList">
  <rim:ValueList>
    <rim:Value>('a','b')</rim:Value>
  </rim:ValueList>
```

```
              </rim:Slot>
```

3630 A parameter specified as multiple Slots shall be interpreted as conjunction (AND semantics). For
example:

```
        <rim:Slot name="$XDSDocumentEntryEventCodeList">
          <rim:ValueList>
            <rim:Value>('a')</rim:Value>
3635      </rim:ValueList>
        </rim:Slot>
        <rim:Slot name="$XDSDocumentEntryEventCodeList">
          <rim:ValueList>
            <rim:Value>('b')</rim:Value>
3640      </rim:ValueList>
        </rim:Slot>
```

shall match an XDSDocumentEntry object with an eventCodeList attribute containing both 'a' and 'b'.

Furthermore, the following specification of the $XDSDocumentEntryEventCodeList parameter:

```
        <rim:Slot name="$XDSDocumentEntryEventCodeList">
3645      <rim:ValueList>
            <rim:Value>('a','b')</rim:Value>
          </rim:ValueList>
        </rim:Slot>
        <rim:Slot name="$XDSDocumentEntryEventCodeList">
3650      <rim:ValueList>
            <rim:Value>('c')</rim:Value>
          </rim:ValueList>
        </rim:Slot>
```

shall be interpreted as matching a document having eventCode (a OR b) AND c.

3655

3.18.4.1.2.3.6 Valid Document Status Values

The Registry Object status values, in ebRIM v 3.0 format, used by XDS are:

```
     urn:oasis:names:tc:ebxml-regrep:StatusType:Submitted
     urn:oasis:names:tc:ebxml-regrep:StatusType:Approved
3660  urn:oasis:names:tc:ebxml-regrep:StatusType:Deprecated
```

3.18.4.1.2.3.6.1 Valid AdhocQueryResponse Status Values

The status attribute of AdhocQueryResponse shall contain one of the following values:

```
     urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success
     urn:ihe:iti:2007:ResponseStatusType:PartialSuccess
3665  urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure
```

See section 4.1.13 Error Reporting for the interpretation of these values.

3.18.4.1.2.3.7 Parameters for Required Queries

The sections below document the queries defined in the Query Registry transaction [ITI-16]. These
sections document a collection of Stored Queries. Document Registry actors implementing this
3670 transaction shall support all queries in this collection and all parameters defined for each query.
Document Consumer actors implementing this transaction shall implement one or more of these queries
as needed to support the use cases it implements.

Note that dollar sign ($) prefix on query parameters is required by ebRS 3.0.

In the query parameter tables below, each row represents a query parameter. Optional parameters which
3675 are not included in the query invocation have no affect on the query. Queries return registry objects that
match all the supplied parameters. When multiple values are included for a parameter, objects are
returned that match any included value (within the context of the larger query).

In the following tables, coding schemes are represented by a pair of parameters, one representing the
code value and the second representing the coding scheme name from which the code value is taken.
3680 For example, in the FindDocuments query, are found parameters

- $XDSDocumentEntryClassCode – classCode values of interest
- $XDSDocumentEntryClassCodeScheme – coding scheme for each class code value

While the 'codes' can be specified without the 'code schemes', if any code schemes are specified (if the
code schemes parameter is specified) then the code schemes for all codes listed shall be present and in
3685 the same order as the codes.

3.18.4.1.2.3.7.1 FindDocuments

Find documents (XDSDocumentEntry objects) in the registry for a given patientID with a matching
'status' attribute. The other parameters can be used to restrict the set of XDSDocumentEntry objects
returned.

3690 **Returns:** XDSDocumentEntry objects matching the query parameters

Parameter Name	Attribute	Opt	Mult
$XDSDocumentEntryPatientId	XDSDocumentEntry. patientId	R	--
$XDSDocumentEntryClassCode	XDSDocumentEntry. classCode	O	M
$XDSDocumentEntryClassCodeScheme	XDSDocumentEntry. classCode[1]	O[2]	M[2]
$XDSDocumentEntryPracticeSettingCode	XDSDocumentEntry. practiceSettingCode	O	M
$XDSDocumentEntryPracticeSettingCodeScheme	XDSDocumentEntry. practiceSettingCode[1]	O[2]	M[2]
$XDSDocumentEntryCreationTimeFrom	Lower value of XDSDocumentEntry. creationTime	O	--
$XDSDocumentEntryCreationTimeTo	Upper value of XDSDocumentEntry. creationTime	O	--
$XDSDocumentEntryServiceStartTimeFrom	Lower value of XDSDocumentEntry. serviceStartTime	O	--
$XDSDocumentEntryServiceStartTimeTo	Upper value of XDSDocumentEntry. serviceStartTime	O	--
$XDSDocumentEntryServiceStopTimeFrom	Lower value of XDSDocumentEntry. serviceStopTime	O	--
$XDSDocumentEntryServiceStopTimeTo	Upper value of XDSDocumentEntry. serviceStopTime	O	--
$XDSDocumentEntryHealthcareFacilityTypeCode	XDSDocumentEntry.	O	M

Parameter Name	Attribute	Opt	Mult
	healthcareFacilityTypeCode		
$XDSDocumentEntryHealthcareFacilityTypeCodeScheme	XDSDocumentEntry. healthcareFacilityTypeCode[1]	O[2]	M[2]
$XDSDocumentEntryEventCodeList	XDSDocumentEntry. eventCodeList[3]	O	M
$XDSDocumentEntryEventCodeListScheme	XDSDocumentEntry. eventCodeList[1]	O[2]	M[2]
$XDSDocumentEntryConfidentialityCode[3]	XDSDocumentEntry. confidentialityCode[3]	O	M
$XDSDocumentEntryConfidentialityCodeScheme	XDSDocumentEntry. confidentialityCode	O[2]	M[2]
$XDSDocumentEntryAuthorPerson4	XDSDocumentEntry. author	O	M
$XDSDocumentEntryFormatCode	XDSDocumentEntry. formatCode	O	M
$XDSDocumentEntryStatus	XDSDocumentEntry. status	R	M

[1]This attribute is not listed by name in table 4.1-5 Document Metadata Attribute Definition. It is included in the documentation of the attribute that bears the same name without the 'Scheme' suffix. As an example, XDSDocumentEntry.ClassCodeScheme is not an attribute listed in attribute table for XDSDocumenEntry. It is documented as part of XDSDocumentEntry.classCode, specifically as the 'codingScheme' Slot.

3695

[2]This parameter is optional but if included shall 1) have the same number of values as the corresponding 'code' attribute, 2) the ith value of the 'code' attribute (e.g. XDSDocumentEntryClassCode) shall correspond to the ith value of the 'codeScheme' attribute (e.g. XDSDocumentEntryClassCodeScheme).

3700   [3]Supports AND/OR semantics as specified in section 3.18.4.1.2.3.5.

[4]The value for this parameter is a pattern compatible with the SQL keyword LIKE which allows the use of the following wildcard characters: % to match any (or no) characters and _ to match a single character. The match shall be applied to the text contained in the Value elements of the authorPerson Slot on the author Classification (value strings of the authorPerson sub-attribute)

3705

3.18.4.1.2.3.7.2 FindSubmissionSets

Find submission sets (XDSSubmissionSet objects) in the registry for a given patientID with matching 'status' attribute. The other parameters can be used to restrict the collection of XDSSubmissionSet objects returned.

3710   **Returns:** XDSSubmissionSet objects matching the query parameters

Parameter Name	Attribute	Opt	Mult
$XDSSubmissionSetPatientId	XDSSubmissionSet. patientId	R	--
$XDSSubmissionSetSourceId	XDSSubmissionSet. sourceId	O	M
$XDSSubmissionSetSubmissionTimeFrom	XDSSubmissionSet. submissionTime Lower value	O	--
$XDSSubmissionSetSubmissionTimeTo	XDSSubmissionSet. submissionTime Upper value	O	--
$XDSSubmissionSetAuthorPerson[1]	XDSSubmissionSet. authorPerson	O	--
$XDSSubmissionSetContentType	XDSSubmissionSet.	O	M

Parameter Name	Attribute	Opt	Mult
	contentTypeCode		
$XDSSubmissionSetStatus	XDSSubmissionSet. status	R	M

[1]The value for this parameter is a pattern compatible with the SQL keyword LIKE which allows the use of the following wildcard characters: % to match any (or no) characters and _ to match a single character. The match shall be applied to the text contained in the Value elements of the authorPerson Slot on the author Classification (value strings of the authorPerson sub-attribute).

3715 **3.18.4.1.2.3.7.3 FindFolders**

Find folders (XDSFolder objects) in the registry for a given patientID with matching 'status' attribute. The other parameters can be used to restrict the collection of XDSFolder objects returned.

Returns: XDSFolder objects matching the query parameters

Parameter Name	Attribute	Opt	Mult
$XDSFolderPatientId	XDSFolder.patientId	R	--
$XDSFolderLastUpdateTimeFrom	XDSFolder. lastUpdateTime lower value	O	--
$XDSFolderLastUpdateTimeTo	XDSFolder. lastUpdateTime upper bound	O	--
$XDSFolderCodeList[3]	XDSFolder. codeList	O	M
$XDSFolderCodeListScheme	XDSFolder. codeList[1]	O[2]	M[2]
$XDSFolderStatus	XDSFolder.status	R	M

[1]This attribute is not listed by name in table 4.1-5 Document Metadata Attribute Definition. It is
3720 included in the documentation of the attribute that bears the same name without the 'Scheme' suffix. As an example, XDSDocumentEntry.ClassCodeScheme is not an attribute listed in attribute table for XDSDocumenEntry. It is documented as part of XDSDocumentEntry.classCode, specifically as the 'codingScheme' Slot.

[2]This parameter is optional but if included shall 1) have the same number of values as the corresponding
3725 'code' attribute, 2) the ith value of the 'code' attribute (e.g. XDSDocumentEntryClassCode) shall correspond to the ith value of the 'codeScheme' attribute (e.g. XDSDocumentEntryClassCodeScheme).

[3]Supports AND/OR semantics as specified in section 3.18.4.1.2.3.5.

3.18.4.1.2.3.7.4 GetAll

Get all registry content for a patient given the indicated status, format codes, and confidentiality codes.

3730 **Returns:**

- XDSSubmissionSet, XDSDocumentEntry, and XDSFolder objects with patientId attribute matching $patientId parameter
- Association objects with sourceObject or targetObject attribute matching one of the above objects

Parameter Name	Attribute	Opt	Mult
$patientId	XDSFolder. patientId, XDSSubmissionSet. patientId, XDSDocumentEntry. patientId	R	--
$XDSDocumentEntryStatus	XDSDocumentEntry. status	R	M

Parameter Name	Attribute	Opt	Mult
$XDSSubmissionSetStatus	XDSSubmissionSet. status	R	M
$XDSFolderStatus	XDSFolder. status	R	M
$XDSDocumentEntryFormatCode	XDSDocumentEntry. formatCode	O	M
$XDSDocumentEntryConfidentialityCode[1]	XDSDocumentEntry. confidentialityCode[1]	O	M

[1]Supports AND/OR semantics as specified in section 3.18.4.1.2.3.5.

3735 **3.18.4.1.2.3.7.5 GetDocuments**

Retrieve a collection of XDSDocumentEntry objects. XDSDocumentEntry objects are selected either by their entryUUID or uniqueId attribute.

Returns: XDSDocumentEntry objects requested

Parameter Name	Attribute	Opt	Mult
$XDSDocumentEntryEntryUUID	XDSDocumentEntry. entryUUID	O[1]	M
$XDSDocumentEntryUniqueId	XDSDocumentEntry. uniqueId	O[1]	M
$homeCommunityId	None	O[2]	--

[1]Either $XDSDocumentEntryEntryUUID or $XDSDocumentEntryUniqueId shall be specified. This
3740 transaction shall return an error if both parameters are specified.

[2]The homeCommunityId value is specified as the home attribute on the AdhocQuery element of the query request, as in: <AdhocQuery id="…" home="urn:oid:1.2.3" … >. Document Consumer actors shall specify the homeCommunityId value if they received a value for this attribute as part of the previous Registry Stored Query response entry which contained the specified EntryUUID or UniqueID.
3745 See Section 3.18.4.1.2.3.8 for more details.

Note: A query for a single XDSDocumentEntry.uniqueId can return multiple results. See section 4.1.4 under the topic of Document metadata duplication for explanation.

3.18.4.1.2.3.7.6 GetFolders

Retrieve a collection of XDSFolder objects. XDSFolder objects are selected either by their entryUUID
3750 or uniqueId attribute.

Returns: XDSFolder objects requested.

Parameter Name	Attribute	Opt	Mult
$XDSFolderEntryUUID	XDSFolder. entryUUID	O[1]	M
$XDSFolderUniqueId	XDSFolder. uniqueId	O[1]	M
$homeCommunityId	None	O[2]	--

[1]Either $XDSFolderEntryUUID or $XDSFolderUniqueId shall be specified. This transaction shall return an error if both parameters are specified.

[2]The homeCommunityId value is specified as the home attribute on the AdhocQuery element of the
3755 query request, as in: <AdhocQuery id="…" home="urn:oid:1.2.3" … >. Document Consumer actors shall specify the homeCommunityId value if they received a value for this attribute as part of the previous Registry Stored Query response entry which contained the specified EntryUUID or UniqueID. See Section 3.18.4.1.2.3.8 for more details.

3.18.4.1.2.3.7.7 GetAssociations

3760   Retrieve Association objects whose sourceObject or targetObject attribute match $uuid.

Returns: Association objects

Parameter Name	Attribute	Opt	Mult
$uuid	None	R	M
$homeCommunityId	None	O[1]	-

[1]The homeCommunityId value is specified as the home attribute on the AdhocQuery element of the query request, as in: <AdhocQuery id="…" home="urn:oid:1.2.3" … >.   Document Consumer actors shall specify the homeCommunityId value if they received a value for this attribute as

3765   part of the previous Registry Stored Query response entry which contained the specified EntryUUID or UniqueID. See Section 3.18.4.1.2.3.8 for more details.

3.18.4.1.2.3.7.8 GetDocumentsAndAssociations

Retrieve a collection of XDSDocumentEntry objects and the Association objects surrounding them.
3770   XDSDocumentEntry objects are selected either by their entryUUID or uniqueId attribute. This is the GetDocuments query and GetAssociations query combined into a single query.

Returns:

- XDSDocumentEntry objects

- Association objects whose sourceObject or targetObject attribute matches one of the above objects

Parameter Name	Attribute	Opt	Mult
$XDSDocumentEntryEntryUUID	XDSDocumentEntry. entryUUID	O[1]	M
$XDSDocumentEntryUniqueId	XDSDocumentEntry. uniqueId	O[1]	M
$homeCommunityId	None	O[2]	--

3775   [1]Either $XDSDocumentEntryEntryUUID or $XDSDocumentEntryUniqueId shall be specified. This transaction shall return an error if both parameters are specified.

[2]The homeCommunityId value is specified as the home attribute on the AdhocQuery element of the query request, as in: <AdhocQuery id="…" home="urn:oid:1.2.3" … >. Document Consumer actors shall specify the homeCommunityId value if they received a value for this attribute as part of the
3780   previous Registry Stored Query response entry which contained the specified EntryUUID or UniqueID. See Section 3.18.4.1.2.3.8 for more details.

3.18.4.1.2.3.7.9 GetSubmissionSets

Retrieve the XDSSubmissionSet objects used to submit a collection of XDSDocumentEntry and
3785   XDSFolder objects. The XDSDocumentEntry and XDSFolder objects of interest are identified by their UUIDs in the $uuid parameter.

Selection: XDSSubmissionSet objects are selected because Association objects exist that have:

- Type HasMember

- targetObject attribute containing one of the UUIDs provided in the $uuid parameter

3790
- sourceObject attribute referencing an XDSSubmissionSet object

Returns:

- XDSSubmissionSet objects described above

- Association objects described in the Selection section above

Parameter Name	Attribute	Opt	Mult
$uuid	XDSDocumentEntry. entryUUID and XDSFolder. entryUUID	R	M
$homeCommunityId	None	O[1]	--

[1]The homeCommunityId value is specified as the home attribute on the AdhocQuery element of the
3795   query request, as in: <AdhocQuery id="…" home="urn:oid:1.2.3" … >.   Document
Consumer actors shall specify the homeCommunityId value if they received a value for this attribute as
part of the previous Registry Stored Query response entry which contained the specified EntryUUID or
UniqueID. See Section 3.18.4.1.2.3.8 for more details.

3800   **3.18.4.1.2.3.7.10 GetSubmissionSetAndContents**

Retrieve an XDSSubmissionSet object along with its contents. XDSSubmissionSet objects are selected
either by their entryUUID or uniqueId attribute. The XDSDocumentEntry objects returned shall match:

- One of the confidentiality codes listed if that parameter is included and

- One of the format codes listed if that parameter is included

3805   **Returns:**

- XDSSubmissionSet object specified in the query

- Association objects with type HasMember whose sourceObject attribute references the above
  XDSSubmissionSet object

- XDSDocumentEntry and XDSFolder objects referenced by the targetObject attribute of one of the
3810   above Associations

- Association object with type HasMember whose sourceObject attribute references an XDSFolder
  object targeted by the preceding rule and whose targetObject attribute references an
  XDSDocumentEntry object also targeted by the preceding rule.

Parameter Name	Attribute	Opt	Mult
$XDSSubmissionSetEntryUUID	XDSSubmissionSet. entryUUID	O[1]	--
$XDSSubmissionSetUniqueId	XDSSubmissionSet. uniqueId	O[1]	--
$XDSDocumentEntryFormatCode	XDSDocumentEntry. formatCode	O	M
$XDSDocumentEntryConfidentialityCode	XDSDocumentEntry. confidentialityCode[2]	O	M
$homeCommunityId	None	O[3]	--

3815   [1]Either $XDSSubmissionSetEntryUUID or $XDSSubmissionSetUniqueId shall be specified. This
transaction shall return an error if both parameters are specified.

[2]Supports AND/OR semantics as specified in section 3.18.4.1.2.3.5.

[3]The homeCommunityId value is specified as the home attribute on the AdhocQuery element of the query request, as in: <AdhocQuery id="…" home="urn:oid:1.2.3" … >. Document Consumer actors shall specify the homeCommunityId value if they received a value for this attribute as part of the previous Registry Stored Query response entry which contained the specified EntryUUID or UniqueID. See Section 3.18.4.1.2.3.8 for more details.

3.18.4.1.2.3.7.11 GetFolderAndContents

Retrieve an XDSFolder object and its contents. XDSFolder objects are selected either by their entryUUID or uniqueId attribute. The XDSDocumentEntry objects returned shall match one of the confidentiality codes listed if that parameter is included.

Returns:

- XDSFolder object specified in the query

- Association objects of type HasMember that have a sourceObject attribute referencing the XDSFolder object specified in the query

- XDSDocumentEntry objects referenced by the targetObject attribute of one of the Association objects specified above

Parameter Name	Attribute	Opt	Mult
$XDSFolderEntryUUID	XDSFolder. entryUUID	O[1]	--
$XDSFolderUniqueId	XDSFolder. uniqueId	O[1]	--
$XDSDocumentEntryFormatCode	XDSDocumentEntry. formatCode	O	M
$XDSDocumentEntryConfidentialityCode	XDSDocumentEntry. confidentialityCode[2]	O	M
$homeCommunityId	None	O[3]	--

[1]Either $XDSFolderEntryUUID or $XDSFolderUniqueId shall be specified. This transaction shall return an error if both parameters are specified.

[2]Supports AND/OR semantics as specified in section 3.18.4.1.2.3.5.

[3]The homeCommunityId value is specified as the home attribute on the AdhocQuery element of the query request, as in: <AdhocQuery id="…" home="urn:oid:1.2.3" … >. Document Consumer actors shall specify the homeCommunityId value if they received a value for this attribute as part of the previous Registry Stored Query response entry which contained the specified EntryUUID or UniqueID. See Section 3.18.4.1.2.3.8 for more details.

3.18.4.1.2.3.7.12 GetFoldersForDocument

Retrieve XDSFolder objects that contain the XDSDocumentEntry object provided with the query. XDSDocumentEntry objects are selected either by their entryUUID or uniqueId attribute.

Returns: XDSFolder objects that contain specified XDSDocumentEntry object. More specifically, for each Association object of type HasMember that has a targetObject attribute referencing the target XDSDocumentEntry object, return the object referenced by its sourceObject if it is of type XDSFolder.

Parameter Name	Attribute	Opt	Mult
$XDSDocumentEntryEntryUUID	XDSDocumentEntry. entryUUID	O[1]	--
$XDSDocumentEntryUniqueId	XDSDocumentEntry. uniqueId	O[1]	--
$homeCommunityId	None	O[2]	--

3850   [1]Either $XDSDocumentEntryEntryUUID or $XDSDocumentEntryUniqueId shall be specified. This transaction shall return an error if both parameters are specified.

[2]The homeCommunityId value is specified as the home attribute on the AdhocQuery element of the query request, as in: <AdhocQuery id="…" home="urn:oid:1.2.3" … >. Document Consumer actors shall specify the homeCommunityId value if they received a value for this attribute as part of the

3855   previous Registry Stored Query response entry which contained the specified EntryUUID or UniqueID. See Section 3.18.4.1.2.3.8 for more details.

> Note: A query for a single XDSDocumentEntry.uniqueId can return multiple results. See section 4.1.4 under the topic of Document metadata duplication for explanation.

3.18.4.1.2.3.7.13 GetRelatedDocuments

3860   Retrieve XDSDocumentEntry objects that are related to the specified document via Association objects. Also return the Association objects. The specified document is designated by UUID or uniqueId. The query shall return

- Association objects where:

    - The sourceObject attribute OR the targetObject attribute references the specified
3865   document AND

    - Both sourceObject attribute and targetObject attribute reference documents AND

    - The associationType attribute matches a value included in the $AssociationTypes parameter

- XDSDocumentEntry objects referenced by the targetObject attribute OR the sourceObject attribute
3870   of an Association object matched above.

> Note: A side effect of the query is that the specified document is returned in the results if at least one Association is returned.

> Note: A side effect of this query is that if the document specified by the $XDSDocumentEntryUUID or $XDSDocumentEntryUniqueId parameters has no associations linking it to other documents, then no documents and no associations are returned.

3875   See section 4.1.6 Document Relationships and Associations for background.

Returns: Association objects and related XDSDocumentEntry objects

Given : An XDSDocumentEntry object and a collection of association types.

Parameter Name	Attribute	Opt	Mult
$XDSDocumentEntryEntryUUID	XDSDocumentEntry. entryUUID	O[1]	--
$XDSDocumentEntryUniqueId	XDSDocumentEntry. uniqueId	O[1]	--
$AssociationTypes	Not a named attribute	R	M
$homeCommunityId	None	O[2]	--

[1]Either $XDSDocumentEntryEntryUUID or $XDSDocumentEntryUniqueId shall be specified. This
transaction shall return an error if both parameters are specified.

[2]The homeCommunityId value is specified as the home attribute on the AdhocQuery element of the
query request, as in: <AdhocQuery id="…" home="urn:oid:1.2.3" … >. Document Consumer actors
shall specify the homeCommunityId value if they received a value for this attribute as part of the
previous Registry Stored Query response entry which contained the specified EntryUUID or UniqueID.
See Section 3.18.4.1.2.3.8 for more details.

> Note: A query for a single XDSDocumentEntry.uniqueId can return multiple results. See section 4.1.4 under the topic of Document
> metadata duplication for explanation.

3.18.4.1.2.3.8 Use of homeCommunityId

The Registry Stored Query makes use of the homeCommunityId which is a globally unique identifier for
a community and is used to obtain the Web Services endpoint of services that provide access to data in
that community. homeCommunityId is structured as an OID limited to 64 characters and specified in
URI syntax, for example the homeCommunityId of 1.2.3 would be formatted as `urn:oid:1.2.3`.

Its use is as follows:

- It is returned within the response to Registry Stored Query transactions to indicate the
  association of a response element with a community. It is specified as the ebRIM 'home' attribute
  within the ExtrinsicObject, RegistryPackage and ObjectRef elements. Document Consumers
  process the value as an opaque unique identifier.

- It is an optional parameter to Registry Stored Query requests, not requiring a patient id
  parameter, and Retrieve Document Set requests to indicate which community to direct the
  request.

For stored queries which do not require the patient id as a parameter , meaning query by EntryUUID or
UniqueID:

- If the Document Consumer received the EntryUUID or uniqueID in a previous Registry Stored
  Query response which contained a homeCommunityId, then the Document Consumer shall
  specify the homeCommunityId parameter.

- The homeCommunityId value is specified as the home attribute on the AdhocQuery element of
  the query request, as in:
  `<AdhocQuery id="…" home="urn:oid:1.2.3" … >`

- Each query request can have at most one homeCommunityId value. If the Document Consumer
  specifies multiple entryUUID or uniqueID values they must all be associated with the same
  homeCommunityId value. Multiple individual query requests can be used to retrieve data
  associated with different homeCommunityIds.

3.18.4.1.2.4 Stored Query IDs

The standard XDS queries are assigned the following Query IDs. These IDs are used in the
AdhocQueryRequest to reference queries stored on the Document registry actor. Query IDs are in UUID
format (RFC4122). An error shall be returned when an unsupported stored query ID is received.

Note: This query mechanism can be extended by adding a query by allocating a Query ID, defining query parameters, and implementing the query in the Document Registry.

3920

Query Name	Query ID
FindDocuments	`urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d`
FindSubmissionSets	`urn:uuid:f26abbcb-ac74-4422-8a30-edb644bbc1a9`
FindFolders	`urn:uuid:958f3006-baad-4929-a4de-ff1114824431`
GetAll	`urn:uuid:10b545ea-725c-446d-9b95-8aeb444eddf3`
GetDocuments	`urn:uuid:5c4f972b-d56b-40ac-a5fc-c8ca9b40b9d4`
GetFolders	`urn:uuid:5737b14c-8a1a-4539-b659-e03a34a5e1e4`
GetAssociations	`urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155`
GetDocumentsAndAssociations	`urn:uuid:bab9529a-4a10-40b3-a01f-f68a615d247a`
GetSubmissionSets	`urn:uuid:51224314-5390-4169-9b91-b1980040715a`
GetSubmissionSetAndContents	`urn:uuid:e8e3cb2c-e39c-46b9-99e4-c12f57260b83`
GetFolderAndContents	`urn:uuid:b909a503-523d-4517-8acf-8e5834dfc4c7`
GetFoldersForDocument	`urn:uuid:10cae35a-c7f9-4cf5-b61e-fc3278ffb578`
GetRelatedDocuments	`urn:uuid:d90e5407-b356-4d91-a89f-873917b4b0e6`

3.18.4.1.2.5 Intentionally Left Blank

3.18.4.1.2.6 Managing Large Query Responses

EbXML version 3.0 supports query results pagination (ebRS version 3.0 chapter 6.2). The interactions
3925 between the stored query capability and the query results pagination capability within the standard have never been reconciled and are not recommended for use together. It is recommended instead that query pagination be implemented within the Document Consumer actor.

This can be accomplished by specifying returnType="ObjectRef" on all large queries. This returns a list of references (UUIDs) instead of full objects (large XML structures). This is practical for queries
3930 returning thousands of objects. To construct a page for display, a small number of objects can be retrieved through a second query. This is repeated for each page. As an example, the following sequence of queries could be used to list a large number of documents:

- FindDocuments query with returnType="ObjectRef" which returns a large collections of ObjectRefs (UUIDs)

3935
- GetDocuments query with returnType="LeafClass" issued with a subset of the above returned UUIDs which returns the details to construct one page of listing

OR

GetDocumentsAndAssocations query with returnType="LeafClass" issued with a subset of the above returned UUIDs which returns the details to construct one page of listing. By retrieving the Association
3940 objects, the existence of document replacement, transformation, and ammedment can be included into the display.

3.18.4.1.2.7 Web Services Transport

The query request and response will be transmitted using Web Services, according to the requirements specified in Appendix V. The specific values for the WSDL describing the Stored Query Service are
3945 described in this section.

The Document Registery actor shall accept a Registry Stored Query Request formatted as a SIMPLE SOAP message and respond with a Registry Stored Query Response formatted as a SIMPLE SOAP message. The Document Consumer actor shall generate the Registry Stored Query Request formatted as a SIMPLE SOAP message and accept a Registry Stored Query Response formatted as a SIMPLE SOAP
3950 message.

IHE-WSP201) The attribute /wsdl:definitions/@name shall be "DocumentRegistry".

The following WSDL naming conventions shall apply:

```
        wsdl:definitions/@name="DocumentRegistry":
        query message      -> "RegistryStoredQuery_Message"
3955    query response     -> "RegistryStoredQuery_Response_Message"
        portType           -> "DocumentRegistry_PortType"
        operation          -> "RegistryStoredQuery"
        SOAP 1.2 binding   -> "DocumentRegistry_Binding_Soap12"
        SOAP 1.2 port      -> "DocumentRegistry_Port_Soap12"
3960    SOAP 1.1 binding   -> "DocumentRegistry_Binding_Soap11"
        SOAP 1.1 port      -> "DocumentRegistry_Port_Soap11"
```

 IHE-WSP202) The targetNamespace of the WSDL shall be "urn:ihe:iti:xds-b:2007"

These are the requirements for the Registry Stored Query transaction presented in the order in which
3965 they would appear in the WSDL definition:

- The following types shall be imported (xsd:import) in the /definitions/types section:

  - namespace=" urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0", schemaLocation="query.xsd"

- The /definitions/message/part/@element attribute of the Registry Stored Query Request
3970   message shall be defined as "query:AdhocQueryRequest"

- The /definitions/message/part/@element attribute of the Registry Stored Query Response message shall be defined as "query:AdhocQueryResponse"

- The /definitions/portType/operation/input/@wsaw:Action attribute for the Registry Stored Query Request message shall be defined as "urn:ihe:iti:2007:RegistryStoredQuery"

3975
- The /definitions/portType/operation/output/@wsaw:Action attribute for the Registry Stored Query Response message shall be defined as "urn:ihe:iti:2007:RegistryStoredQueryResponse"

- The /definitions/binding/operation/soap12:operation/@soapAction attribute should be defined as "urn:ihe:iti:2007:RegistryStoredQuery"

3980   The following WSDL fragment shows an example of Registry Stored Query transaction definition:

```xml
<?xml version="1.0" encoding="utf-8"?>
<definitions ...>
  ...
  <types>
    <xsd:schema elementFormDefault="qualified" targetNamespace="urn:ihe:iti:xds-b:2007">
      <xsd:import
        namespace="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
        schemaLocation="schema\query.xsd"/>
      ...
    </xsd:schema>
  </types>
  <message name="RegistryStoredQuery_Message">
    <documentation>Registry Stored Query</documentation>
    <part name="body" element="query:AdhocQueryRequest"/>
  </message>
  <message name="RegistryStoredQueryResponse_Message">
    <documentation>Registry Stored Query Response</documentation>
    <part name="body" element="query:AdhocQueryResponse"/>
  </message>
  ...
  <portType name="XDSRegistry_PortType">
    <operation name="RegistryStoredQuery">
      <input message="ihe:RegistryStoredQuery_Message"
          wsaw:Action="urn:ihe:iti:2007:RegistryStoredQuery"/>
      <output message="ihe:RegistryStoredQueryResponse_Message"
          wsaw:Action="urn:ihe:iti:2007:RegistryStoredQueryResponse"/>
    </operation>
    ...
  </portType>
  ...
</definitions>
```

A full WSDL for the Document Repository and Document Registry actors is found in Appendix W.

3.18.4.1.2.7.1 Sample SOAP Messages

4015   The samples in the following two sections show a typical SOAP request and its relative SOAP response. The sample messages also show the WS-Addressing headers <a:Action/>, <a:MessageID/>, <a:ReplyTo/>…; these WS-Addressing headers are populated according to the IHE Appendix V: Web Services for IHE Transactions. The body of the SOAP message is omitted for brevity; in a real scenario the empty element will be populated with the appropriate metadata.

4020   Samples presented in this section are also available online on the IHE FTP site, see Appendix W.

3.18.4.1.2.7.1.1 Sample Registry Stored Query SOAP Request

```xml
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">urn:ihe:iti:2007:RegistryStoredQuery</a:Action>
    <a:MessageID>urn:uuid:def119ad-dc13-49c1-a3c7-e3742531f9b3</a:MessageID>
    <a:ReplyTo s:mustUnderstand="1">>
```

```
          <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
        </a:ReplyTo>
4030    <a:To>http://localhost/service/IHEXDSRegistry.svc</a:To>
      </s:Header>
      <s:Body>
          <query:AdhocQueryRequest
                      xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
4035                  xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
                      xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0">
              <query:ResponseOption returnComposedObjects="true" returnType="LeafClass"/>
              <rim:AdhocQuery id=" urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d ">
                      <rim:Slot name="$XDSDocumentEntryPatientId">
4040                          <rim:ValueList>

          <rim:Value>'st3498702^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO'</rim:Value>
                              </rim:ValueList>
                      </rim:Slot>
4045                  <rim:Slot name="$XDSDocumentEntryStatus">
                              <rim:ValueList>
                                      <rim:Value>('urn:oasis:names:tc:ebxml-
regrep:ResponseStatusType:Approved')</rim:Value>
                              </rim:ValueList>
4050                  </rim:Slot>
                      <rim:Slot name="$XDSDocumentEntryCreationTimeFrom">
                              <rim:ValueList>
                                      <rim:Value>200412252300</rim:Value>
                              </rim:ValueList>
4055                  </rim:Slot>
                      <rim:Slot name="$XDSDocumentEntryCreationTimeTo">
                              <rim:ValueList>
                                      <rim:Value>200501010800</rim:Value>
                              </rim:ValueList>
4060                  </rim:Slot>
                      <rim:Slot name="$XDSDocumentEntryHealthcareFacilityTypeCode">
                              <rim:ValueList>
                                      <rim:Value>('Emergency Department')</rim:Value>
                              </rim:ValueList>
4065                  </rim:Slot>
              </rim:AdhocQuery>
          </query:AdhocQueryRequest>
      </s:Body>
    </s:Envelope>
```

4070 3.18.4.1.2.7.1.2 Sample Registry Stored Query SOAP Response

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">urn:ihe:iti:2007:RegistryStoredQueryResponse</a:Action>
4075    <a:RelatesTo>urn:uuid:def119ad-dc13-49c1-a3c7-e3742531f9b3</a:RelatesTo>
  </s:Header>
  <s:Body>
    <query:AdhocQueryResponse xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"/>
  </s:Body>
4080 </s:Envelope>
```

3.18.4.1.3 Expected Actions

The Document Registry actor shall

1. Accept a parameterized query in an AdhocQueryRequest message

4085   2. Verify the required parameters are included in the request. Additionally, special rules documented in the above section 'Parameters for Required Queries' shall be verified.

3. Errors shall be returned for the following conditions:
   - Unknown query ID (error code XDSUnknownStoredQuery)
   - Required parameter missing (error code XDSStoredQueryParamNumber)

4090 See section 4.1.13 Error Reporting for additional error codes and general information on formating error responses.

4. Retrieve the internal implementation template of the query based on the Query ID supplied in the query request. Substitute appropriate parameters as indicated in section 3.18.4.1.2.3.7 Parameters for Required Queries and execute the query.

4095
   - The Document Registry shall accept the homeCommunityId value if it is specified in a Registry Stored Query request.

5. Return XML formatted metadata in an AdhocQueryResponse message.
   - The Document Registry may specify the homeCommunityID attribute on any
4100 appropriate elements   The homeCommunityId attribute corresponds to the 'home' attribute specified in the ebRIM standard. For more information on homeCommunityId see Section 3.18.4.1.2.3.8 . The elements that may include the home attribute are:
   - If returntype="LeafClass" the ExtrinsicObject and RegistryPackage elements
4105 shall contain the home attribute.
   - If returnType="ObjectRef" the ObjectRef element shall contain the home attribute

4110 This transaction may return both errors and results in an AdhocQueryResponse message. To do this, the returned AdhocQueryResponse message would contain both a RegistryObjectList element and a RegistryErrorList element. See section 4.1.13 of the Technical Framework for additional details on formatting of error responses.

4115

3.18.4.1.3.1 Sample Query Request

This example query specifies:
- The FindDocuments query (id attribute of AdhocQuery element)
- patientID st3498702^^^&1.3.6.1.4.1.21367.2005.3.7&ISO
4120
- Return Approved documents only
- Time range (creation time) 200412252300 to 200501010800
- Healthcare Facility Type Code of Emergency Department

Note that ebRS 3.0 specifies the use of Slot to specify name/value(s) pairs as parameters to a Stored Query.

4125   Note: query parameter names are highlighted for readability.


```
<query:AdhocQueryRequest
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
   xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
   xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0">
  <query:ResponseOption returnComposedObjects="true" returnType="LeafClass"/>
  <rim:AdhocQuery id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d">
    <rim:Slot name="$XDSDocumentEntryPatientId">
      <rim:ValueList>
        <rim:Value>'st3498702^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO'</rim:Value>
      </rim:ValueList>
    </rim:Slot>
    <rim:Slot name="$XDSDocumentEntryStatus">
      <rim:ValueList>
        <rim:Value>('urn:oasis:names:tc:ebxml-regrep:StatusType:Approved')</rim:Value>
      </rim:ValueList>
    </rim:Slot>
    <rim:Slot name="$XDSDocumentEntryCreationTimeFrom">
      <rim:ValueList>
        <rim:Value>200412252300</rim:Value>
      </rim:ValueList>
    </rim:Slot>
    <rim:Slot name="$XDSDocumentEntryCreationTimeTo">
      <rim:ValueList>
        <rim:Value>200501010800</rim:Value>
      </rim:ValueList>
    </rim:Slot>
    <rim:Slot name="$XDSDocumentEntryHealthcareFacilityTypeCode">
      <rim:ValueList>
        <rim:Value>('Emergency Department')</rim:Value>
      </rim:ValueList>
    </rim:Slot>
  </rim:AdhocQuery>
</query:AdhocQueryRequest>
```

The following example shows a get documents query for XDSDocumentEntry objects for a specified list of entryUUIDs (urn:uuid:aff99222-18e3-4812-bc71-c410b2860e18, urn:uuid:aff99222-18e3-4812-bc71-c410b2860e19, urn:uuid:aff99222-18e3-4812-bc71-c410b2860e20) and corresponding homeCommunityId value (urn:oid:1.2.3):

4165

```
<query:AdhocQueryRequest … >
    <query:ResponseOption returnComposedObjects="true"
returnType="LeafClass"/>
    <rim:AdhocQuery id="urn:uuid:5c4f972b-d56b-40ac-a5fc-c8ca9b40b9d4"
home="urn:oid:1.2.3">
        <rim:Slot name="$XDSDocumentEntryEntryUUID">
            <rim:ValueList>
              <rim:Value>
              ("urn:uuid:aff99222-18e3-4812-bc71-c410b2860e18",
               "urn:uuid:aff99222-18e3-4812-bc71-c410b2860e19",
               "urn:uuid:aff99222-18e3-4812-bc71-c410b2860e20")
              </rim:Value>
            </rim:ValueList>
        </rim:Slot>
    </rim:AdhocQuery>
</query:AdhocQueryRequest>
```

3.18.4.1.3.2 Intentionally Left Blank

3.18.4.1.3.3 Sample Query Response

This sample query response corresponds to the above query. Note that the query response message is coded in version 3.0 ebRIM and ebRS. This sample response and the ebXML Registry version 3.0 schema files are available online. The Implementation Guide found at http://wiki.ihe.net/index.php?title=ITI_Implementation_Guide contains such supplemental material.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<AdhocQueryResponse
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0
      file:/Users/bill/RegSchema/V3.0/query.xsd"
    xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
    xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
  <rim:RegistryObjectList>
    <rim:ExtrinsicObject
        xmlns:q="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
        xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
        id="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
        isOpaque="false"
        mimeType="text/xml"
        objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
        status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved">
      <rim:Slot name="URI">
        <rim:ValueList>
          <rim:Value>http://localhost:8080/XDS/Repository/08a15a6f-5b4a-42de-8f95-
89474f83abdf.xml</rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="authorInstitution">
        <rim:ValueList>
          <rim:Value>Fairview Hospital</rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="creationTime">
        <rim:ValueList>
          <rim:Value>200412261119</rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="hash">
        <rim:ValueList>
          <rim:Value>4cf4f82d78b5e2aac35c31bca8cb79fe6bd6a41e</rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="languageCode">
        <rim:ValueList>
          <rim:Value>en-us</rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="serviceStartTime">
        <rim:ValueList>
          <rim:Value>200412230800</rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="serviceStopTime">
        <rim:ValueList>
          <rim:Value>200412230801</rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="size">
        <rim:ValueList>
          <rim:Value>54449</rim:Value>
        </rim:ValueList>
```

```
                  </rim:Slot>
                  <rim:Slot name="sourcePatientId">
4250                <rim:ValueList>
                      <rim:Value>jd12323^^^wsh</rim:Value>
                    </rim:ValueList>
                  </rim:Slot>
                  <rim:Slot name="sourcePatientInfo">
4255                <rim:ValueList>
                      <rim:Value>PID-3|pid1^^^domain</rim:Value>
                      <rim:Value>PID-5|Doe^John^^^</rim:Value>
                      <rim:Value>PID-7|19560527</rim:Value>
                      <rim:Value>PID-8|M</rim:Value>
4260                  <rim:Value>PID-11|100 Main St^^Metropolis^Il^44130^USA</rim:Value>
                    </rim:ValueList>
                  </rim:Slot>
                  <rim:Name>
                    <rim:LocalizedString charset="UTF-8" value="Sample document 1" xml:lang="en-us"/>
4265              </rim:Name>
                  <rim:Description/>
                  <rim:Classification
                    classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
                    classifiedObject="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
4270                id="urn:uuid:ac872fc0-1c6e-439f-84d1-f76770a0ccdf"
                    nodeRepresentation="Education"
                    objectType="Urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification">
                  <rim:Slot name="codingScheme">
                    <rim:ValueList>
4275                  <rim:Value>Connect-a-thon classCodes</rim:Value>
                    </rim:ValueList>
                  </rim:Slot>
                  <rim:Name>
                    <rim:LocalizedString charset="UTF-8" value="Education" xml:lang="en-us"/>
4280              </rim:Name>
                  <rim:Description/>
                </rim:Classification>
                <rim:Classification
                    classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"
4285              classifiedObject="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
                    id="urn:uuid:f1a8c8e4-3593-4777-b7e0-8b0773378705"
                    nodeRepresentation="C"
                    objectType="Urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification">
                  <rim:Slot name="codingScheme">
4290                <rim:ValueList>
                      <rim:Value>Connect-a-thon confidentialityCodes</rim:Value>
                    </rim:ValueList>
                  </rim:Slot>
                  <rim:Name>
4295                <rim:LocalizedString charset="UTF-8" value="Celebrity" xml:lang="en-us"/>
                  </rim:Name>
                  <rim:Description/>
                </rim:Classification>
                <rim:Classification
4300                classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d"
                    classifiedObject="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
                    id="urn:uuid:b6e49c73-96c8-4058-8c95-914d83bd262a"
                    nodeRepresentation="CDAR2/IHE 1.0"
                    objectType="Urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification">
4305              <rim:Slot name="codingScheme">
                    <rim:ValueList>
                      <rim:Value>Connect-a-thon formatCodes</rim:Value>
                    </rim:ValueList>
                  </rim:Slot>
4310              <rim:Name>
                    <rim:LocalizedString charset="UTF-8" value="CDAR2/IHE 1.0" xml:lang="en-us"/>
                  </rim:Name>
                  <rim:Description/>
                </rim:Classification>
4315            <rim:Classification
                    classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1"
                    classifiedObject="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
                    id="urn:uuid:61e2b376-d74a-4984-ac21-dcd0b8890f9d"
```

```
                       nodeRepresentation="Emergency Department"
4320                   objectType="Urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification">
                    <rim:Slot name="codingScheme">
                     <rim:ValueList>
                       <rim:Value>Connect-a-thon healthcareFacilityTypeCodes</rim:Value>
                     </rim:ValueList>
4325                </rim:Slot>
                    <rim:Name>
                     <rim:LocalizedString charset="UTF-8" value="Assisted Living" xml:lang="en-us"/>
                    </rim:Name>
                    <rim:Description/>
4330             </rim:Classification>
                    <rim:Classification
                       classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead"
                       classifiedObject="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
                       id="urn:uuid:fb7677c5-c42f-485d-9010-dce0f3cd4ad5"
4335                   nodeRepresentation="Cardiology"
                       objectType="Urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification">
                    <rim:Slot name="codingScheme">
                     <rim:ValueList>
                       <rim:Value>Connect-a-thon practiceSettingCodes</rim:Value>
4340                 </rim:ValueList>
                    </rim:Slot>
                    <rim:Name>
                     <rim:LocalizedString charset="UTF-8" value="Cardiology" xml:lang="en-us"/>
                    </rim:Name>
4345                <rim:Description/>
                 </rim:Classification>
                    <rim:Classification
                       classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983"
                       classifiedObject="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
4350                   id="urn:uuid:0a8a8ed9-8be5-4a63-9b68-a511adee8ed5"
                       nodeRepresentation="34098-4"
                       objectType="Urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification">
                    <rim:Slot name="codingScheme">
                     <rim:ValueList>
4355                   <rim:Value>LOINC</rim:Value>
                     </rim:ValueList>
                    </rim:Slot>
                    <rim:Name>
                     <rim:LocalizedString
4360                     charset="UTF-8"
                         value="Conference Evaluation Note" xml:lang="en-us"/>
                    </rim:Name>
                    <rim:Description/>
                 </rim:Classification>
4365             <rim:ExternalIdentifier
                       id="urn:uuid:db9f4438-ffff-435f-9d34-d76190728637"
                       registryObject="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
                       identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"
                       objectType="ExternalIdentifier"
4370                   value="st3498702^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO">
                    <rim:Name>
                     <rim:LocalizedString
                         charset="UTF-8"
                         value="XDSDocumentEntry.patientId"
4375                     xml:lang="en-us"/>
                    </rim:Name>
                    <rim:Description/>
                 </rim:ExternalIdentifier>
                    <rim:ExternalIdentifier
4380                   id="urn:uuid:c3fcbf0e-9765-4f5b-abaa-b37ac8ff05a5"
                       registryObject="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
                       identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
                       objectType="ExternalIdentifier"
                       value="1.3.6.1.4.1.21367.2005.3.99.1.1010">
4385                <rim:Name>
                     <rim:LocalizedString
                         charset="UTF-8"
                         value="XDSDocumentEntry.uniqueId"
                         xml:lang="en-us"/>
```

```
4390              </rim:Name>
              <rim:Description/>
          </rim:ExternalIdentifier>
        </rim:ExtrinsicObject>
        <rim:ObjectRef xmlns:q="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
4395   xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" id="urn:uuid:41a5887f-8865-4c09-adf7-
       e362475b143a"/>
          <rim:ObjectRef xmlns:q="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
       xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" id="urn:uuid:f4f85eac-e6cb-4883-b524-
       f2705394840f"/>
4400       <rim:ObjectRef xmlns:q="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
       xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" id="urn:uuid:a09d5840-386c-46f2-b5ad-
       9c3699a4309d"/>
          <rim:ObjectRef xmlns:q="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
       xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" id="urn:uuid:f33fb8ac-18af-42cc-ae0e-
4405   ed0b0bdb91e1"/>
          <rim:ObjectRef xmlns:q="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
       xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" id="urn:uuid:cccf5598-8b07-4b77-a05e-
       ae952c785ead"/>
          <rim:ObjectRef xmlns:q="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
4410   xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" id="urn:uuid:f0306f51-975f-434e-a61c-
       c59651d33983"/>
          <rim:ObjectRef xmlns:q="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
       xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" id="urn:uuid:58a6f841-87b3-4a3e-92fd-
       a8ffeff98427"/>
4415       <rim:ObjectRef xmlns:q="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
       xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" id="urn:uuid:2e82c1f6-a085-4c72-9da3-
       8640a32e42ab"/>
        </rim:RegistryObjectList>
       </AdhocQueryResponse>
```

4420   The following query response is the same as above (repeated sections replaced with …) with the
        homeCommunityId attribute specified, in bold for readability. Subsequent requests specifying
        entryUUID of `urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf` or uniqueID of
        `1.3.6.1.4.1.21367.2005.3.99.1.1010` shall include the homeCommunityId value of urn:oid:1.2.3 in
        the query.

4425
```
<?xml version="1.0" encoding="UTF-8"?>
<AdhocQueryResponse ... status="Success">
      <rim:RegistryObjectList>
         <rim:ExtrinsicObject … id="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
4430  isOpaque="false"  mimeType="text/xml" objectType="urn:uuid:7edca82f-054d-47f2-a032-
      9b2a5b5186c1" status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved"
      home="urn:oid:1.2.3">


      …
4435
              <rim:ExternalIdentifier id="urn:uuid:c3fcbf0e-9765-4f5b-abaa-
      b37ac8ff05a5" registryObject="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
      identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
      objectType="ExternalIdentifier" value="1.3.6.1.4.1.21367.2005.3.99.1.1010">
4440             <rim:Name>
                   <rim:LocalizedString charset="UTF-8"
      value="XDSDocumentEntry.uniqueId" xml:lang="en-us"/>
                </rim:Name>
                <rim:Description/>
4445          </rim:ExternalIdentifier>
          </rim:ExtrinsicObject>
        </rim:RegistryObjectList>
      </AdhocQueryResponse>
```

4450 **3.18.4.1.3.4 Intentionally Left Blank**

3.18.4.1.3.5 Basic Patient Privacy Enforcement Option

If the Basic Patient Privacy Enforcement Option is implemented:

1. All Document Consumer Actors may provide a list of confidentialityCode in XDS Registry Stored Query Transaction and the XDS Registry will return only document that have at least one
4455 matching confidentialityCode. In this way documents without at least one of the requested codes will not be returned.

2. The Document Consumer actor shall be able to be configured with the Patient Privacy Consent Policies, Patient Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the XDS Affinity Domain Policy. The details of this are product
4460 specific and not specified by IHE.

3. The Document Consumer shall not allow access to documents for which the Document Consumer does not understand at least one of the confidentialityCode returned. This assures that a Document Consumer will not improperly handle documents with confidentialityCode that may be more restrictive than the Document Consumer is configured to support.

4465 4. The Document Consumer actor shall abide by the XDS Affinity Domain Policies represented by the confidentialityCode in the metadata associated with the document. The Document Consumer actor likely will have user access controls or business rule capabilities to determine the details of how confidentiality codes apply to query results. The details of this are product specific and not specified by IHE. These rules shall reduce the query results to only those that are appropriate to
4470 the current situation for that actor and user.

5. Note: The Registry is already required to return only documents that match the requested confidentialityCode (filter) indicated in the Registry Stored Query.

6. Note: Products implementing the Registry Actor may be able to further filter Registry Stored Query results through looking at all the Patient Privacy Acknowledgement Documents registered
4475 for the patient that have the availabilityStatus of Approved and for which have not expired.

3.18.4.1.3.6 Basic Patient Privacy Proof Option

If the Basic Patient Privacy Consents Proof Option is implemented:

1. The Document Consumer actor shall be capable of querying for 'Approved' Patient Privacy Consent Acknowledgement Documents in the XDS Affinity Domain. This query should be done
4480 by document class so as to catch both formats of document (Consent). The Document Consumer actor shall be capable of recognizing the eventCodeList from the resulting XDS Metadata. There is no required handling of Patient Privacy Consent Acknowledgement Document XDS Metadata. There is no requirement for the Document Consumer to retrieve the Patient Privacy Consent Acknowledgement Document content.

4485 **3.18.5 Security Considerations**

Relevant XDS Affinity Domain Security background is discussed in the Register Document transaction (see ITI TF-2: 3.14.5.1).

3.18.5.1 Audit Record Considerations

The Registry Stored Query Transaction is a Query Information event as defined in table 3.20.6-1. The
4490   Actors involved shall record audit events according to the following:

3.18.5.1.1 Document Consumer audit message:

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110112, DCM, "Query")
	EventActionCode	M	"E" (Execute)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-18", "IHE Transactions", "Registry Stored Query")
Source (Document Consumer) (1)			
Human Requestor (0..n)			
Destination (Document Registry) (1)			
Audit Source (Document Consumer) (1)			
Patient (0..1)			
Query Parameters(1)			

Where:

Source **AuditMessage/** **ActiveParticipant**	UserID	C	When WS-Addressing is used: <ReplyTo/>
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human Requestor (if known) **AuditMessage/** **ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

Destination **AuditMessage/** **ActiveParticipant**	UserID	M	SOAP endpoint URI.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source	AuditSourceID	U	Not specialized.
AuditMessage/ AuditSourceIdentification	AuditEnterpriseSiteID	U	not specialized
	AuditSourceTypeCode	U	not specialized

4495

Patient	ParticipantObjectTypeCode	M	"1" (Person)
(AudittMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
Query Parameters	ParticipantObjectTypeCode	M	"2" (system object)
(AudittMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV("ITI-18", "IHE Transactions", "Registry Stored Query")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	Stored Query ID (UUID)
	ParticipantObjectName	C	If known the value of <ihe:HomeCommunityId/>
	ParticipantObjectQuery	M	the AdhocQueryRequest, base64 encoded.
	ParticipantObjectDetail	U	not specialized

3.18.5.1.2 Document Registry audit message:

	Field Name	**Opt**	**Value Constraints**
Event	EventID	M	EV(110112, DCM, "Query")
AuditMessage/ EventIdentification	EventActionCode	M	"E" (Execute)
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	EV("ITI-18", "IHE Transactions", "Registry Stored Query")
Source (Document Consumer) (1)			
Destination (Document Registry) (1)			
Audit Source (Document Registry) (1)			
Patient (0..1)			
Query Parameters(1)			

Where:

Source	UserID	C	When WS-Addressing is used: <ReplyTo/>
AuditMessage/ ActiveParticipant	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

	UserID	M	SOAP endpoint URI.

	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	U	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source	*AuditSourceID*	U	*Not specialized.*
AuditMessage/ AuditSourceIdentification	*AuditEnterpriseSiteID*	U	*not specialized*
	AuditSourceTypeCode	U	*not specialized*

4500

Patient	ParticipantObjectTypeCode	M	"1" (Person)
(AudittMessage/ ParticipantObjectIdenti fication)	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	U	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	U	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	U	*not specialized*
	ParticipantObjectQuery	U	*not specialized*
	ParticipantObjectDetail	U	*not specialized*
Query Parameters	ParticipantObjectTypeCode	M	"2" (system object)
(AudittMessage/ ParticipantObjectIdenti fication)	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	U	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ITI-18", "IHE Transactions", "Registry Stored Query")
	ParticipantObjectSensitivity	U	*not specialized*
	ParticipantObjectID	M	Stored Query ID (UUID)
	ParticipantObjectName	C	If known the value of <ihe:HomeCommunityId/>
	ParticipantObjectQuery	M	the AdhocQueryRequest, base64 encoded.
	ParticipantObjectDetail	U	*not specialized*

3.19 Authenticate Node

This section corresponds to Transaction 19 of the IHE ITI Technical Framework. Transaction 19 is used by the Secure Node actors

4505 **3.19.1 Scope**

In the Authenticate Node transaction, the local Secure Node presents its identity to a remote Secure Node, and authenticates the identity of the remote node. After this mutual authentication other secure transactions may take place through this secure pipe between the two nodes.

In addition, the Secure Node authenticates the identity of the user who requests access to the node. This
4510 user authentication is a local operation that does not involve communication with a remote node.

3.19.2 Use Case Roles
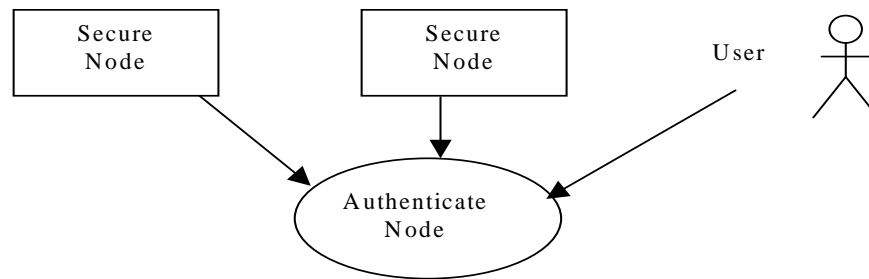
Actor: Secure Node

Role: Establish a protocol specific trust relationship between two nodes in a network. Establishes the
4515 identity of a user, and authorizes access to the patient data and applications at the node.

Actor: User

Role: Someone who wants to have access to the data and applications available at the node.

3.19.3 Referenced Standards

4520 DICOM 2003 PS 3.15:
Security Profiles. Annex B1: The Basic TLS Secure Transport Connection profile.

IETF: Transport Layer Security (TLS) 1.0 (RFC 2246)

ITU-T: Recommendation X.509 (03/00). "Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks"

4525 **3.19.4 Interaction Diagram**

Note: This diagram does not imply sequencing of Authentication Node and Local User Authentication.

Local
Secure Node

Remote
Secure Node

Authenticate Node

Authenticate Node

Local User Authentication
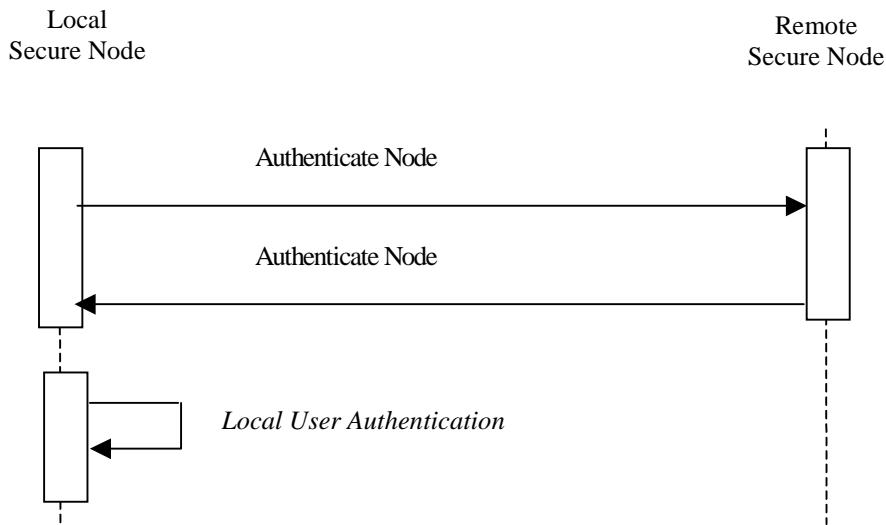
3.19.5 Trigger Events

The Local Secure Node starts the authentication process with the Remote Secure Node when
information exchange between the two nodes is requested. The first transaction shall be the Authenticate
Node transaction, and all other PHI transactions performed by IHE actors shall be secure transactions.
This authentication process is needed when a secure connection is established.

The Basic Secure Node shall always apply the Authenticate Node process to every DICOM, HTTP, or
HL7 connection.

3.19.6 Message Semantics

The Authenticate node transaction involves the exchange of certificates representing the identities of the
nodes. These identities are used to authenticate the nodes, to inform authorization, and audit logging.

3.19.6.1 Certificate Validation

The local organization (e.g., XDS Affinity Domain) will make the choice of what mixture of chain of
trust and direct comparison is used to authenticate communications. This may be entirely based on
chaining trust to selected CAs, entirely based upon provision of node certificates for direct comparison,
or a mixture of both.

> Note: The CAs used for ATNA chain of trust will be different than the default browser trusted list of CAs used for authenticating
> internet web servers. A worldwide CA, such as Verisign, is not generally trusted to determine which individual nodes
> within an organization should and should not communicate patient identifiable information.

When Authenticating the Remote Secure Node, the Local Secure Node:

- Shall be able to perform certificate validation based on signature by a trusted CA (See 3.19.6.1.1)
  and

- Shall be able to perform direct certificate validation to a set of trusted certificates (See 3.19.6.1.2)

It may reject communications when the certificate validation fails, or may restrict communications to only that which is appropriate for an unidentified other party.

3.19.6.1.1   Chain to a trusted certificate authority

4555   The Secure Node or Secure Application:

- Shall provide the means for configuring which CAs are trusted to authenticate node certificates for use in a chain of trust. These CAs shall be identified by means of the public signing certificate for the signing CA.

- Shall support digital certificates encoded using both Deterministic Encoding Rules (DER) and Basic
4560   Encoding Rules (BER).

- Shall accept communications for which there is a certificate that is signed by a CA that is listed as a trusted signing authority.

3.19.6.1.2   Direct certificate validation

4565   The Secure Node or Secure Application:

- Shall provide means for installing of the required certificates, for example, via removable media or network interchange (where the set of trusted certificates can be a mixture of CA signed certificates and self-signed certificates).

- Shall support digital certificates encoded using both Deterministic Encoding Rules (DER) and Basic
4570   Encoding Rules (BER).

- Shall accept communications for which there is a certificate configured as acceptable for direct certificate validation.

3.19.6.1.3   Other Certificate requirements

4575   The Secure Node shall not require any specific certificate attribute contents, nor shall it reject certificates that contain unknown attributes or other parameters. Note that for node certificates the CN often is a hostname, attempting to use this hostname provides no additional security and will introduce a new failure mode (e.g., DNS failure).

4580   The certificates used for mutual authentication shall be X509 certificates based on RSA key with key length in the range of 1024-4096, where the key length chosen is based on local site policy. Maximum expiration time acceptable for certificates should be defined in the applicable security policy. The IHE Technical Framework recommends a maximum expiration time of 2 years.

4585   The method used to determine of the authenticated nodes, which ones are authorized to communicate is not specified. This may be a dual use of the set of trusted certificates, some attribute in the certificates,

access control lists, or some other method. Using a certificate chain back to an external trusted certificate authority to determine authorizations is strongly discouraged.

4590 **3.19.6.2 DICOM and HL7 Connections**

HL7 and DICOM transactions are required to adhere to the specifications in this section.

When configured for use on a physically secured network, the normal DICOM and HL7 connection mechanisms shall be used.

When configured for use not on a physically secured network implementations shall use the TLS
4595 protocol, and the following cyphersuite shall be supported:

TLS_RSA_WITH_NULL_SHA

If the ATNA Encryption Option is implemented, the following cyphersuite shall also be supported:

TLS_RSA_WITH_AES_128_CBC_SHA.

The recommended "well-known port 2762" as specified by DICOM shall be used when the Secure node
4600 is configured for use not on a physically secured network. When the secure node is configured for use on a physically secured network, a different port number shall be used, preferably the standard port 104. HL7 does not specify port numbers, but the port number used when configured for use on a physically secured network shall be different than the port number used when configured for use not on a physically secured network.

4605 All Secure Nodes shall be configurable for use on a physically secured network or not on a physically secured network. If Secure Node is configured for physical security, then it may use the non-TLS DICOM port and protocol.

3.19.6.3 HTTP Connections

3.19.6.3.1 Expected Actions

4610 The HTTP connection shall be made using a TLS connection in the same manner as HL7 and DICOM TLS connections described above, although the port number shall be configurable.

HTTP communications shall require the encryption-option.

> Note: IHE permits DICOM and HL7 connections to use encryption none because these connections are often internal to the organization, protected by other security mechanisms, and in the case of DICOM convey very large quantitites of data. The
4615 mandatory imposition of additional encryption on that traffic has significant performance impact. HTTP communications are much less voluminous, and many existing browser implementations do not support encryption none.

If Secure Node is configured for physical security, then it shall use the normal HTTP protocol.

3.19.6.4 Web-Services

4620 **3.19.6.4.1 Expected Actions**

A trusted association shall be established between the two nodes utilizing WS-I Basic Security Profile Version 1.1. This association will be used for all secure transactions between the IHE actors in the two

nodes. Note that IHE ITI Volume 2 section 3.19.6.2 "HTTP Connections" and WS-I Basic Security Profile – section 3 "Transport Layer Mechanisms" (i.e. http://ws-i.org/profiles/basic-security/1.1/transport) are identical and interoperable.

3.19.7 Local User Authentication

The Secure Node starts the authentication process with a User when the User wants to log on to the node. The secure node shall not allow access to PHI to an operator who has not successfully completed the local user authentication. Local user authentication is not an IHE specified network transaction, although it may utilize a network system for user authentication.

This is a local invocation of functions at the Secure Node. The identity of the User will be established by the Secure Node actor based on methods such as:

- Username with Password
- Biometrics
- Smart card
- Magnetic Card

The User shall log in using his or her own unique individually assigned identity. Identities must be unique across the secure domain. A user may have more than one identity. The Secure Node shall be configurable to maintain a list of authorized users for the Secure Node.

The rules for assignment of unique individual identities to users is part of the Security Policy of the healthcare enterprise. Development of these rules is outside the scope of the IHE Technical Framework. The following examples list a few special cases related to user identification that may occur in practice.

3.19.7.1 Example: Team approach

When the operator is part of a team performing a procedure, the other members of the team involved in creating and accessing the data should be manually identified and recorded in the procedure log (which may be paper or electronic), and it is assumed that all have accessed the data even though they were not (and cannot be in most cases) actually logged on to the piece of equipment.

During some procedures, it may be necessary for one operator to relieve the operator who has already been authenticated by the system. It is recommended that the first operator log off and that the system authenticate the new operator.

The audit log supports identification of the active participant. This is often defined as one key member of the team. Other means are used to track the entry and exit of various members of the team. IHE does not specify any specific team identification process.

3.19.7.2 Example: Access to locked exam room, no user logon on modality.

There may be situations where the acquisition modality has no user logon features, and access to the equipment is controlled by controlling access to the examination room. In these situations an equipment-specific user ID will be used, and access to the room should be recorded in the procedure log (which may be paper or electronic).

4660 ### 3.19.7.3 Example: Enterprise User Authentication

The healthcare enterprise may implement local user authentication using the Enterprise User Authentication Profile (EUA). This implementation may be mixed with other non-EUA access to the secure domain, based upon each node's internal use an EUA availability.

3.20 Record Audit Event

4665   This section corresponds to Transaction 20 of the IHE ITI Technical Framework. Transaction 20 is used by the all IHE actors that support the Audit Trail and Node Authentication Integration Profile to communicate with the Audit Record Repository actors.

3.20.1 Scope

In the Record Audit Event transaction, the IHE actor creates an entry in the Audit Log at the Audit
4670   Record Repository.

3.20.2 Use Case Roles
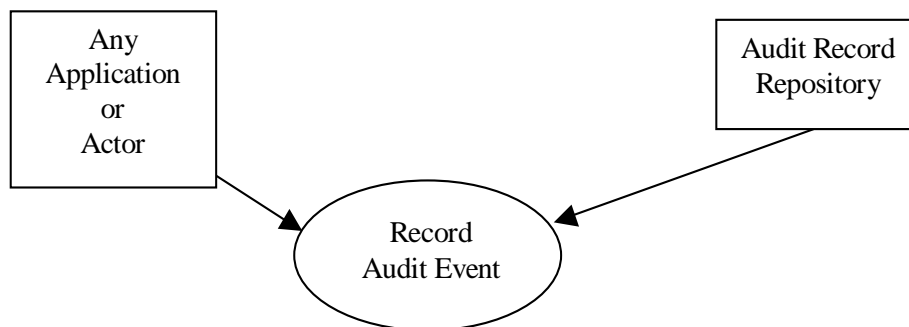
Application or Actor: Any actor or any other application that is grouped with the Secure Node Actor.

Role: Create an audit record and transmit this record to the Audit Record Repository.

4675   **Actor:** Audit Record Repository

Role: Receive an audit record from the Audit Record Creator and store this for audit purposes.

3.20.3 Referenced Standards

IETF:	The BSD Syslog Protocol. (RFC 3164);
	Reliable Delivery for Syslog (RFC 3195);
4680	Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications (RFC 3881).
DICOM:	Supplement 95
ASTM:	E2147-01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems.
4685 **NIST:**	SP 800-92 Guide to Computer Security Log Management.
W3C:	Recommendation: Extensible Markup Language (XML) 1.0

3.20.4 Interaction Diagram
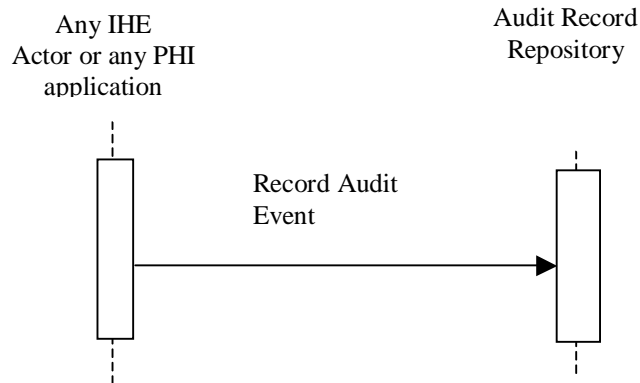
3.20.5 Record Audit Event

4690   The Audit Record Repository shall accept the Audit Record message. The usage of the result by the Audit Record Repository is beyond the scope of the IHE Technical Framework.

3.20.6 Trigger Events and Message semantics

An Audit Log is a record of actions performed on data by users. Actions are queries, views, additions, deletions and changes. The IHE actor creates an Audit Record when an IHE transaction-related event
4695   occurs or when a non-transaction event occurs.

IHE specifies that events defined in Table 3.20.6-1 shall be reportable by means of the IHE Audit Trail. Radiology devices may also find that their subset of events is reportable by means of the IHE Provisional Audit Message Format. This is not recommended other than as a strategy for managing the upgrade of products and systems to the DICOM Audit Message Standard with IHE Extensions.

4700

Table 3.20.6-1. Audit Record trigger events

Trigger Event	Description	Source Vocabulary
Actor-start-stop	Startup and shutdown of any actor. Applies to all actors. Is distinct from hardware powerup and shutdown.	DICOM (Sup 95) "Application Activity"
Audit-Log-Used	The audit trail repository has been accessed or modified by something other than the arrival of audit trail messages.	DICOM (Sup 95) "Audit Log Used"
Begin-storing-instances	Begin storing SOP Instances for a study. This may be a mix of instances.	DICOM (Sup 95) "Begin Transferring DICOM Instances"
Health-service-event	Health services scheduled and performed within an instance or episode of care. This includes scheduling, initiation, updates or amendments, performing or completing the act, and cancellation. See note below.	IHE Extension (section 3.20.7.3) "Health Services Provision Event"
Instances-deleted	SOP Instances are deleted from a specific study. One event covers all instances deleted for the particular study.	DICOM (Sup 95) "DICOM Instances Accessed" or "DICOM Study Deleted"
Instances-Stored	Instances for a particular study have been stored on this system. One event covers all instances stored for the	DICOM (Sup 95) "DICOM

Trigger Event	Description	Source Vocabulary
	particular study.	Instances Transferred"
Medication	Medication orders and administration within an instance or episode of care. This includes initial order, dispensing, delivery, and cancellation. See note below.	IHE Extension (section 3.20.7.3) "Medication Event"
Mobile-machine-event	Mobile machine joins or leaves secure domain.	DICOM (Sup 95) "Network Entry"
Node-Authentication-failure	A secure node authentication failure has occurred during TLS negotiation, e.g. invalid certificate.	DICOM (Sup 95) "Security Alert"
Order-record-event	Order record created, accessed, modified or deleted. Involved actors: Order Placer. This includes initial order, updates or amendments, delivery, completion, and cancellation. See note below.	DICOM (Sup 95) "Order Record"
Patient-care-assignment	Staffing or participant assignment actions relevant to the assignment of healthcare professionals, caregivers attending physician, residents, medical students, consultants, etc. to a patient It also includes change in assigned role or authorization, e.g., relative to healthcare status change, and de-assignment	IHE Extension (section 3.20.7.3) "Patient Care Resource Assignment"
Patient-care-episode	Specific patient care episodes or problems that occur within an instance of care. This includes initial assignment, updates or amendments, resolution, completion, and cancellation. See note below.	IHE Extension (section 3.20.7.3) "Patient Care Episode"
Patient-care-protocol	Patient association with a care protocol. This includes initial assignment, scheduling, updates or amendments, completion, and cancellation. See note below.	IHE Extension (section 3.20.7.3) "Patient Care Protocol"
Patient-record-event	Patient record created, modified, or accessed.	DICOM (Sup 95) "Patient Record"
PHI-export	Any export of PHI on media, either removable physical media such as CD-ROM or electronic transfer of files such as email. Any printing activity, paper or film, local or remote, that prints PHI.	DICOM (Sup 95) "Export"
PHI-import	Any import of PHI on media, either removable physical media such as CD-ROM or electronic transfers of files such as email.	DICOM (Sup 95) "Import"
Procedure-record-event	Procedure record created, modified, accessed or deleted.	DICOM (Sup 95) "Procedure Record"
Query Information	A query has been received, either as part of an IHE transaction, or as part other products functions. For example: 1) Modality Worklist Query 2) Instance or Image Availability Query 3) PIX, PDQ, or XDS Query Notes: The general guideance is to log the query event with the query parameters and not the result of the query. The result of a query may be very large and is likely to be of limited value vs the overhead. The query parameters can be used effectively to detect bad behavior and the expectation is that given the query parameters the result could be regenerated if necessary.	DICOM (Sup 95) "Query"

Trigger Event	Description	Source Vocabulary
Security Alert	Security Administrative actions create, modify, delete, query, and display the following: 1. Configuration and other changes, e.g., software updates that affect any software that processes protected information. Hardware changes may also be reported in this event. 2. Security attributes and auditable events for the application functions used for patient management, clinical processes, registry of business objects and methods (**e.g. WSDL, UDDI**), program creation and maintenance, etc. 3. Security domains according to various organizational categories such as entity-wide, institutional, departmental, etc. 4. Security categories or groupings for functions and data such as patient management, nursing, clinical, etc. 5. The allowable access permissions associated with functions and data, such as create, read, update, delete, and execution of specific functional units or object access or manipulation methods. 6. Security roles according to various task-grouping categories such as security administration, admissions desk, nurses, physicians, clinical specialists, etc. It also includes the association of permissions with roles for role-based access control. 7. User accounts. This includes assigning or changing password or other authentication data. It also includes the association of roles with users for role-based access control, or permissions with users for user-based access control. 8. Unauthorized user attempt to use security administration functions. 9. Audit enabling and disabling. 10. User authentication revocation. 11. Emergency Mode Access (aka Break-Glass) Security administration events should always be audited.	DICOM (Sup 95) "Security Alert"
User Authentication	This message describes the event of a user attempting to log on or log off, whether successful or not. No Participant Objects are needed for this message.	DICOM (Sup 95) "User Authentication"
Study-Object-Event	Study is created, modified, accessed, or deleted. This reports on addition of new instances to existing studies as well as creation of new studies.	DICOM (Sup 95) "DICOM Instances Accessed"
Study-used	SOP Instances from a specific study are created, modified or accessed. One event covers all instances used for the particular study.	DICOM (Sup 95) "DICOM Instances Accessed"

Note: The IHE extension has reduced the scope of many of the IETF events to remove phrases like "checking for clinical contra-indications". This is done to highlight that the events should be reported are those that are related to the access, use, creation, and distribution of PHI. This audit log is not intended to be a general purpose monitoring system to track all kinds of medical activity. As a result, many clinically significant events will not be separately reported.

4705

3.20.6.1 Audit Record Transportation

This profile defines two transport mechanisms for the audit messages:

1. (Future) Transport utilizing the Reliable Syslog protocol in "cooked" mode as defined in RFC-3195, subject to such changes as result from current IETF activity.4

4710

2. Transport utilizing the BSD Syslog protocol defined in RFC-3164.

The Audit repository shall support both transport mechanisms for the receipt of messages. Individual IHE Actors may choose to utilize either of the two transport mechanisms, unless they also comply with another Profile that further restricts the use. IHE recommends the use of reliable syslog because it deals with issues such as delivery confirmation, message loss prevention, and message truncation prevention.

4715 The Reliable Syslog protocol specifies the use of local cache and storage. Messages are preserved locally until they are confirmed to have been successfully stored at the recipient. After delivery they may be removed at the convenience of the local machine and local functions.

3.20.6.2 Audit Record format

The IHE defines several audit record formats, and future profiles may define more message formats. An
4720 IHE actor shall utilize one or more of these audit record formats. All audit record formats utilize XML encoding and are defined by XML schema.

The present list of audit record schema are:

1. The IHE Audit Trail format. This is a schema based on the standards developed and issued by the IETF, HL7, and DICOM organizations to meet the medical auditing needs as specified by
4725 ASTM.

2. IHE Provisional Audit Record format, defined below. This was previously defined as part of the IHE Radiology technical framework. Its use is deprecated, this implies that no extensions will be made and new applications should use the new IHE Audit Trail format.

3.20.6.3   Audit Message Transports

4730 The IHE actor will create the Audit Record and transmit this to the Audit Record Repository as soon as possible. When for some reason the Audit Record repository is not available, the IHE actor shall store the Audit Record in a local buffer until the Audit Record Repository is available again. The local Audit Record at the IHE actor may be deleted when this record has been transmitted to the Audit Record Repository.

4735   Note: The Reliable Syslog protocol has explicit support for management of occasionally connected and mobile devices.

---

4   The Reliable Syslog implementation in the field has progressed very slowly. The IHE is waiting for the outcome of ongoing IETF activities. These may result in confirming the original IETF decision to promulgate Reliable Syslog "cooked", may result in modifications to that protocol, or may result in its replacement. IHE implementations may chose to proceed with this protocol to establish evidence for the IETF that it does perform as needed, but should be aware that it may be changed.

3.20.6.3.1   Reliable Syslog

The Reliable Syslog "cooked" mode defined in RFC-3195 shall be used to transport the audit messages. The schema used for the messages shall be identified as part of the "cooked" connection establishment.

3.20.6.3.2   BSD Syslog

The BSD syslog is appropriate in some situations, it was defined in the IHE Rad Technical Framework, and it is widely used legacy protocol. The XML messages are permitted to violate the BSD limitations in the following ways:

- The syslog port number shall be configurable, with the BSD port number (514) as the default.

- Messages are limited in length to 32768 bytes. Note that the underlying transport might not accept messages longer than 1024. They may be truncated. The Audit Repository must be prepared for arbitrary truncation of messages. The IHE Provisional schema uses shortened names to reduce the size of messages, but some may exceed 1024 bytes. When these are truncated the resulting XML will be incorrect and will need to be corrected by the Audit Repository to close the truncated portions of the message.

- The XML may contain Unicode characters that are encoded using the UTF-8 encoding rules. UTF-8 avoids utilizing the control characters that are mandated by the syslog protocol, but it may appear to be gibberish to a system that is not prepared for UTF-8. Audit repositories must accept UTF-8 encodings and store them without damage, e.g. preserve all 8 bits.

- The MSG portion of the syslog packet shall only contain the audit XML message. The TAG portion shall not be included in the message.

- The MSG shall be in 'minimal length' UTF-8.

- The XML message contained in the MSG portion of the syslog packet shall not begin with a unicode BOM (byte order mark).

The PRI field shall be set using the facility value of 10 (security/authorization messages). Most messages should have the severity value of 5 (normal but significant), although applications may choose values of 4 (Warning condition) if that is appropriate to the more detailed information in the audit message.   This means that for most audit messages the PRI field will contain the value "<85>". Audit repositories shall be prepared to deal appropriately with any incoming PRI value.

3.20.7 Audit Message Formats

3.20.7.1 RFC-3881 format

A common XML schema was defined based upon joint work by IHE, HL7, DICOM, ASTM E31, and the Joint NEMA/COCIR/JIRA Security and Privacy Committee. The IHE IT Infrastructure technical framework prefers use of this schema for audit records generated by all IHE actors.   The schema can be found at: `http://www.xml.org/xml/schema/7f0d86bd/healthcare-security-audit.xsd`

The DICOM Standard, Supplement 95 Audit Trail Messages provides vocabulary and further specification of the use of these schema elements for events that may occur in the context of DICOM

___

equipment. IHE has evaluated this and determined that it is more broadly applicable, and extended it for more general healthcare use.

For reference, the schema elements are diagrammed below. The diagrams are read from left to right:
4780   elements to the right are part of the lefthandside element.

 Required single element. A NetworkEntry element consists of exactly one MachineAction element.

 Optional single element. A NetworkEntry element consists of zero or one MachineAction element.

4785   Optional multiple elements. A NetworkEntry element consists of zero or any number of MachineAction elements.

 Selections of one out of several elements. A user consists either of a LocalUser element or of a RemoteNode element.

 Compound element: The "+" in an element box means that the element consists of
4790   further elements. If these expansion elements have not occurred up to this point in the document, can be expected to follow below in the document.

element AuditMessage

4795   element AuditMessage/EventIdentification
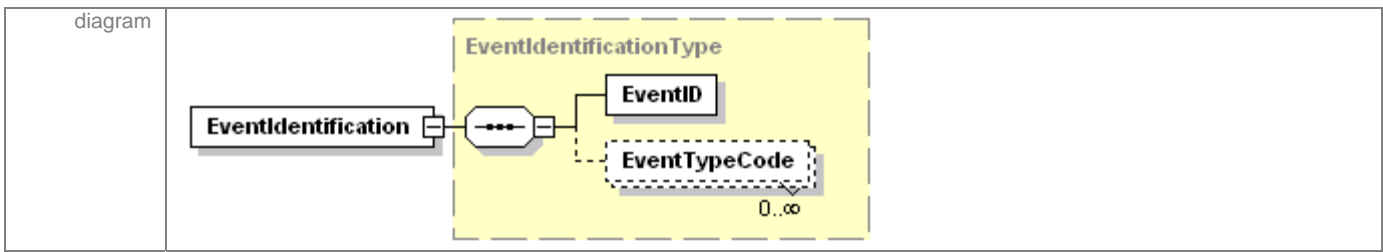
element AuditMessage/ActiveParticipant
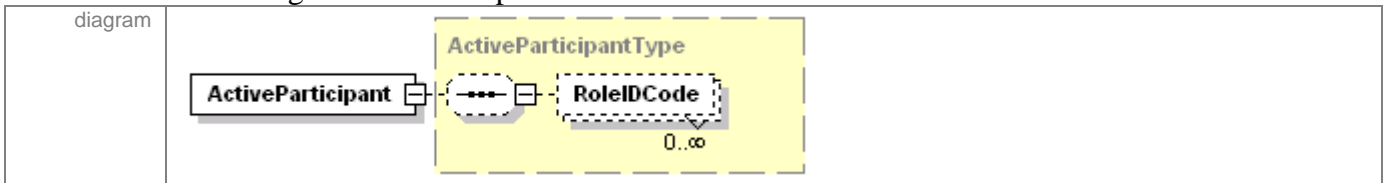
element AuditMessage/AuditSourceIdentification
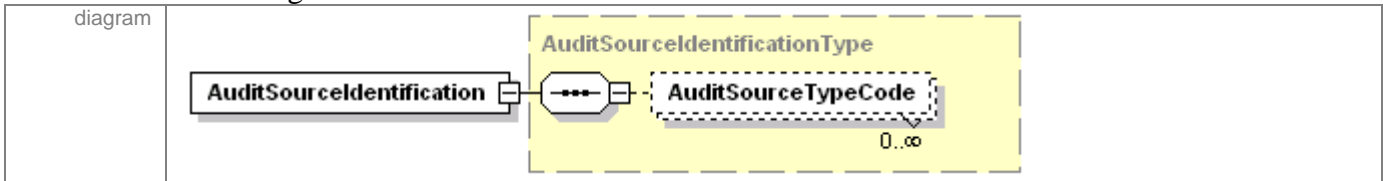
4800

element AuditMessage/ParticipantObjectIdentification
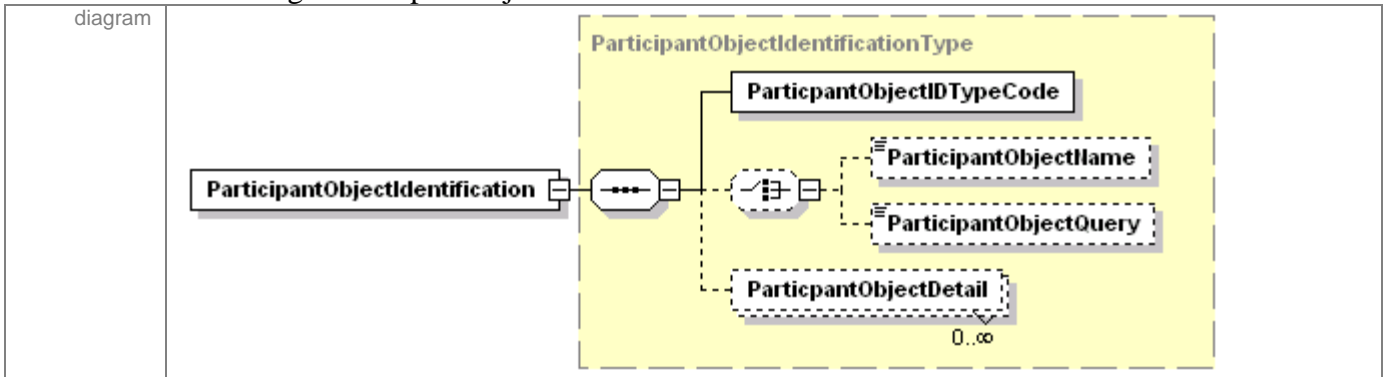
Note: ParticipantObjectDetail should not include unnecessary detail such as duplication of the attributes otherwise encoded in the audit message.

4805

3.20.7.2 DICOM Audit Trail

A Secure Node actor shall be able to detect events that are defined by the DICOM standard in Supplement 95, and generate Record Audit Event transactions that conform to the DICOM standard when these events take place.

4810 The DICOM Standard provides a schema for the basic messages and states that extensions are valid. This profile does not restrict private extensions that comply with the W3C XML encoding rules for the use of schemas, namespaces, etc.

3.20.7.3 IHE Audit Trail

The DICOM standard and RFC-3881 do not address all the kinds of security and privacy events that can
4815 take place in the healthcare environment. The additional IHE defined events enumerated in section 3.20.7.5 shall be used for their defined purpose.

The notation used in these tables is that used in the DICOM standard. The messages shall be encoded as instances based on the RFC-3881 schema. In cases where there is an event that applies to more than one patient, there shall be a separate audit message for each patient..

4820

3.20.7.4 Other event reports

Events that do not correspond to DICOM events or IHE Extension events can be reported. They shall comply with RFC-3881. Neither ATNA profile, DICOM, nor RFC-3881 restrict private extensions to
4825 the RFC-3881 schema however any private extensions shall comply with the W3C XML encoding rules for the use of schemas, namespaces, etc.

3.20.7.5 Controlled Terminology for IHE Extensions

This profile defines the following controlled terminology for use in the IHE extensions.

Context ID ccc1
4830 **Audit Event ID**
Type: Extensible   Version: 2004xxxx

Coding Scheme Designator	Coding Scheme Version	Code Value	Code Meaning
IHE		IHE0001	Health Services Provision Event
IHE		IHE0002	Medication Event
IHE		IHE0003	Patient Care ResourceAssignment
IHE		IHE0004	Patient Care Episode
IHE		IHE0005	Patient Care Protocol

IHE Code Definitions (Coding Scheme Designator "IHE" Coding Scheme Version "2004")

Code Value	Code Meaning	Definition	Notes
IHE0001	Health Services Provision Event	Health services scheduled and performed within an instance or episode of care. This includes scheduling, initiation, updates or amendments, performing or completing the act, and cancellation.	
IHE0002	Medication Event	Medication orders and administration within an instance or episode of care. This includes initial order,dispensing, delivery, and cancellation.	
IHE0003	Patient Care Resource Assignment	Staffing or participant assignment actions relevant to the assignment of healthcare professionals, caregivers attending physician, residents, medical students, consultants, etc. to a patient It also includes change in assigned role or authorization, e.g., relative to healthcare status change, and de-assignment	
IHE0004	Patient Care Episode	Specific patient care episodes or problems that occur within an instance of care. This includes initial assignment, updates or amendments, resolution, completion, and cancellation.	
IHE0005	Patient Care Protocol	Patient association with a care protocol. This includes initial assignment, scheduling, updates or amendments, completion, and cancellation.	

4835 ### 3.20.7.6 IHE Provisional Audit Message Form

A provisional XML Schema was defined for the contents of the audit records generated by the IHE actors in the deprecated Basic Security Integration Profile as part of the IHE Radiology domain. The ATNA profile includes this schema as an alternative format for audit messages. It is less flexible than the IHE Audit Trail format, and is no longer the recommended format for IHE use. The preferred
4840 format is the IHE Audit Trail format with extensions that is described above.

However, the IHE Provisional Audit Message format is suitable for many diagnostic equipment settings and can be transformed into an equivalent IHE Audit Trail format. It is also installed and in use at many locations. So the IHE Provisional Audit Message format is part of the IHE IT profile. The transition from its format to the IHE Audit Trail format is encouraged to reduce the burden on Audit Repositories
4845 which may result from processing this alternative format.

A provisional XML Schema has been defined for the contents of the audit records generated by the IHE actors in the Basic Security Integration Profile from the radiology technical framework. The audit records are used to generate an audit record log for activities related to protected health information.

The IHE Provisional Audit Message Schema is described in ITI TF-2: Appendix F.

4850

3.20.7.7 RoleIDCode with access control roles

RoleIDCode is a CodedValueType. When describing a human users participation in an event, this value should represent the access control roles/permissions that authorized the event/trans. Use of standards based roles/permissions is preferable to site or application specific. As RFC-3881 indicates Many security systems are unable to produce this data, hence it is optional.

4855

For example: at a site "St Fraser" they have defined a functional role code "NURSEA" for attending nurse. This can be represented as

    EV("NURSEA", "St Fraser", "Attending Nurse")

4860

Candidate standards based structual/functional role codes can be found at ISO, HL7, ASTM, and various other sources.

3.21 Patient Demographics Query

4865   This section corresponds to Transaction ITI-21 of the IHE Technical Framework. Transaction ITI-21 is used by the Patient Demographics Consumer and Patient Demographics Supplier actors.

3.21.1 Scope

This transaction involves a request by the Patient Demographics Consumer Actor for information about patients whose demographic data match data provided in the query message. The request is received by
4870   the Patient Demographics Supplier Actor. The Patient Demographics Supplier Actor immediately processes the request and returns a response in the form of demographic information for matching patients.

3.21.2 Use Case Roles
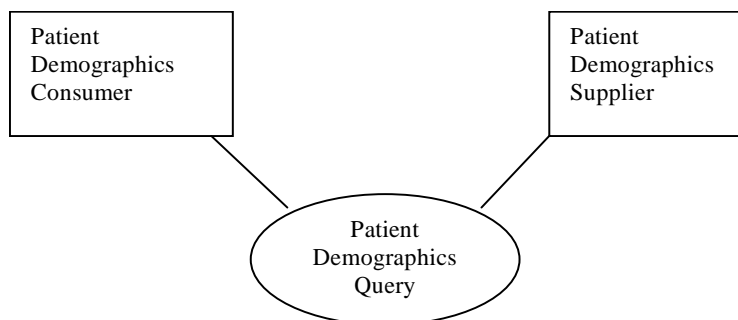
4875   **Actor:** Patient Demographics Consumer

Role: Requests a list of patients matching a minimal set of demographic criteria (*e.g.*, ID or partial name) from the Patient Demographics Supplier. Populates its attributes with demographic information received from the Patient Demographics Supplier.

Actor: Patient Demographics Supplier

4880   **Role:** Returns demographic information for all patients matching the demographic criteria provided by the Patient Demographics Consumer.

3.21.3 Referenced Standards

HL7:   Version 2.5, Chapter 2 – Control

4885   Version 2.5, Chapter 3 – Patient Administration

Version 2.5, Chapter 5 – Query

3.21.4 Interaction Diagram
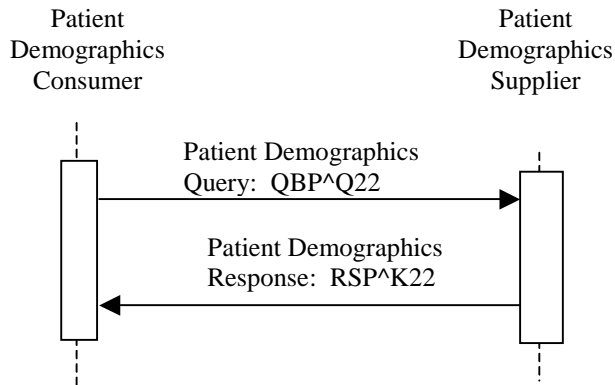
3.21.4.1 Patient Demographics Query

4890 **3.21.4.1.1 Trigger Events**

A Patient Demographics Consumer's need to select a patient based on demographic information about patients whose information matches a minimal set of known data will trigger the Patient Demographics Query based on the following HL7 trigger event:

Q22 – Find Candidates

4895 **3.21.4.1.2 Message Semantics**

The Patient Demographics Query is conducted by the HL7 QBP^Q22 message. The Patient Demographics Consumer actor shall generate the query message whenever it needs to select from a list of patients whose information matches a minimal set of demographic data. The segments of the message listed below are required, and their detailed descriptions are provided in the following

4900 subsections.

Table 3.21-1 QBP Query by Parameter

QBP	Query by Parameter	Chapter in HL7 2.5
MSH	Message Header	2
QPD	Query Parameter Definition	5
RCP	Response Control Parameter	5
[DSC]	Continuation Pointer	2

The receiver shall respond to the query by sending the RSP^K22 message. This satisfies the requirements of original mode acknowledgment; no intermediate ACK message is to be sent.

4905 Each Patient Demographics Query request specifies two distinct concepts. The Patient Demographics Query is always targeted at a single source of patient demographic information (referred to in this Transaction as the *patient information source*). A Patient Demographics Supplier may have knowledge of more than one source of demographics. A Patient Demographics Supplier shall support at least one source of patient demographics and may support multiple sources of demographics. Section 3.21.4.1.2.1

4910 describes how the the Patient Demographics Consumer specifies which source of demographics are

_____

requested by the query. Each query response shall return demographics from a single patient information source.

4915 The second concept present in the query is the set of patient identifier domains referenced by the query. These patient identifier domains may or may not be associated with the patient information source. A Patient Demographics Supplier shall support at least one patient identifier domain and may support multiple identifier domains. Section 3.21.4.1.2.2 describes how the Patient Demographics Consumer requests identifiers from one or more patient identifier domains. Query responses may return patient identifiers from 0, 1 or multiple patient identifier domains.

4920

3.21.4.1.2.1 MSH Segment

The MSH segment shall be constructed as defined in the "Message Control" section (ITI TF-2: Appendix C.1.2).

The Patient Demographics Supplier is able to obtain demographics from at least one and possibly
4925 multiple patient information sources. When more than one patient information source is available, Field *MSH-5-Receiving Application* specifies the patient information source that this query is targeting. The Patient Demographics Supplier shall return this value in *MSH-3-Sending Application* of the RSP^K22 response. The value specified in MSH-5 is not related to the value requested in QPD-8 What Domains Returned.

4930 A list shall be published of all Receiving Applications that the Patient Demographics Supplier supports, for the Patient Demographics Consumer to choose from. Each query is processed against one and only one source of patient demographic information.

Field *MSH-9-Message Type* shall have at least two components. The first component shall have a value of **QBP**; the second component shall have a value of **Q22**. The third component is optional; however, if
4935 present, it shall have a value of **QBP_Q21**.

3.21.4.1.2.2 QPD Segment

The Patient Demographics Consumer Actor shall send attributes within the QPD segment as described in Table 3.21-2.

Table 3.21-2. IHE Profile - QPD segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	250	CE	R	0471	01375	Message Query Name
2	32	ST	R+		00696	Query Tag
3		QIP	R			Demographics Fields
8		CX	O			What Domains Returned

4940 Adapted from the HL7 standard, version 2.5

The Consumer shall specify "IHE PDQ Query" for QPD-1 Message Query Name.

3.21.4.1.2.2.1 Populating QPD-3-Demographics Fields

Field *QPD-3-Demographics Fields* consists of one or more repetitions, each of which contains two components that together contain the name and value of a distinct parameter to the query. Acceptable segments are PID and PD1.

The first component of each parameter contains the name of an HL7 element in the form

@<seg>.<field no>.<component no>.<subcomponent no>

The above format is populated according to common HL7 usage for specifying elements used in query parameters, as follows:

<seg> represents a 3-character segment ID from the HL7 Standard.

<field no> is the number of a field within the segment as shown in the SEQ column of the segment attribute table for the segment selected.

<component no>, for fields whose data types contain multiple components, shall contain the cardinal number of the component being valued. For fields whose data types do not contain multiple components, <component no> shall not be valued and its preceding period shall not appear.

<subcomponent no>, for components whose data types contain multiple subcomponents, shall contain the cardinal number of the subcomponent being valued. For components whose data types do not contain multiple subcomponents, <subcomponent no> shall not be valued and its preceding period shall not appear.

The second subcomponent of each parameter contains the value that is to be matched. If it is desired to constrain the quality of a match within the bounds of an algorithm known to the Supplier, the algorithm and constraint values may be specified in Fields QPD-4 through QPD-7.

The Patient Demographics Consumer may specify, and the Patient Demographics Supplier shall support, the fields in the following table.

The Patient Demographics Supplier shall return demographic records that reflect the best fit to all of the search criteria.

Table 3.21-3. PDQ Profile – QPD-3 fields required to be supported

FLD	ELEMENT NAME
PID.3	Patient Identifier List
PID.5	Patient Name
PID.7	Date/Time of Birth
PID.8	Administrative Sex
PID.11	Patient Address
PID.18	Patient Account Number

An example of parameter expressions in QPD-3:

```
@PID.5.1.1^SMITH~@PID.8^F
```

requests all patients whose family name (first subcomponent (data type ST) of the first component (data type FN) of PID-5-Patient Name (data type XPN)) matches the value 'SMITH' and whose sex (PID-8-Sex (data type IS)) matches the value 'female'.

3.21.4.1.2.2.2 Populating QPD-8-What Domains Returned

As is specified in the discussion of the Find Candidates (Q22) Query in Chapter 3 of the HL7 Standard, field QPD-8 restricts the set of domains for which identifiers are returned in PID-3:

1. In a multiple-domain environment, QPD-8 may be used to identify one or more domains of interest to the Patient Demographics Consumer and from which the Consumer wishes to obtain a value for *PID-3-Patient Identifier*. Note that the patient information source designated by MSH-5 may or may not be associated with any of the Patient ID Domains listed in *QPD-8-What Domains Returned*.

   If QPD-8 is empty, the Patient Demographics Supplier shall return all Patient IDs known by the Patient Demographics Supplier for each patient that matches the search criteria. See Case 1 in Section 3.21.4.2.2.8 for details on how this information is returned.

   If QPD-8 is specified and the domains are recognized, the Patient Demographics Supplier shall return the Patient IDs for each patient that matches the search criteria. See Case 2 in Section 3.21.4.2.2.8 for details on how this information is returned.

   Any domain not recognized by the Patient Demographics Supplier is an error condition. See Case 3 in Section 3.21.4.2.2.8 how to handle this condition.

2. In a single-domain environment, QPD-8 may be ignored by the Patient Demographics Supplier. The Supplier shall always return the identifier from the Patient ID Domain known by the Patient Demographics Supplier.

Within field QPD-8, only component 4 (Assigning Authority) shall be valued.

The Patient Demographics Supplier may or may not be able to supply additional identifiers from the domains specified in QPD-8. A discussion of how QPD-8 is processed is included in the architectural discussion in the "Using Patient Data Query (PDQ) in a Multi-Domain Environment" section (ITI TF-2: Appendix M).

The Patient Demographics Consumer shall be able to support at least one of the following mechanisms for specifying QPD-8:

1. Transmit an empty value and receive all identifiers in all domains known by the Patient Demographics Supplier (one or more domains), or

2. Transmit a single value and receive zero or more identifiers in a single domain, or

3. Transmit multiple values and receive mutiple identifiers in those multiple domains.

3.21.4.1.2.3 RCP Segment

The Patient Demographics Consumer Actor shall send attributes within the RCP segment as described in Table 3.21-5. Fields not listed are optional and may be ignored.

Table 3.21-5. IHE Profile - RCP segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	1	ID	R	0091	00027	Query Priority
2	10	CQ	O	0126	00031	Quantity Limited Request

Adapted from the HL7 standard, version 2.5

3.21.4.1.2.3.1 Populating RCP-1-Query Priority

Field *RCP-1-Query Priority* shall always contain **I**, signifying that the response to the query is to be returned in Immediate mode.

3.21.4.1.2.3.2 Populating RCP-2-Quantity Limited Request

The Patient Demographics Consumer Actor may request that responses to the query be sent, using the HL7 Continuation Protocol, in increments of a specified number of patient records. (In the context of the HL7 query, a patient record is defined as the PID segment and any segments accompanying it for each patient.) It is desirable to request an incremental response if the query could result in hundreds or thousands of matches or "hits."

The Patient Demographics Supplier Actor shall support the HL7 Continuation Protocol.

Field RCP-2 is of data type CQ, which contains two components. The first component contains the number of increments, always expressed as an integer greater than 0, while the second component contains the kind of increment, always RD to signify that incremental replies are specified in terms of records.

For example, 50RD requests 50 records at a time.

See the "Incremental Response Processing" section (ITI TF-2: 3.21.4.1.3.3) and the "Expected Actions" section of the Patient Demographics Query Response message (ITI TF-2: 3.21.4.2.3) for more information on the implementation of the continuation protocol.

3.21.4.1.2.4 DSC Segment

The Patient Demographics Consumer Actor may request additional increments of data by specifying this segment on the query request. This segment should be omitted on the initial query request. Its purpose is to request additional increments of the data from the Patient Demographic Supplier Actor.

Table 3.21-9. IHE Profile - DSC segment

SEQ	LEN	DT	OPT	TBL#	ITEM #	ELEMENT NAME
1	180	ST	O		00014	Continuation Pointer
2	1	ID	O	0398	01354	Continuation Style

3.21.4.1.2.4.1 Populating DSC-1 Continuation Pointer

To request additional increments of data, DSC-1 (Continuation Pointer) shall echo the value from RSP^K22 DSC-1.

3.21.4.1.2.4.2 Populating DSC-2 Continuation Style

5045 DSC-2 (Continuation Style) shall always contain I, signifying that this is part of an interactive continuation message.

3.21.4.1.3 Expected Actions

3.21.4.1.3.1 Immediate Acknowledgement

5050 The Patient Demographics Supplier shall immediately return an RSP^K22 response message as specified below in Section 3.21.4.2, "Patient Demographics Response." The RSP^K22 response message incorporates original mode application acknowledgment as specified in the "Acknowledgment Modes" section (ITI TF-2: C.1.3). The Supplier shall use *MSH-3-Sending Application* of the RSP^K22 to return the value it received from the Patient Demographics Consumer in Field *MSH-5-Receiving*
5055 *Application* of the QBP^Q22 message.

3.21.4.1.3.2 Query Parameter Processing

The Patient Demographics Supplier Actor shall be capable of accepting, searching on, and responding with attributes in the QPD segment as specified in Table 3.21-2.

The Patient Demographics Supplier Actor must be capable of receiving all valid combinations of
5060 subcomponents that make up the Assigning Authority component (*i.e.*, all valid combinations of QPD-3.8).

Handling of phonetic issues, alternate spellings, upper and lower case, wildcards, accented characters, etc., if deemed appropriate, is to be supported by the Patient Demographics Supplier rather than by the Patient Demographics Consumer. The Supplier shall return at least all exact matches to the query
5065 parameters sent by the Consumer; IHE does not further specify matching requirements.

3.21.4.1.3.3 Incremental Response Processing

The Patient Demographics Supplier Actor shall be capable of accepting and processing attributes in the RCP segment as listed in Table 3.21-5. In particular, the Patient Demographics Supplier Actor shall respond in immediate mode (as specified by a *RCP-1-Query Priority* value of **I**).

5070 Also, the Patient Demographics Supplier Actor shall be able to interpret *RCP-2-Quantity Limited Request* to return successive responses of partial lists of records according to the HL7 Continuation Protocol, as described in Section 3.21.4.2 below and in the HL7 Standard.

3.21.4.2 Patient Demographics Response

3.21.4.2.1 Trigger Events

The Patient Demographics Supplier's response to the Find Candidates message shall be the following message:

K22 – Find Candidates response

3.21.4.2.2 Message Semantics

The Patient Demographics Response is conducted by the RSP^K22 message. The Patient Demographics Supplier Actor shall generate this message in direct response to the QBP^Q22 message previously received. This message satisfies the Application Level, Original Mode Acknowledgement for the HL7 QBP^Q22 message.

The segments of the message listed without enclosing square brackets in the Table below are required. Detailed descriptions of all segments listed in the table below are provided in the following subsections. Other segments of the message are optional.

Table 3.21-6 RSP Segment Pattern Response

RSP	Segment Pattern Response	Chapter in HL7 2.5
MSH	Message Header	2
MSA	Message Acknowledgement	2
[{ERR}]	Error	2
QAK	Query Acknowledgement	5
QPD	Query Parameter Definition	5
[{ PID	Patient Identification	3
[PD1]		
[QRI] }]	Query Response Instance	5
[DSC]	Continuation Pointer	2

3.21.4.2.2.1 MSH Segment

The MSH segment shall be constructed as defined in the "Message Control" section (ITI TF-2: C.1.2).

Field *MSH-3-Sending Application* specifies the patient information source that processed the query. The Patient Demographics Supplier shall use Field *MSH-3-Sending Application* of the RSP^K22 message to return the value it received from the Patient Demographics Consumer in Field *MSH-5-Receiving Application* of the QBP^Q22 message.

Field *MSH-9-Message Type* shall have at least two components. The first component shall have a value of **RSP**; the second component shall have a value of **K22**. The third component is optional; however, if present, it shall have a value of **RSP_K22**.

3.21.4.2.2.2 MSA Segment

5100 The Patient Demographics Supplier Actor is not required to send any attributes within the MSA segment beyond what is specified in the HL7 standard. See the "Acknowledgment Modes" section (ITI TF-2: C.1.3) for the list of all required and optional fields within the MSA segment.

3.21.4.2.2.3 QAK Segment

The Patient Demographics Supplier Actor shall send attributes within the QAK segment as defined in 5105 table 3.21-7. For the details on filling in QAK-2 (Query Response Status) refer to the "Patient Demographics Supplier Actor Query Response Behavior" section (ITI TF-2: 3.21.4.2.2.8).

QAK-1 (Query Tag) shall echo the same value of QPD-2 (Query Tag) of the QBP^Q22 message, to allow the Patient Demographics Query Consumer to match the response to the corresponding query request.

5110

Table 3.21-7. PDQ Profile - QAK segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	32	ST	R		00696	Query Tag
2	2	ID	R+	0208	00708	Query Response Status

Adapted from the HL7 standard, version 2.5

3.21.4.2.2.4 QPD Segment

5115 The Patient Demographics Supplier Actor shall echo the QPD Segment value that was sent in the QBP^Q22 message.

3.21.4.2.2.5 PID Segment

The Patient Demographics Supplier Actor shall return one PID segment group (*i.e.*, one PID segment plus any segments associated with it in the message syntax shown in Table 3.21-5) for each matching 5120 patient record found. The Supplier shall return the attributes within the PID segment as specified in Table 3.21-8. In addition, the Patient Demographics Supplier Actor shall return all other attributes within the PID segment for which it is able to supply values.

Table 3.21-8. PDQ Profile - PID segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
3	250	CX	R		00106	Patient Identifier List
5	250	XPN	R		00108	Patient Name
7	26	TS	R2		00110	Date/Time of Birth
8	1	IS	R2	0001	00111	Administrative Sex
11	250	XAD	R2		00114	Patient Address
18	250	CX	R2		00121	Patient Account Number

5125 Adapted from the HL7 standard, version 2.5

The Patient Demographics Supplier may or may not be able to supply additional identifiers from the domains specified in QPD-8. Inability to supply an identifier in a particular domain is not an error, provided that the domain is recognized.

The PID segment and its associated PD1 and QRI segments are returned only when the Patient Demographics Supplier Actor is able to associate the search information in QPD-3 with one or more patient records in the patient information source associated with *MSH-5-Receiving Application*. See the "Patient Demographics Supplier Actor Query Response Behavior" section (ITI TF-2: 3.21.4.2.2.8) for a detailed description of how the Patient Demographics Supplier Actor responds to the query request under various circumstances.

3.21.4.2.2.6 QRI Segment

For each patient for which the Patient Demographics Supplier Actor returns a PID Segment, it may optionally return the QRI (Query Response Instance) segment, but is not required to do so. Refer to the HL7 Standard, Version 2.5, Chapter 5, Section 5.5.5, for more information.

3.21.4.2.2.7 DSC Segment

If the number of records is specified in *RCP-2-Quantity Limited Request*, the Patient Demographics Supplier Actor shall return an incremental response of that number of records when the number of matching records it finds exceeds the number of records specified in RCP-2.

As long as the Patient Demographics Supplier Actor has records to return in addition to those returned in the incremental response, the Supplier shall return a DSC Segment. The single field of the DSC Segment shall contain a unique alphanumeric value (the Continuation Pointer) that the Patient Demographics Consumer may return in the DSC of the QBP^Q22 message to request the next increment of responses. The Supplier shall return increments as many times as the Consumer requests them (and there are increments to return), and shall stop when the Consumer sends a cancel query (QCN^J01) message (or when there are no more increments to return).

3.21.4.2.2.8 Patient Demographics Supplier Actor Query Response Behavior

The Patient Demographics Supplier shall perform the matching of patient data based on the query parameter values it receives. The information provided by the Patient Demographics Supplier Actor to Patient Demographics Consumer Actors is a list of possible matching patients from the patient information source associated with the value that the Consumer sent in *MSH-5-Receiving Application* of the query message.

If domains are specified in *QPD-8-What Domains Returned* and are recognized by the Patient Demographics Supplier, the response will also, for each patient, contain any Patient ID values found in the specified domains.

The mechanics of the matching algorithms used are internal to the Patient Demographics Supplier Actor and are outside of the scope of this framework.

The Patient Demographics Supplier Actor shall respond to the query request as described by the following 3 cases:

Case 1: The Patient Demographics Supplier Actor finds (in the patient information source associated with *MSH-5-Receiving Application*) at least one patient record matching the criteria sent in *QPD-3-Demographics Fields*. No patient identifier domains are requested in *QPD-8-What Domains Returned*.

AA (application accept) is returned in MSA-1.

OK (data found, no errors) is returned in QAK-2.

One PID segment group (*i.e.*, one PID segment plus any segments associated with it in the message syntax shown in Table 3.21-5) is returned from the patient information source for each patient record found. If the Patient Demographics Supplier Actor returns data for multiple patients, it shall return these data in successive occurrences of the PID segment group.

Within each PID segment, field *PID-3-Patient Identifier List* contains one or more identifiers from the set of Patient ID Domains known by the Patient Demograpics Supplier.

If an incremental number of records are specified in *RCP-2-Quantity Limited Request*, and the number of records to be sent exceeds that incremental number, the Supplier returns only the incremental number of records, followed by a DSC segment containing a uniquely valued Continuation Pointer.

The consumer will specify the value of the continuation pointer in the DSC segment on the subsequent query request to request the next increment of responses.

Case 2: The Patient Demographics Supplier Actor finds (in the patient information source associated with *MSH-5-Receiving Application*) at least one patient record matching the criteria sent in *QPD-3-Demographics Fields*. One or more patient identifier domains are requested in *QPD-8-What Domains Returned*; the Supplier recognizes all the requested domains.

AA (application accept) is returned in MSA-1.

OK (data found, no errors) is returned in QAK-2.

One PID segment group (*i.e.*, one PID segment plus any segments associated with it in the message syntax shown in Table 3.21-5) is returned for each matching patient record found. If the Patient Demographics Supplier Actor returns data for multiple patients, it shall return these data in successive occurrences of the PID segment group.

Within each PID segment, field *PID-3-Patient Identifier List* contains, in successive occurrences delimited by the repetition separator, the identifiers from all the Patient ID Domains requested in QPD-8. In each occurrence of PID-3, component 4 contains the assigning authority value for one Patient ID Domain, and component 1 contains the Patient ID value in that domain. If an identifier does not exist for a domain that was specified on QPD-8, nothing is returned in the list.

If an incremental number of records is specified in *RCP-2-Quantity Limited Request*, and the number of records to be sent exceeds that incremental number, the Supplier returns only the incremental number of records, followed by a DSC segment containing a uniquely valued Continuation Pointer.

The consumer will specify the value of the continuation pointer in the DSC segment on the subsequent query request to request the next increment of responses.

Case 3: The Patient Demographics Supplier Actor does not recognize one or more of the domains in *QPD-8-What Domains Returned*.

AE (application error) is returned in MSA-1 and in QAK-2.

For each domain that was not recognized, an ERR segment is returned in which the components of *ERR-2-Error Location* are valued as follows.

5205

COMP #	COMPONENT NAME	VALUE
1	Segment ID	**QPD**
2	Sequence	**1**
3	Field Position	**8**
4	Field Repetition	*(see below)*
5	Component Number	*(empty)*
6	Subcomponent Number	*(empty)*

ERR-2.4-Field Repetition identifies the ordinal occurrence of QPD-8 that contained the unrecognized domain. As specified by HL7, *ERR-2.5-Component Number* and *ERR-2.6-Subcomponent Number* are not valued because we are referring to the entire field QPD-8.

ERR-3-HL7 Error Code is populated with the error condition code **204** (unknown key identifier).
5210 Together with the values in ERR-2, this signifies that the Patient Demographics Supplier Actor did not recognize the domain for *QPD-8-What Domains Returned*.

3.21.4.2.3 Expected Actions

The Patient Demographics Consumer will use the demographic information provided by the Patient Demographics Supplier to perform the functions for which it requested the information, *e.g.*, providing a
5215 pick list to the user.

If the Supplier has sent a DSC segment containing a continuation pointer value, additional increments of data are available upon request by the Consumer. After receiving each increment of data that includes a
5220 DSC segment containing a continuation pointer value, the Consumer should take one of the following actions.

- If the Consumer wishes to receive another increment of the data, the Consumer reissues the query message using a new unique value in *MSH-10-message control ID* and adding the DSC segment after the RCP segment. DSC-1 shall echo the continuation pointer returned in RSP^K22
5225   DSC-1 segment.

- If the Consumer does not wish to receive another increment of the data, the Consumer issues a cancel query (QCN^J01) message. The consumer shall echo the query tag from QAK-1 in QID-1 and the query message name from QPD-1 in QID-2.

- If the Consumer does not reissue the query or send a cancel query message, the query will
5230   eventually terminate.

If the Supplier has not sent a DSC segment containing a continuation pointer value, no more increments of data are available and no further action by the Consumer is required.

3.21.4.3 Canceling a query

5235 The Patient Demographic Consumer can send a cancel trigger to notify the Patient Demographic Supplier that no more incremental responses will be requested, and the interactive query can be terminated. This cancellation trigger is optional. How long the Patient Demographic Supplier retains query results (for incremental response) is an implementation decision and therefore beyond the scope of IHE.

5240

3.21.4.3.1   Trigger Events

The Patient Demographic Consumer which received a RSP^K22 response message indicating there are more incremental responses data available, can terminate the interactive query with the following HL7 trigger event:

5245

J01 – Cancel query status

3.21.4.3.2   Message Semantics

Canceling a query is conducted by the QCN^J01 message. The Patient Demographic Consumer can
5250 generate this message to notify the Patient Demographic Supplier that no more data is desired. The segments of the message listed below are required, and their details descriptions are provided in the following subsections.

Table 3.21.10 QCN Cancel query

QCN	Cancel query	Chapter in HL7 2.5
MSH	Message Header	2
QID	Query identification Segment	5

5255

The receiver shall acknowledge this cancel by the HL7 ACK message. See Appendix C.1.3, "Acknowledgement Modes", for definition and discussion of the ACK message.

3.21.4.3.2.1 MSH Segment

5260

The MSH segment shall be constructed as defined in the "Message Control" section (ITI TF-2: Appendix C.1.2).

MSH-9 (Message Type) shall have three components. The first component shall have the value of QCN;
5265 the second component shall have a value of J01. The third component shall have the value of QCN_J01.

3.21.4.3.2.2 QID Segment

The QID segment contains the information necessary to uniquely identify the query being cancelled.
5270

Table 3.21-9. IHE Profile - QID segment

SEQ	LEN	DT	OPT	TBL #	ITEM #	ELEMENT NAME
1	32	ST	R		00696	Query Tag
2	250	CE	R	0471	01375	Message Query Name

5275 **3.21.4.3.2.2.1   Populating QID-1 Query Tag**

QID-1 (Query Tag) uniquely identifies the query to be canceled. This field shall contain the same value specified in QPD-2.

5280 **3.21.4.3.2.2.2   Populating QID-2 Message Query Name**

QID-2 (Message Query Name) identifies the name of the query. It is an identifier of the conformance statement for this query. This field shall contain the same value specified in QPD-1.

5285 **3.21.5 Security Considerations**

3.21.5.1 Audit Record Considerations

The Patient Demographics Query Transaction is a Query Information event as defined in table 3.20.6-1. The Actors involved shall record audit events according to the following:

3.21.5.1.1   Patient Demographics Consumer audit message:

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110112, DCM, "Query")
	EventActionCode	M	"E" (Execute)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-21", "IHE Transactions", "Patient Demographics Query")
Source (Patient Demograhics Consumer) (1)			
Human Requestor (0..n)			
Destination (Patient Demographics Supplier) (1)			
Audit Source (Patient Demographics Consumer) (1)			
Patient (0..n)			
Query Parameters(1)			

5290 Where:

Source **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Demographics Consumer Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human Requestor (if known) **AuditMessage/** **ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

Destination **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Demographics Source facility and receiving application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source **AuditMessage/** **AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Patient **(AudittMessage/** **ParticipantObjectIdentifi** **cation)**	ParticipantObjectTypeCode	M	"1" (Person)
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
	ParticipantObjectTypeCode	M	"2" (system object)
	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ITI-21", "IHE Transactions", "Patient Demographics Query")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	*U*	*not specialized*

	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	the QPD segment of the query - Base64 encoded
	ParticipantObjectDetail	M	MSH-10 - the message identifier

5295 **3.21.5.1.2   Patient Demographics Source audit message:**

	Field Name	**Opt**	**Value Constraints**
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110112, DCM, "Query")
	EventActionCode	M	"E" (Execute)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-21", "IHE Transactions", "Patient Demographics Query")
Source (Patient Demographics Consumer) (1)			
Destination (Patient Demographics Supplier) (1)			
Audit Source (Patient Demographics Supplier) (1)			
Patient (0..n)			
Query Parameters(1)			

Where:

Source **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Demographics Consumer Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Destination **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Demographics Supplier facility and receiving application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source **AuditMessage/** **AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

	ParticipantObjectTypeCode	M	"1" (Person)

	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
Query Parameters (AudittMessage/ ParticipantObjectIdentifi cation)	ParticipantObjectTypeCode	M	"2" (system object)
	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ITI-21", "IHE Transactions", "Patient Demographics Query")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	*U*	*not specialized*
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	the QPD segment of the query - Base64 encoded
	ParticipantObjectDetail	M	MSH-10 - the message identifier

5300

3.22 Patient Demographics and Visit Query

This section corresponds to Transaction ITI-22 of the IHE Technical Framework. Transaction ITI-22 is used by the Patient Demographics Consumer and Patient Demographics Supplier actors.

3.22.1 Scope

5305   This transaction involves a request by the Patient Demographics Consumer Actor for information about patients whose demographic and visit data match data provided in the query message. The request is received by the Patient Demographics Supplier actor. The Patient Demographics Supplier actor immediately processes the request and returns a response in the form of demographic and visit information for matching patients.

5310   ### 3.22.2 Use Case Roles
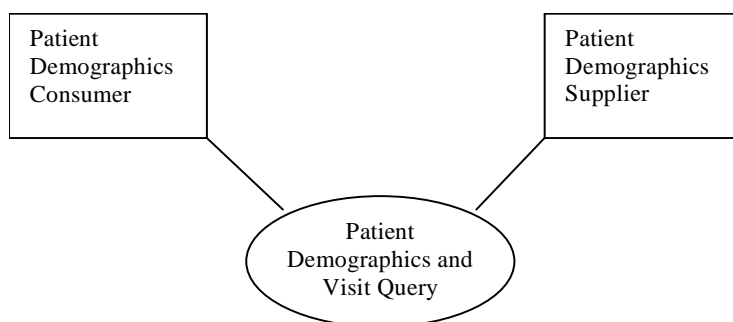
Actor: Patient Demographics Consumer

Role: Requests a list of patients matching a minimal set of demographic (*e.g.*, ID or partial name) and visit criteria from the Patient Demographics Supplier. Populates its attributes with demographic and

5315   visit information received from the Patient Demographics Supplier.

Actor: Patient Demographics Supplier

Role: Returns demographic and visit information for all patients matching the demographic and visit criteria provided by the Patient Demographics Consumer.

5320   ### 3.22.3 Referenced Standards

HL7:   Version 2.5, Chapter 2 – Control

Version 2.5, Chapter 3 – Patient Administration

Version 2.5, Chapter 5 – Query

3.22.4 Interaction Diagram

5325
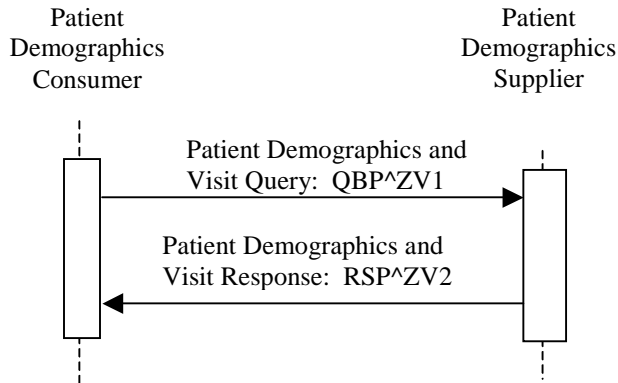
3.22.4.1 Patient Demographics and Visit Query

3.22.4.1.1   Trigger Events

A Patient Demographics Consumer's need to select a patient based on demographic and visit
information about patients whose information matches a minimal set of known data will trigger the
Patient Demographics and Visit Query based on the following HL7 trigger event:

ZV1 – Find Candidates from Visit Information

3.22.4.1.2   Message Semantics

The Patient Demographics and Visit Query transaction is conducted by the HL7 QBP^ZV1 message.
The Patient Demographics Consumer actor shall generate the query message whenever it needs to select
from a list of patients whose information matches a minimal set of demographic and visit data. The
segments of the message listed below are required, and their detailed descriptions are provided in the
following subsections.

Table 3.22-1. QBP Query by Parameter

QBP	Query by Parameter	Chapter in HL7 2.5
MSH	Message Header	2
QPD	Query Parameter Definition	5
RCP	Response Control Parameter	5
[DSC]	Continuation Pointer	2

The receiver shall respond to the query by sending the RSP^ZV2 message. This satisfies the
requirements of original mode acknowledgment; no intermediate ACK message is to be sent.

Each Patient Demographics and Visit Query request specifies two distinct concepts. The Patient
Demographics and Visit Query is always targeted at a single source of patient demographic information
(referred to in this Transaction as the ***patient information source***). A Patient Demographics Supplier
may have knowledge of more than one source of demographics. A Patient Demographics Supplier shall
support at least one source of patient demographics and may support multiple sources of demographics.
Section 3.21.4.1.2.1 describes how the the Patient Demographics Consumer specifies which source of
demographics are requested by the query. Each query response shall return demographics from a single
patient information source.

The second concept present in the query is the set of patient identifier domains referenced by the query. These patient identifier domains may or may not be associated with the patient information source. A Patient Demographics Supplier shall support at least one patient identifier domain and may support multiple identifier domains. Section 3.21.4.1.2.2 describes how the Patient Demographics Consumer requests identifiers from one or more patient identifier domains. Query responses may return patient identifiers from 0, 1 or multiple patient identifier domains.

3.22.4.1.2.1 MSH Segment

5360   The MSH segment shall be constructed as defined in the "Message Control" section (ITI TF-2: C.1.2).

The Patient Demographics Supplier is able to obtain demographics from at least one and possibly multiple patient information sources. When more than one patient information source is available, Field *MSH-5-Receiving Application* specifies the patient information source that this query is targeting. The Patient Demographics Supplier shall return this value in *MSH-3-Sending Application* of the RSP^ZV2 response. The value specified in MSH-5 is not related to the value requested in QPD-8 What Domains Returned.

A list shall be published of all Receiving Applications that the Patient Demographics Supplier supports, for the Patient Demographics Consumer to choose from. Each query is processed against one and only one source of patient demographic information.

5370   Field *MSH-9-Message Type* shall have at least two components. The first component shall have a value of **QBP**; the second component shall have a value of **ZV1**. The third component is optional; however, if present, it shall have a value of **QBP_Q21**.

3.22.4.1.2.2 QPD Segment

The Patient Demographics Consumer Actor shall send attributes within the QPD segment as described in Table 3.22-2.

Table 3.22-2. PDQ Profile - QPD segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	250	CE	R	0471	01375	Message Query Name
2	32	ST	R+		00696	Query Tag
3		QIP	R			Demographics and Visit Fields
8		CX	O			What Domains Returned

Adapted from the HL7 standard, version 2.5

The Consumer shall specify "IHE PDVQ Query" for QPD-1 Message Query Name.

5380

3.22.4.1.2.2.1   Parameters in QPD-3-Demographics and Visit-Related Fields

Field *QPD-3-Demographics and Visit-Related Fields* consists of one or more repetitions, each of which contains two components that together contain the name and value of a distinct parameter to the query. Acceptable segments are PID, PD1, PV1, and PV2.

5385   The first component of each parameter contains the name of an HL7 element in the form

@<seg>.<field no>.<component no>.<subcomponent no>

The above format is populated according to common HL7 usage for specifying elements used in query parameters, as follows:

<seg> represents a 3-character segment ID from the HL7 Standard.

5390   <field no> is the number of a field within the segment as shown in the SEQ column of the segment attribute table for the segment selected.

<component no>, for fields whose data types contain multiple components, shall contain the cardinal number of the component being valued. For fields whose data types do not contain multiple components, <component no> shall not be valued and its preceding period should not appear.

5395   <subcomponent no>, for components whose data types contain multiple subcomponents, shall contain the cardinal number of the subcomponent being valued. For components whose data types do not contain multiple subcomponents, <subcomponent no> shall not be valued and its preceding period shall not appear.

The second subcomponent of each parameter contains the value that is to be matched. If it is desired to
5400   constrain the quality of a match within the bounds of an algorithm known to the Supplier, the algorithm and constraint values may be specified in Fields QPD-4 through QPD-7.

The Patient Demographics Consumer may specify, and the Patient Demographics Supplier shall support, the fields in the following table.

5405

Table 3.22-3. PDQ Profile – QPD-3 fields required to be supported

FLD	ELEMENT NAME
PID.3	Patient Identifier List
PID.5	Patient Name
PID.7	Date/Time of Birth
PID.8	Administrative Sex
PID.11	Patient Address
PID.18	Patient Account Number

In addition, the Patient Demographics Supplier should support the fields in the following table, and it shall support at least one of them. Some fields may not be relevant to particular care settings (*e.g.*, inpatient, day patient) and will thus not be supportable by domains in those care settings.

5410   **Table 3-22.4. PDQ Profile – QPD-3 fields recommended to be supported**

FLD	ELEMENT NAME
PV1.2	Patient Class

PV1.3	Assigned Patient Location
PV1.7	Attending Doctor
PV1.8	Referring Doctor
PV1.9	Consulting Doctor
PV1.10	Hospital Service
PV1.17	Admitting Doctor
PV1.19	Visit Number

The Patient Demographics Supplier shall return demographic records that reflect the best fit to all of the search criteria.

5415   Examples of parameter expressions in QPD-3:

```
@PID.5.1.1^SMITH~@PID.8^F
```

requests all patients whose family name (first subcomponent (data type ST) of the first component (data type FN) of PID-5-Patient Name (data type XPN)) matches the value 'SMITH' and whose sex (PID-8-
5420   Sex (data type IS)) matches the value 'female'.

```
@PV1.3.2^389~@PV1.3.3^2
```

requests all patients whose room number (second component (data type IS) of PV1-3-Assigned Patient Location (data type PL)) matches the value 389 and whose bed number (third component (data type IS)
5425   of PV1-3-Assigned Patient Location (data type PL)) matches the value 2.

3.22.4.1.2.2.2   Populating QPD-8-What Domains Returned

As in the Patient Demographics Query (Transaction ITI-21), field QPD-8 restricts the set of domains for which identifiers are returned in PID-3:

5430   1. In a multiple-domain environment, QPD-8 may be used to identify one or more domains of interest to the Patient Demographics Consumer and from which the Consumer wishes to obtain a value for *PID-3-Patient Identifier*. Note that the patient information source designated by MSH-5 may or may not be associated with any of the Patient ID Domains listed in *QPD-8-What Domains Returned*.

5435   If QPD-8 is empty, the Patient Demographics Supplier shall return all Patient IDs known by the Patient Demographics Supplier for each patient that matches the search criteria. See Case 1 in Section 3.21.4.2.2.8 for details on how this information is returned.

If QPD-8 is specified and the domains are recognized, the Patient Demographics Supplier shall return the Patient IDs for each patient that matches the search criteria. See Case 2 in Section
5440   3.21.4.2.2.8 for details on how this information is returned.

Any domain not recognized by the Patient Demographics Supplier is an error condition. See Case 3 in Section 3.21.4.2.2.8 how to handle this condition.

2. In a single-domain environment, QPD-8 may be ignored by the Patient Demographics Supplier. The Supplier shall always return the identifier from the Patient ID Domain known by the Patient Demographics Supplier.

Within field QPD-8, only component 4 (Assigning Authority) shall be valued.

The Patient Demographics Supplier may or may not be able to supply additional identifiers from the domains specified in QPD-8. A discussion of how QPD-8 is processed is included in the architectural discussion in the "Using Patient Data Query (PDQ) in a Multi-Domain Environment" section (ITI TF-2: Appendix M).

The Patient Demographics Consumer shall be able to support at least one of the following mechanisms for specifying QPD-8:

1. Transmit an empty value and receive all identifiers in all domains known by the Patient Demographics Supplier (one or more domains), or

2. Transmit a single value and receive zero or more identifiers in a single domain, or

3. Transmit multiple values and receive mutiple identifiers in those multiple domains.

3.22.4.1.2.3 RCP Segment

The Patient Demographics Consumer Actor shall send attributes within the RCP segment as described in Table 3.22-5. Fields not listed are optional.

Table 3.22-5. IHE Profile - RCP segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	1	ID	R	0091	00027	Query Priority
2	10	CQ	O	0126	00031	Quantity Limited Request

Adapted from the HL7 standard, version 2.5

3.22.4.1.2.3.1   Populating RCP-1-Query Priority

Field *RCP-1-Query Priority* shall always contain **I**, signifying that the response to the query is to be returned in Immediate mode.

3.22.4.1.2.3.2   Populating RCP-2-Quantity Limited Request

The Patient Demographics Consumer Actor may request that responses to the query be sent, using the HL7 Continuation Protocol, in increments of a specified number of patient records. (In the context of the HL7 query, a patient record is defined as the PID segment and any segments accompanying it for each patient.) It is desirable to request an incremental response if the query could result in hundreds or thousands of matches or "hits."

The Patient Demographics Supplier Actor shall support the HL7 Continuation Protocol.

Field RCP-2 is of data type CQ, which contains two components. The first component contains the number of increments, always expressed as an integer greater than 0, while the second component contains the kind of increment, always RD to signify that incremental replies are specified in terms of records.

For example, 50RD requests 50 records at a time.

See the "Incremental Response Processing" section (ITI TF-2: 3.22.4.1.3.3) and the "Expected Actions" section of the Patient Demographics Query Response message (ITI TF-2: 3.22.4.2.3) for more information on the implementation of the continuation protocol.

3.22.4.1.2.4 DSC Segment

The Patient Demographics Consumer Actor may request additional increments of data by specifying this segment on the query request. This segment should be omitted on the initial query request. Its purpose is to request additional increments of the data from the Patient Demographic Supplier Actor.

Table 3.22-9. IHE Profile - DSC segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	180	ST	O		00014	Continuation Pointer
2	1	ID	O	0398	01354	Continuation Style

3.22.4.1.2.4.1 Populating DSC-1 Continuation Pointer

To request additional increments of data, DSC-1 (Continuation Pointer) shall echo the value from RSP^K22 DSC-1.

3.22.4.1.2.4.2 Populating DSC-2 Continuation Style

DSC-2 (Continuation Style) shall always contain "I", signifying that this is part of an interactive continuation message.

3.22.4.1.3 Expected Actions

3.22.4.1.3.1 Immediate Acknowledgement

The Patient Demographics Supplier shall immediately return an RSP^ZV2 response message as specified below in Section 3.22.4.2, "Patient Demographics Response." The RSP^ZV2 response message incorporates original mode application acknowledgment as specified in the "Acknowledgment Modes" section (ITI TF-2: C.1.3). The Supplier shall use Field *MSH-3-Sending Application* of the RSP^ZV2 message to return the value it received from the Patient Demographics Consumer in Field *MSH-5-Receiving Application* of the QBP^ZV1 message.

3.22.4.1.3.2 Query Parameter Processing

The Patient Demographics Supplier Actor shall be capable of accepting, searching on, and responding with attributes in the QPD segment as specified in Table 3.22-2.

The Patient Demographics Supplier Actor must be capable of receiving all valid combinations of
subcomponents that make up the Assigning Authority component (*i.e.*, all valid combinations of QPD-3.8).

Handling of phonetic issues, alternate spellings, upper and lower case, wildcards, accented characters,
etc., if deemed appropriate, is to be supported by the Patient Demographics Supplier rather than by the
Patient Demographics Consumer. The Supplier shall return at least all exact matches to the query
parameters sent by the Consumer; IHE does not further specify matching requirements.

3.22.4.1.3.3 Incremental Response Processing

The Patient Demographics Supplier Actor shall be capable of accepting and processing attributes in the
RCP segment as listed in Table 3.22-5. In particular, the Patient Demographics Supplier Actor shall
respond in immediate mode (as specified by a *RCP-1-Query Priority* value of **I**).

Also, the Patient Demographics Supplier Actor shall be able to interpret *RCP-2-Quantity Limited
Request* to return successive responses of partial lists of records according to the HL7 Continuation
Protocol, as described in Section 3.22.4.2 below and in the HL7 Standard.

3.22.4.2 Patient Demographics and Visit Response

3.22.4.2.1   Trigger Events

The Patient Demographics Supplier's response to the Find Candidates with Visit Information message
shall be the following message:

ZV2 – Find Candidates with Visit Information response

3.22.4.2.2   Message Semantics

The Patient Demographics and Visit Response transaction is conducted by the RSP^ZV2 message. The
Patient Demographics Supplier Actor shall generate this message in direct response to the QBP^ZV1
message previously received. This message satisfies the Application Level, Original Mode
Acknowledgement for the HL7 QBP^ZV1 message.

The segments of the message listed without enclosing square brackets in Table 3.22-6 are required.
Detailed descriptions of all segments listed in the table below are provided in the following subsections.
Other segments of the message are optional.

Table 3.22-6 RSP Segment Pattern Response

RSP	Segment Pattern Response	Chapter in HL7 2.5
MSH	Message Header	2
MSA	Message Acknowledgement	2
[{ERR}]	Error	2
QAK	Query Acknowledgement	5
QPD	Query Parameter Definition	5

[{ PID	Patient Identification	3
[PD1]	Additional Patient Demographics	3
PV1	Patient Visit	3
[PV2]	Patient Visit – Additional Information	3
[QRI] }]	Query Response Instance	5
[DSC]	Continuation Pointer	2

5540

3.22.4.2.2.1 MSH Segment

The MSH segment shall be constructed as defined in the "Message Control" section (ITI TF-2: C.1.2).

Field *MSH-3-Sending Application* specifies the patient information source that processed the query. The Patient Demographics Supplier shall use Field *MSH-3-Sending Application* of the RSP^ZV2 message to
5545 return the value it received from the Patient Demographics Consumer in Field *MSH-5-Receiving Application* of the QBP^Q22 message.

Field *MSH-9-Message Type* shall have at least two components. The first component shall have a value of **RSP**; the second component shall have a value of **ZV2**. The third component is optional; however, if present, it shall have a value of **RSP_ZV2**.

5550 ### 3.22.4.2.2.2 MSA Segment

The Patient Demographics Supplier Actor is not required to send any attributes within the MSA segment beyond what is specified in the HL7 standard. See the "Acknowledgment Modes" section (ITI TF-2: C.1.3) for the list of all required and optional fields within the MSA segment.

3.22.4.2.2.3 QAK Segment

5555 The Patient Demographics Supplier Actor shall send attributes within the QAK segment as defined in table 3.22-7. For the details on filling in QAK-2 (Query Response Status) refer to the "Patient Demographics Supplier Actor Query Response Behavior" section (ITI TF-2: 3.22.4.2.2.11).

QAK-1 (Query Tag) shall echo the same value of QPD-2 (Query Tag) of the QBP^Q22 message, to allow the Patient Demographics Query Consumer to match the response to the corresponding query
5560 request.

Table 3.22-7. IHE Profile - QAK segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	32	ST	R		00696	Query Tag
2	2	ID	R+	0208	00708	Query Response Status

Adapted from the HL7 standard, version 2.5

3.22.4.2.2.4 QPD Segment

5565 The Patient Demographics Supplier Actor shall echo the QPD Segment value that was sent in the QBP^ZV1 message.

3.22.4.2.2.5 PID Segment

The Patient Demographics Supplier Actor shall return one PID segment group (*i.e.*, one PID segment plus any segments associated with it in the message syntax shown in Table 3.22-6) for each matching patient record found. The Supplier shall return the attributes within the PID segment as specified in Table 3.22-8. In addition, the Patient Demographics Supplier Actor shall return all other attributes within the PID segment for which it is able to supply values.

5570

Table 3.22-8. PDQ Profile - PID segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
3	250	CX	R		00106	Patient Identifier List
5	250	XPN	R		00108	Patient Name
7	26	TS	R2		00110	Date/Time of Birth
8	1	IS	R2	0001	00111	Administrative Sex
11	250	XAD	R2		00114	Patient Address
18	250	CX	R2		00121	Patient Account Number

Adapted from the HL7 standard, version 2.5

5575   The Patient Demographics Supplier may or may not be able to supply additional identifiers from the domains specified in QPD-8. Inability to supply an identifier in a particular domain is not an error, provided that the domain is recognized.

The PID segment and the PD1, PV1, PV2, and QRI segments that are associated with it are returned only when the Patient Demographics Supplier Actor is able to associate the search information in QPD-

5580   3 with one or more patient records in the patient information source associated with *MSH-5-Receiving Application*. See the "Patient Demographics Supplier Actor Query Response Behavior" section (ITI TF-2: 3.22.4.2.2.11) for a detailed description of how the Patient Demographics Supplier Actor responds to the query request under various circumstances.

3.22.4.2.2.6 PD1 Segment

5585   For each patient for which the Patient Demographics Supplier Actor returns a PID segment, it may optionally return the PD1 (Patient Additional Demographics) segment, but is not required to do so.

3.22.4.2.2.7 PV1 Segment

For each patient for which the Patient Demographics Supplier Actor returns a PID segment, it shall also return a PV1 Segment in which attributes are populated as specified in Table 3.22-9. In addition, the

5590   Patient Demographics Supplier Actor shall return all other attributes within the PV1 segment for which it is able to supply values.

Table 3.22-9. PDQ Profile – PV1 segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
2	1	IS	R	0004	00132	Patient Class
3	80	PL	R2		00133	Assigned Patient Location
7	250	XCN	R2	0010	00137	Attending Doctor
8	250	XCN	R2	0010	00138	Referring Doctor
9	250	XCN	R2	0010	00139	Consulting Doctor

10	3	IS	R2	0069	00140	Hospital Service
17	250	XCN	R2	0010	00147	Admitting Doctor
19	250	CX	R2		00149	Visit Number

Adapted from the HL7 standard, version 2.5

3.22.4.2.2.8 PV2 Segment

5595 For each patient for which the Patient Demographics Supplier Actor returns a PID segment, it may optionally return the PV2 (Patient Visit – Additional Information) segment, but is not required to do so.

3.22.4.2.2.9 QRI Segment

For each patient for which the Patient Demographics Supplier Actor returns a PID segment, it may optionally return the QRI (Query Response Instance) segment, but is not required to do so. Refer to the
5600 HL7 Standard, Version 2.5, Chapter 5, Section 5.5.5, for more information.

3.22.4.2.2.10 DSC Segment

If a number of records is specified in *RCP-2-Quantity Limited Request*, the Patient Demographics Supplier Actor shall return an incremental response of that number of records when the number of matching records it finds exceeds the number of records specified in RCP-2.

5605 As long as the Patient Demographics Supplier Actor has records to return in additional to those returned in the incremental response, the Supplier shall return a DSC Segment. The single field of the DSC Segment shall contain a unique alphanumeric value (the Continuation Pointer) that the Patient Demographics Consumer may return in the DSC segment of the QBP^ZV1 message to request the next increment of responses. The Supplier shall return increments as many times as the Consumer requests
5610 them (and there are increments to return), and shall stop when the Consumer sends a cancel query (QCN^J01) message (or when there are no more increments to return). The Supplier shall signal no more increments by omitting the DSC segment.

3.22.4.2.2.11 Patient Demographics Supplier Actor Query Response Behavior

The Patient Demographics Supplier shall perform the matching of patient data based on the query
5615 parameter values it receives. The information provided by the Patient Demographics Supplier Actor to Patient Demographics Consumer Actors is a list of possible matching patients from the patient information source associated with the value that the Consumer sent in *MSH-5-Receiving Application* of the query message.

If domains are specified in *QPD-8-What Domains Returned* and are recognized by the Patient
5620 Demographics Supplier, the response will also, for each patient, contain any Patient ID values found in the specified domains.

The mechanics of the matching algorithms used are internal to the Patient Demographics Supplier Actor and are outside of the scope of this framework.

The Patient Demographics Supplier Actor shall respond to the query request as described by the
5625 following 3 cases:

Case 1: The Patient Demographics Supplier Actor finds (in the patient information source associated with *MSH-5-Receiving Application*) at least one patient record matching the criteria sent in *QPD-3-Demographics Fields*. No patient identifier domains are requested in *QPD-8-What Domains Returned*.

AA (application accept) is returned in MSA-1.

5630   **OK** (data found, no errors) is returned in QAK-2.

One PID-PV1 segment group (*i.e.*, one PID segment and one PV1 segment, plus any segments associated with them in the message syntax shown in Table 3.22-6) is returned from the patient information source for each patient record found. If the Patient Demographics Supplier Actor returns data for multiple patients, it shall return these data in successive occurrences of the PID-PV1 segment

5635   group.

Within each PID segment, field *PID-3-Patient Identifier List* contains one or more identifiers from the set of Patient ID Domains known by the Patient Demograpics Supplier.

If an incremental number of records are specified in *RCP-2-Quantity Limited Request*, and the number of records found exceeds that incremental number, the Supplier returns only the incremental number of

5640   records, followed by a DSC segment containing a uniquely valued Continuation Pointer.

The consumer will specify the value of the continuation pointer in the DSC segment on the subsequent query request to request the next increment of responses.

Case 2: The Patient Demographics Supplier Actor finds (in the patient information source associated

5645   with *MSH-5-Receiving Application*) at least one patient record matching the criteria sent in *QPD-3-Demographics Fields*. One or more patient identifier domains are requested in *QPD-8-What Domains Returned*; the Supplier recognizes all the requested domains.

AA (application accept) is returned in MSA-1.

OK (data found, no errors) is returned in QAK-2.

5650   One PID-PV1 segment group (*i.e.*, one PID and one PV1 segment plus any segments associated with them in the message syntax shown in Table 3.22-6) is returned for each matching patient record found. If the Patient Demographics Supplier Actor returns data for multiple patients, it shall return these data in successive occurrences of the PID segment group.

Within each PID segment, field *PID-3-Patient Identifier List* contains, in successive occurrences

5655   delimited by the repetition separator, the identifiers from all the Patient ID Domains requested in QPD-8. In each occurrence of PID-3, component 4 contains the assigning authority value for one Patient ID Domain, and component 1 contains the Patient ID value in that domain. If an identifier does not exist for a domain that was specified on QPD-8, nothing is returned in the list.

If an incremental number of records is specified in *RCP-2-Quantity Limited Request*, and the number of

5660   records to be sent exceeds that incremental number, the Supplier returns only the incremental number of records, followed by a DSC segment containing a uniquely valued Continuation Pointer.

The consumer will specify the value of the continuation pointer in the DSC segment on the subsequent query request to request the next increment of responses.

5665 **Case 3**: The Patient Demographics Supplier Actor does not recognize one or more of the domains in *QPD-8-What Domains Returned*.

AE (application error) is returned in MSA-1 and in QAK-2.

For each domain that was not recognized, an ERR segment is returned in which the components of *ERR-2-Error Location* are valued as follows.

5670

COMP #	COMPONENT NAME	VALUE
1	Segment ID	**QPD**
2	Sequence	**1**
3	Field Position	**8**
4	Field Repetition	*(see below)*
5	Component Number	*(empty)*
6	Subcomponent Number	*(empty)*

ERR-2.4-Field Repetition identifies the ordinal occurrence of QPD-8 that contained the unrecognized domain. As specified by HL7, *ERR-2.5-Component Number* and *ERR-2.6-Subcomponent Number* are not valued because we are referring to the entire field QPD-8.

ERR-3-HL7 Error Code is populated with the error condition code **204** (unknown key identifier).
5675 Together with the values in ERR-2, this signifies that the Patient Demographics Supplier Actor did not recognize the domain for *QPD-8-What Domains Returned*.

3.22.4.2.3 Expected Actions

The Patient Demographics Consumer will use the demographic information provided by the Patient Demographics Supplier to perform the functions for which it requested the information, *e.g.*, providing a
5680 pick list to the user.

If the Supplier has sent a DSC segment containing a continuation pointer value, additional increments of data are available upon request by the Consumer. After receiving each increment of data that includes a DSC segment containing a continuation pointer value, the Consumer should take one of the following actions.

5685 • If the Consumer wishes to receive another increment of the data, the Consumer reissues the query message using a new unique value in *MSH-10-message control ID* and adding the DSC segment after the RCP segment. DSC-1 shall echo the continuation pointer returned in RSP^K22 DSC-1 segment.

• If the Consumer does not wish to receive another increment of the data, the Consumer issues a
5690 cancel query (QCN^J01) message.

• If the Consumer does not reissue the query or send a cancel query message, the query will eventually terminate.

If the Supplier has not sent a DSC segment containing a continuation pointer value, no more increments of data are available and no further action by the Consumer is required.

5695

3.22.4.3 Canceling a query

The Patient Demographic Consumer can send a cancel trigger to notify the Patient Demographic
Supplier that no more incremental response will be requested, and interactive query can be terminated.
This cancellation trigger is optional. How long the Patient Demographic Supplier retains query results
5700   (for incremental response) is an implementation decision and therefore beyond the scope of IHE.

3.22.4.3.1   Trigger Events

The Patient Demographic Consumer which received a RSP^K22 response message indicating there
more incremental response data available, can terminate the interactive query with the following HL7
5705   trigger event:

J01 – Cancel query status

3.22.4.3.2   Message Semantics

5710   Canceling a query is conducted by the QCN^J01 message. The Patient Demographic Consumer can
generate this message to notify the Patient Demographic Supplier that no more data is desired. The
segments of the message listed below are required, and their details descriptions are provided in the
following subsections.

5715   **Table 3.22.10 QCN Cancel query**

QCN	Cancel query	Chapter in HL7 2.5
MSH	Message Header	2
QID	Query identification Segment	5

The receiver shall acknowledge this cancel by the HL7 ACK message. See Appendix C.1.3,
"Acknowledgement Modes", for definition and discussion of the ACK message.

5720   **3.22.4.3.2.1 MSH Segment**

The MSH segment shall be constructed as defined in the "Message Control" section (ITI TF-2:
Appendix C.1.2).

MSH-9 (Message Type) shall have three components. The first component shall have the value of QCN;
5725   the second component shall have a value of J01. The third component shall have the value of QCN_J01.

3.22.4.3.2.2 QID Segment

The QID segment contains the information necessary to uniquely identify the query being cancelled.
5730

Table 3.22-9. IHE Profile - QID segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	32	ST	R		00696	Query Tag
2	250	CE	R	0471	01375	Message Query Name

5735 **3.22.4.3.2.2.1 Populating QID-1 Query Tag**

QID-1 (Query Tag) uniquely identifies the query to be canceled. This field shall contain the same value specified in QPD-2.

5740 **3.22.4.3.2.2.2 Populating QID-2 Message Query Name**

QID-2 (Message Query Name) identifies the name of the query. It is an identifier of the conformance statement for this query. This field shall contain the same value specified in QPD-1.

5745 **3.22.5 Security Considerations**

3.22.5.1 Audit Record Considerations

The Patient Demographics Query Transaction is a Query Information event as defined in table 3.20.6-1. The Actors involved shall record audit events according to the following:

3.22.5.1.1 Patient Demographics Consumer audit message:

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110112, DCM, "Query")
	EventActionCode	M	"E" (Execute)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-22", "IHE Transactions", "Patient Demographics and Visit Query")
Source (Patient Demograhics Consumer) (1)			
Human Requestor (0..n)			
Destination (Patient Demographics Supplier) (1)			
Audit Source (Patient Demographics Consumer) (1)			
Patient (0..n)			
Query Parameters(1)			

5750 Where:

Source **AuditMessage/ ActiveParticipant**	UserID	M	The identity of the Patient Demographics Consumer Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.
Human Requestor (if known) **AuditMessage/ ActiveParticipant**	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*NA*	
	NetworkAccessPointID	*NA*	

Destination **AuditMessage/ ActiveParticipant**	UserID	M	The identity of the Patient Demographics Source facility and receiving application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source **AuditMessage/ AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Patient **(AudittMessage/ ParticipantObjectIdentifi cation)**	ParticipantObjectTypeCode	M	"1" (Person)
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
	ParticipantObjectTypeCode	M	"2" (system object)
	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ITI-22", "IHE Transactions", "Patient Demographics and Visit Query")

	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	*U*	*not specialized*
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	the QPD segment of the query - Base64 encoded
	ParticipantObjectDetail	M	MSH-10 - the message identifier

5755 **3.22.5.1.2   Patient Demographics Source audit message:**

	Field Name	Opt	Value Constraints
Event **AuditMessage/** **EventIdentification**	EventID	M	EV(110112, DCM, "Query")
	EventActionCode	M	"E" (Execute)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ITI-22", "IHE Transactions", "Patient Demographics and Visit Query")
Source (Patient Demographics Consumer) (1)			
Destination (Patient Demographics Supplier) (1)			
Audit Source (Patient Demographics Supplier) (1)			
Patient (0..n)			
Query Parameters(1)			

Where:

Source **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Demographics Consumer Actor facility and sending application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Destination **AuditMessage/** **ActiveParticipant**	UserID	M	The identity of the Patient Demographics Supplier facility and receiving application from the HL7 message; concatenated together, separated by the | character.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address, as specified in RFC 3881.

Audit Source **AuditMessage/** **AuditSourceIdentification**	*AuditSourceID*	*U*	*Not specialized.*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Patient (AudittMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCode	M	"1" (Person)
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
Query Parameters (AudittMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCode	M	"2" (system object)
	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ITI-22", "IHE Transactions", "Patient Demographics and Visit Query")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	*U*	*not specialized*
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	the QPD segment of the query - Base64 encoded
	ParticipantObjectDetail	M	MSH-10 - the message identifier

5760

3.23 Find Personnel White Pages

This section corresponds to Transaction ITI-23 of the IHE Technical Framework. Transaction ITI-23 is used by the Personnel White Pages Consumer and the DNS Server Actors.

3.23.1 Scope

5765   This Transaction is used to locate the Personnel White Pages directory.

3.23.2 Use Case Roles
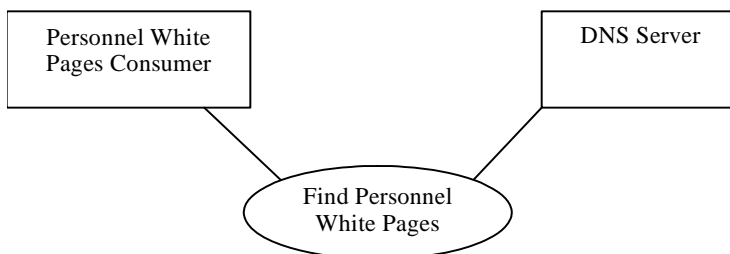
Actor: Personnel White Pages Consumer

Role: Requests Locating information for the Personnel White Pages Directory

5770   Actor: DNS Server

Role: Provides locating information about the Personnel White Pages Directory

3.23.3 Referenced Standard

IETF: RFC-2181 Clarifications to the DNS Specification

_____

RFC-2219 Use of DNS Aliases for Network Services

5775   RFC-2782 A DNS RR for specifying the location of services (DNS SRV)

DICOM: DICOM Supplement 67 – Configuration Management, January 14, 2004.

Note: Normative RFC's are frequently updated by issuance of subsequent RFC's. The original older RFC is not modified to include references to the newer RFC. This profile lists the applicable RFC's in effect at the time of publication. Subsequent updates and clarifications to these RFC's should also be
5780   applied.

3.23.4 Interaction Diagram
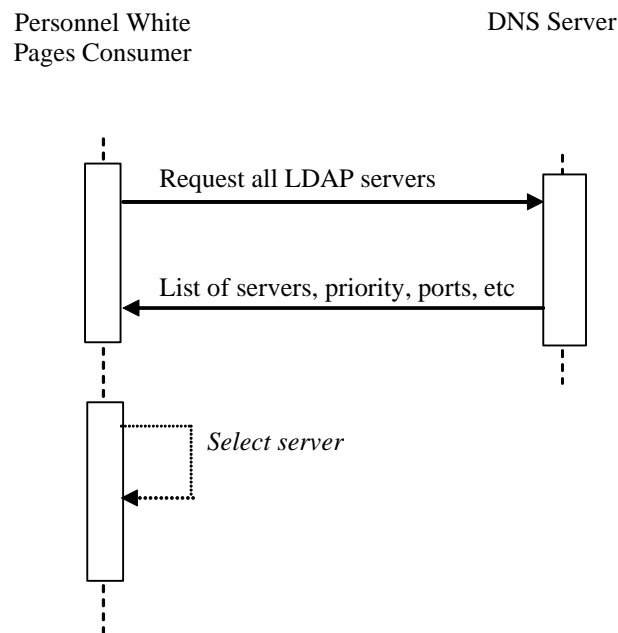
3.23.4.1 Request all LDAP servers

The RFC-2782 DNS RR is used for specifying the location of services (DNS SRV). It specifies a
5785   mechanism for requesting the names and rudimentary descriptions for machines that provide network services. The DNS client requests the descriptions for all machines that are registered as offering a particular service name. In this case the service name requested will be "_ldap._tcp". The DNS server may respond with multiple names for a single request.

3.23.4.1.1   Trigger Events

5790   This transaction is used by the Personnel White Pages Consumer prior to any access to the Personnel White Pages Directory.

3.23.4.1.2   Message Semantics

The Personnel White Pages Consumer shall request a list of all the LDAP servers available. The Personnel White Pages Consumer shall use the priority, capacity, and location information provided by

_____

5795   DNS as part of the server selection process. (RFC-2782 recommends the proper use of these parameters).

Note:

5800   Multiple LDAP servers providing access to a common replicated LDAP database is a commonly supported configuration. This permits LDAP servers to be located where appropriate for best performance and fault tolerance. The DNS server response information provides guidance for selecting the most appropriate server.

There may also be multiple LDAP servers providing different databases. In this situation the client may have to examine several servers to find the one that supports the Personnel White Pages Directory (See ITI TF-2:3.24.4.1.2.2).

5805   The client may have a mechanism for manual default selection of the LDAP server to be used if the DNS server does not provide an LDAP server location.

3.23.4.1.3   Expected Actions

The DNS Server shall return all known LDAP servers in accordance with RFC-2782.

3.24 Query Personnel White Pages

5810 This section corresponds to Transaction ITI-24 of the IHE Technical Framework. Transaction ITI-24 is used by the Personnel White Pages Consumer and the Personnel White Pages Directory Actors.

3.24.1 Scope

This Transaction is used to retrieve information from the Personnel White Pages directory.

The RFC-3377 "Lightweight Directory Access Protocol (v3) : Technical Specification" specifies a
5815 mechanism for making queries of a database corresponding to an LDAP schema. The LDAP client can compose requests in the LDAP query language, and the LDAP server will respond with the results for a single request.

3.24.2 Use Case Roles
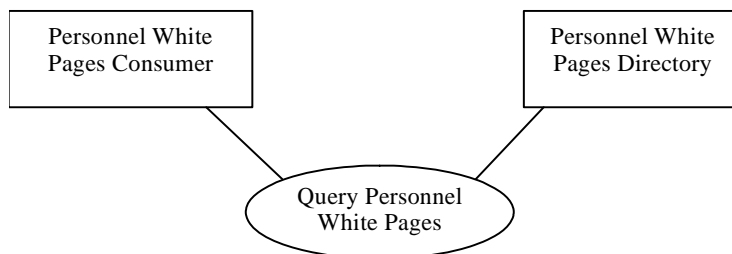
5820 Actor: Personnel White Pages Consumer

Role: Requests information about a human workforce member(s)

Actor: Personnel White Pages Directory

Role: Provides information about one or more human workforce member

3.24.3 Referenced Standard

5825 **IETF:** RFC-2181 Clarifications to the DNS Specification

RFC 1766 Tags for the Identification of Languages

RFC 2251 - Lightweight Directory Access Protocol (v3)

RFC 2252 - Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions

RFC 2253 - Lightweight Directory Access Protocol (v3): UTF-8 String Representation of
5830 Distinguished Names

RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3

RFC 2798 - Definition of the inetOrgPerson LDAP Object Class

RFC 2829 Authentication Methods for LDAP

RFC 2830 LDAPv3: Extension for Transport Layer Security

5835 RFC 3377 - Lightweight Directory Access Protocol (v3): Technical Specification

ISO: ISO/TS 17090 directory standard for healthcare identity management

_____

CRU: Projet de schémas d'annuaires et de schémas de registres de resources numériques interopérables pour les administrations Document technique – v1, novembre 2002

ITU-T: E.123: Notation for national and international telephone numbers

5840 **HL7:** HL7 Version 2.5, Chapter 2 – Control

3.24.4 Interaction Diagram
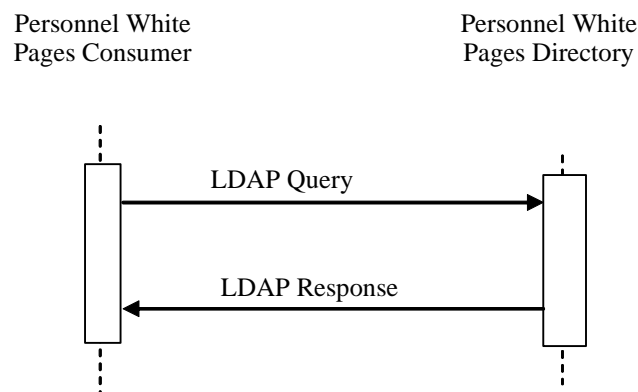
3.24.5 LDAP Query/Response

The Personnel White Pages Consumer may make a wide variety of queries and cascaded queries using
5845 LDAP. The Personnel White Pages Consumer and Personnel White Pages Directory shall support the data model described here.

A commonly supported configuration type has multiple LDAP servers providing access to a common replicated LDAP database. This permits LDAP servers to be located where appropriate for best performance and fault tolerance. The replication rules chosen for the LDAP servers affect the visible
5850 data consistency. LDAP permits inconsistent views of the database during updates and replications. This inconsistency may result in a consumer receiving the person's previous demographics or contact information. This should not be a problem for our use-cases as none of them are life critical.

3.24.5.1 Trigger Events

Personnel White Pages Consumer requires some Personnel White Pages information on one or more
5855 human workforce members.

3.24.5.2 Message Semantics

The transaction uses standard LDAP v3 query/response mechanisms.

3.24.5.2.1   User Authentication

Some of the attributes to be retrieved using this transaction may be considered sensitive to the healthcare
5860 personnel. It is the responsibility of the Personnel White Pages Directory to enforce these protections. To protect records and/or attributes, the Personnel White Pages Consumer may be called upon to provide user credentials.

_____

Anonymous authentication shall be implemented on Personnel White Pages Directory and is optional for Personnel White Pages Consumer. Anonymous authentication shall be implemented as described in LDAP v3 section 4.2 Bind Operation.

Simple Authentication shall be implemented on the Personnel White Pages Directory and is optional for the Personnel White Pages Consumer. Simple authentication shall be implemented as described in LDAP v3 section 4.2 Bind Operation. This authentication type is not recommended for use over networks that are not otherwise secured as the username and password are transferred in the clear. The use of SSL-Simple Authentication is a better choice.

SSL-Simple Authentication shall be implemented on the Personnel White Pages Directory and is optional for the Personnel White Pages Consumer. SSL-Simple Authentication is not defined in any normative text, but is consistently implemented and often referred to as "ldaps". The PWP Consumer shall connect to port 636 using SSL against the PWP Directory Certificate. The LDAP v3 conversation then continues with Simple Authentication as defined in LDAP v3 section 4.2 Bind Operation.

PWP specifies read operations on personnel demographics. The use of bi-directional TLS authentication, such as that defined in ATNA Profile, is not necessary as this profile does not provide access to Protected Health Information (PHI). The use of SSL to cover the authentication and query process is sufficient in this Profile.

3.24.5.2.2   Base DN Discovery

The Personnel White Pages represents a branch within the "LDAP" directory. Branches in LDAP are defined by a "Base DN". The list of Base DNs that are provided by a LDAP directory can be found by doing a LDAP Query with a NULL (i.e. "") Base DN, and ObjectClass="DN". The Personnel White Pages Directory shall contain a person object with the cn="IHE-ITI-PWP". The Personnel White Pages Consumer may thus search through the list of Base DNs that the LDAP Directory contains for this cn object. The Personnel White Pages Directory identified in this way shall contain person/inetOrgPerson objects that conform to the Query Personnel White Pages Directory Transaction.

Note: The first LDAP server that yields a result on the search for IHE-ITI-PWP can be used. There is no need to search further.

3.24.5.2.3   Query Encoding

Note that the LDAP transactions utilize UTF-8 encoding unless otherwise noted. The schema shown here is the commonly used schema found in X.500 Schema for LDAP and inetOrgPerson. Extensions beyond this schema are not recommended. The base schema must be preserved to ensure interoperability. Schema extensions shall not introduce attributes that duplicate the meaning of any attribute specified in this Profile.

These attributes are multi-valued unless explicitly defined as single-valued. At this time there is no universally implemented method to distinguish the purpose for any of the instances in a multi-valued attribute. The IHE recommends that the first entry contain the preferred value, and that applications use the first entry whenever a single value must be selected.

The following table shows the attributes found in Person (OrganizationalPerson and ResidentialPerson) as defined in RFC 2256 and inetOrgPerson as defined in RFC 2798. The first three columns contain the definitions from the standards for reference. Within the table the fourth column is the IHE recommendation for use with further discussion found in the fifth column.

KEY for IHE REQ Column:

5905   **R** – The Personnel White Pages Directory shall contain valid values for these attributes. These values are critical to Healthcare workflow.

R2– The Personnel White Pages Directory shall contain valid values for these attributes if the value is available. These attributes are sufficiently useful that the provider should utilize it in the defined way. Personnel White Pages Consumers should expect that the information in these attributes are valid, but

5910   shall be robust to empty values.

O – The Personnel White Paged Directory may contain values for these optional attributes. The IHE has identified sufficiently useful purpose or defined an interoperable way to use the value. The IHE may profile these values in future profiles.

D – Although these attributes are defined in inetOrgPerson/Person, their use is discouraged. This is

5915   typically due to the attribute being obsolete, poorly implemented, or not available for query.

Attribute Name	Source	• Definition • Standard defined Optionality • Description	IHE REQ	IHE Comment
aliasedObjectName	RFC 2256	• Alias Object Name • Optional • The aliasedObjectName attribute is used by the directory service if the entry containing this attribute is an alias.	O	
Audio	RFC 2798	• Audio • Optional • Not well defined	D	The audio format defined is obsolete.
businessCategory	RFC 2798	• Business Category • Optional • describes the kind of business performed by an organization	D	Not well defined
CarLicense	RFC 2798	• Vehicle license or registration plate • Optional • Used to record the values of the license or registration plate associated with an individual • (e.g. 6ABC246)	O	
Cn	RFC 2256	• Common Name • Required • This is the X.500 commonName attribute, which contains a name of an object. If the user is a person, it is typically the person's full name. • (e.g. Barbara Jensen)	R	See 3.24.4.1.2.3.1 Use of language tag and HL7 Name Data Type (XPN)
departmentNumber	RFC 2798	• Department Number • Optional • Identifies a department within an organization. This can be numeric or alphanumeric • (e.g. Radiology)	O	
Description	RFC 2798	• Description • Optional • This attribute contains a human-readable description of the object.	D	
destinationIndicator	RFC 2256	• Destination Indicator • Optional • This attribute is used for the telegram service	D	Originally defined as part of telegram addressing.

Attribute Name	Source	• Definition • Standard defined Optionality • Description	IHE REQ	IHE Comment
displayName	RFC 2798	• Display Name • Optional • Singular • When displaying a person's name, especially within a one-line summary list, it is useful to be able to identify a name to be used. Since other attribute types such as 'cn' are multivalued, an additional attribute type is needed. Display name is defined for this purpose. • (e.g. Babs Jensen)	R	
employeeNumber	RFC 2798	• Employee Number • Optional • Singular • Numeric or alphanumeric identifier assigned to a person, typically based on order of hire or association with an organization. • (e.g. 42)	O	
employeeType	RFC 2798	• Employee Type • Optional • Used to identify the employer to employee relationship. Typical values used will be "Contractor", "Employee", "Intern", "Temp", "External", and "Unknown" but any value may be used. • (e.g. External)	O	
facsimileTelephoneNumber	RFC 2256	• FAX Number • Optional • A value of this attribute is a telephone number for a facsimile terminal (and, optionally, its parameters). • (e.g. +1 408 555 1992)	R2	See 3.24.4.1.2.3.3 Phone Numbers
GivenName	RFC 2798	• Name • Optional • The givenName attribute is used to hold the part of a person's name which is not their surname nor middle name. • (e.g. Barbara)	R2	
homePhone	RFC 2798	• Home Phone • Optional • (e.g. +1 408 555 1862)	O	
homePostalAddress	RFC 2798	• Home Postal Address • Optional • This attribute contains a home address used by a Postal Service to perform services for the object.	O	

Attribute Name	Source	• Definition • Standard defined Optionality • Description	IHE REQ	IHE Comment
Initials	RFC 2798	• Initials • Optional • The initials attribute contains the initials of some or all of an individuals names, but not the surname(s). • (e.g. BJJ)	R2	
internationaliSDNNumber	RFC 2798	• International ISDN Number • Optional	D	
jpegPhoto	RFC 2798	• JPEG Photograph • Optional • Used to store one or more images of a person using the JPEG File Interchange Format	O	
L	RFC 2256	• Locality Name • Optional • This is the X.500 localityName attribute, which contains the name of a locality, such as a city, county or other geographic region.	O	
labeledURI	RFC 2798	• URI • Optional • (e.g. http://www.ihe.net IHE Home)	O	
Mail	RFC 2798	• E-Mail Address • Optional • User's e-mail address in RFC 822 compliant form • (e.g. bjensen@siroe.com)	R2	
manager	RFC 2798	• Manager • Optional • Distinguished Name of the Manager	O	In Healthcare the manager of an individual is not clear. The manager attribute does not include enough information to determine the type of manager indicated.
Mobile	RFC 2798	• Mobile/cellular phone number • Optional • A value of this attribute is a telephone number complying with ITU Recommendation E.123. • (e.g. +1 408 555 1941)	R2	This attribute should contain only business use mobile phone numbers. See 3.24.4.1.2.3.3 Phone Numbers
O	RFC 2798	• Organization • Optional • Highest-level organization name, e.g., a company name, to which ou attribute entries belong. • (e.g. Saint-ihe-hospital.local)	R2	

Attribute Name	Source	• Definition • Standard defined Optionality • Description	IHE REQ	IHE Comment
objectClass	RFC 2256	• Object Class • Required • The values of the objectClass attribute describe the kind of object which an entry represents. The objectClass attribute is present in every entry, with at least two values. One of the values is either "top" or "alias". • (e.g. top, person, organizationalPerson, inetOrgPerson)	R	
ou	RFC 2256	• Organizational Unit Name • Optional • This is the X.500 organizationalUnitName attribute, which contains the name of an organizational unit. • (e.g. Radiologists)	R2	
pager	RFC 2798	• Pager phone number • Optional • A value of this attribute is a telephone number complying with ITU Recommendation E.123.	R2	This attribute should contain only business use mobile phone numbers. See 3.24.4.1.2.3.3 Phone Numbers
photo	RFC 2798	• Photo • Optional • Photo attribute values are encoded in G3 fax format with an ASN.1 wrapper.	D	The format is too cumbersome. See jpegPhoto.
physicalDeliveryOfficeName	RFC 2256	• Post Office Name • Optional • This attribute contains the name that a Postal Service uses to identify a post office.	R2	
postalAddress	RFC 2256	• Postal Address • Optional • This attribute contains an address used by a Postal Service to perform services for the object.	R2	
postalCode	RFC 2256	• Postal Code • Optional • This attribute contains a code used by a Postal Service to identify a postal service zone, such as a US ZIP code	R2	

Attribute Name	Source	• Definition • Standard defined Optionality • Description	IHE REQ	IHE Comment
postOfficeBox	RFC 2256	• Post Office Box • Optional • This attribute contains the number that a Postal Service uses when a customer arranges to receive mail at a box on premises of the Postal Service.	R2	
preferredDeliveryMethod	RFC 2798	• Delivery Method • Optional • Singular • Coded value (delivery-value) • (e.g. any, physical, telephone)	O	
preferredLanguage	RFC 2798	• Preferred Language • Optional • Singular • Preferred written or spoken language for a person. Values for this attribute type MUST conform to the definition of the Accept-Language header field defined in [RFC2068] with one exception: the sequence "Accept-Language" ":" should be omitted. • The following example indicates that this person prefers French, prefers British English 80%, and general English 70%. (e.g. fr, en-gb;q=0.8, en;q=0.7)	R2	
registeredAddress	RFC 2256	• Registered Address • Optional • A postal address suitable for reception of expedited documents, where it is necessary to have the recipient accept delivery.	O	
roomNumber	RFC 2798	• Room Number • Optional	O	
secretary	RFC 2798	• Secretary • Optional • Distinguished name of the secretary	O	
seeAlso	RFC 2798	• See Also references • Optional • Distinguished name of other interesting Objects	D	
sn	RFC 2256	• Surname • Required • This is the X.500 surname attribute, which contains the family name of a person • (e.g. Jensen)	R	

Attribute Name	Source	• Definition • Standard defined Optionality • Description	IHE REQ	IHE Comment
st	RFC 2256	• State or Province • Optional • This is the X.500 stateOrProvinceName attribute, which contains the full name of a state or province	R2	
street	RFC 2256	• Street Address • Optional • This is the X.500 streetAddress attribute, which contains the physical address of the object to which the entry corresponds, such as an address for package delivery.	R2	
telephoneNumber	RFC 2256	• Telephone number • Optional • A value of this attribute is a telephone number complying with ITU Recommendation E.123.	R2	See 3.24.4.1.2.3.3 Phone Numbers
teletexTerminalIdentifier	RFC 2798	• Teletex Terminal Identifier • Optional	D	
telexNumber	RFC 2798	• Telex Number • Optional	D	
title	RFC 2256	• Title • Optional • This attribute contains the title, such as "Vice President", of a person in their organizational context. The "personalTitle" attribute would be used for a person's title independent of their job function. • (e.g. manager, product development)	R2	
uid	RFC 2798	• User ID • Required • The user ID use for system login. • (e.g. bjensen)	R	See 3.24.4.1.2.3.2 Use of uid
userCertificate	RFC 2798	• User Identity Certificate • Optional • This attribute is to be stored and requested in the binary form, as 'userCertificate;binary'.	D	The PKCS12 format includes the private key and shall not be publicly available.
userPassword	RFC 2256	• User password • Optional • Passwords are stored using an Octet String syntax and are not encrypted. Transfer of cleartext passwords are strongly discouraged where the underlying transport service cannot guarantee confidentiality and may result in disclosure of the password to unauthorized parties.	D	Generally Not Accessible

Attribute Name	Source	• Definition • Standard defined Optionality • Description	IHE REQ	IHE Comment
userPKCS12	RFC 2798	• User PKCS #12 • Optional • PKCS #12 [PKCS12] provides a format for exchange of personal identity information. When such information is stored in a directory service, the userPKCS12 attribute should be used. This attribute is to be stored and requested in binary form, as 'userPKCS12;binary'. The attribute values are PFX PDUs stored as binary data.	D	The PKCS12 format includes the private key and shall not be publicly available.
userSMIMECertificate	RFC 2798	• User S/MIME Certificate • Optional • A PKCS#7 [RFC2315] SignedData, where the content that is signed is ignored by consumers of userSMIMECertificate values. It is recommended that values have a `contentType' of data with an absent `content' field. Values of this attribute contain a person's entire certificate chain and an smimeCapabilities field [RFC2633] that at a minimum describes their SMIME algorithm capabilities. Values for this attribute are to be stored and requested in binary form, as 'userSMIMECertificate;binary'. If available, this attribute is preferred over the userCertificate attribute for S/MIME applications.	O	
x121Address	RFC 2256	• Address for X.121 • Optional	D	
X500uniqueIdentifier	RFC 2798	• Unique identifier • Required • The x500UniqueIdentifier attribute is used to distinguish between objects when a distinguished name has been reused. This is a different attribute type from both the "uid" and "uniqueIdentifier" types.	R	

3.24.5.2.3.1 Use of language tag and HL7 Name Data Type (XCN)

Many people have different variations of their name to be used depending on the context and language. This is easily supported in LDAP through the use of the language tag as documented in RFC 1766. This
5920   language tag can be applied to any attribute but is most useful on names.

HL7 has a well-defined format for encoding names (HL7 XCN). LDAP 'name' attributes marked with a language tag of "lang-x-ihe" shall be encoded using the HL7 XCN Data Type. UTF-8 shall be used for any characters outside ASCII.

Example use of the language tag:

```
5925                objectclass: Top
                    objectclass: person
                    objectclass: organizationalPerson
                    objectclass: inetOrgPerson
                    dn: cn=Wang XiaoDong, ou=Radiologists, o=Saint-ihe-hospital.local
5930                cn: Wang XiaoDong
                    cn: XiaoDong, Wang, Florida Department of Health:123456789
                    cn;lang-cn: 王 小東
                    cn;lang-x-ihe: Wang^XiaoDong^^^^^A~王^小東^^^^^
                    sn: Wang
5935                givenname: XiaoDong
                    givenname;lang-cn: 小東
                    sn;lang-cn: 王
                    ou: People
                    uid: XiaoDong
5940                title: Sample HL7 person
                    mail: Wang.XiaoDong@foo.bar.com
                    telephonenumber: 555-555-5678
```

3.24.5.2.3.2 Use of uid.

5945   The uid attribute is a multi-valued attribute that is intended to be used for User ID. It is likely that one of the values for uid will be the enterprise User ID. Enterprises that implement the PWP Profile shall implement the following values for the uid attribute:
1. If an enterprise has implemented both IHE ITI EUA and PWP profiles, one of the uid attributes shall contain the IHE ITI EUA user identity in <user>@<realm> format.
5950   2. If an enterprise has implemented a UPIN, one of the uid attributes shall contain the UPIN value in the format <UPIN>@UPIN. Where a UPIN is the Universal Physician Identification Number as assigned by the assigning authority in which the facility operates (e.g. CMS in the USA).

3.24.5.2.3.3 Phone Numbers

Phone numbers shall be represented in the PWP Directory using E.123 notation. E.123 is a notation for
5955   national and international telephone numbers. Recommendation E.123 defines a standard way to write telephone numbers, e-mail addresses, and web addresses. It recommends the following formats (when dialing the area code is optional for local calling):

Telephone number:

National notation   (042) 123 4567

5960   International notation +31 42 123 4567

E.123 also recommends that a hypen (-), space ( ), or period (.) be used to visually separate groups of numbers. The parentheses are used to indicate digits that are sometimes not dialed. A slash (/) is used to

___

indicate alternate numbers. This information is important if you want to make sure people know how to dial a phone number in a specific country.

5965 The use of National notation and International notation will be a local PWP Directory policy. PWP Consumers shall expect to receive both notations.

3.24.5.2.4 Expected Actions

The Personnel White Pages Directory shall provide the appropriate response to the indicated query given LDAP query rules, local access control policy, and the current information it the directory.

5970 Note: Any attribute is valid to query on, the results of the query may be quick or may take a long time to complete. Each Personnel White Pages Directory will be optimized differently based on architecture and configuration. We expect that the following attributes will be query keys more often than others (cn, displayname, objectclass, sn, uid, givenName, initials, mail, o, ou, and employeeNumber).

Directory shall support Anonymous, Simple, and SSL-Simple Authentications.

5975

3.25 Intentionally Left Blank

3.26 Intentionally Left Blank

5980 ## 3.27 Intentionally Left Blank

3.28 Intentionally Left Blank

3.29 Intentionally Left Blank

5985

3.30 Patient Identity Management

This section describes Transaction ITI-30, "Patient Identity Management". Transaction ITI-30 is used by the actors Patient Demographics Supplier and Patient Demographics Consumer.

3.30.1 Scope

5990 This transaction transmits patient demographics in a patient identification domain (*i.e.* patient identifiers assigned by the same assigning authority).

The term "patient demographics" is intended to convey the patient identification and full identity and also information on persons related to this patient, such as primary caregiver, family doctor, guarantor, next of kin.

5995 The transaction contains events for creating, updating, merging, linking and unlinking patients.

It enables the sending system to qualify the reliability of a patient identity, and the type of identity used (official name, alias for VIP, unknown patient).

The transaction can be used in acute care settings for both inpatients (*i.e.*, those who are assigned a bed at the facility) and outpatients (*i.e.*, those who are not assigned a bed at the facility).

6000 The transaction can also be used in a pure ambulatory environment.

3.30.2 Use Case Roles
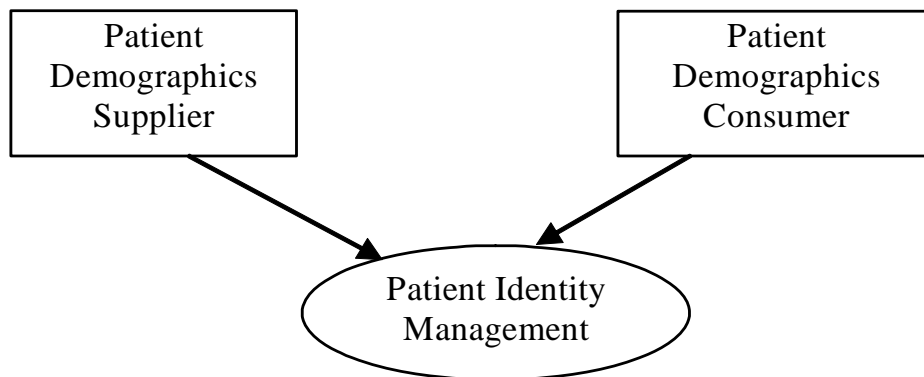
Actor: Patient Demographics Supplier

Role: Adds and modifies patient demographics.

6005 **Actor:** Patient Demographics Consumer

Role: Receives patient demographics.

3.30.3 Referenced Standards

HL7 2.5 Chapters 2, 3, 6, 15

3.30.4 Message sets and options

6010 Transaction ITI-30 supports two options, "Merge" and "Link/Unlink", in order to accommodate the various methods used by healthcare organizations to reconcile duplicated identities.

Any Patient Demographics Supplier or Patient Demographics Consumer actor SHALL support at least one of the two options "Merge" and "Link/Unlink" or both, according to the IHE national extensions of this profile. Any implementation framework will mandate both actors to support the same option.

6015 **3.30.4.1 Required message subset with option "Merge"**

Event	Trigger	Message Static definition
Create new patient	A28	ADT^A28^ADT_A05

Event	Trigger	Message Static definition
Update patient information	A31	ADT^A31^ADT_A05
Change Patient Identifier List	A47	ADT^A47^ADT_A30
Merge two patients	A40	ADT^A40^ADT_A39

3.30.4.2 Required message subset with option "Link/Unlink"

Event	Trigger	Message Static definition
Create new patient	A28	ADT^A28^ADT_A05
Update patient information	A31	ADT^A31^ADT_A05
Change Patient Identifier List	A47	ADT^A47^ADT_A30
Link Patient Information	A24	ADT^A24^ADT_A24
Unlink Patient Information	A37	ADT^A37^ADT_A37

6020 ## 3.30.5 Common HL7 Message Segments

This section describes the common HL7 message segments used in Transaction 30.

Each table represents a segment. Fields for which a precise usage description is needed, particularly those having usage C (conditional), are commented on below the table. The optional fields are usually not commented on.

6025 ### 3.30.5.1 MSH - Message Header Segment

Standard Reference: HL7 Version 2.5, Chapter 2 (Section 2.15, "Message control")

This segment defines the intent, supplier, destination, and some specifics of the syntax of the message. It also uniquely identifies the message itself and dates its production.

Table 3.30-1 : MSH - Message Header

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	Element name
1	1	SI	R	[1..1]		00001	Field Separator
2	4	ST	R	[1..1]		00002	Encoding Characters
3	227	HD	R	[1..1]		00003	Sending Application
4	227	HD	R	[1..1]		00004	Sending Facility
5	227	HD	R	[1..1]		00005	Receiving Application
6	227	HD	R	[1..1]		00006	Receiving Facility
7	26	TS	R	[1..1]		00007	Date/Time of Message
8	40	ST	X	[0..0]		00008	Security
9	15	MSG	R	[1..1]		00009	Message Type
10	20	ST	R	[1..1]		00010	Message Control Id
11	3	PT	R	[1..1]		00011	Processing Id
12	60	VID	R	[1..1]		00012	Version ID
13	15	NM	O	[0..1]		00013	Sequence Number
14	180	ST	X	[0..0]		00014	Continuation Pointer

15	2	ID	X	[0..0]	0155	00015	Accept Acknowledgement Type
16	2	ID	X	[0..0]	0155	00016	Application Acknowledgement Type
17	3	ID	RE	[1..1]	0399	00017	Country Code
18	16	ID	C	[0..1]	0211	00692	Character Set
19	250	CE	RE	[1..1]		00693	Principal Language of Message
20	20	ID	X	[0..0]	0356	01317	Alternate Character Set Handling Scheme
21	427	EI	RE	[0..*]		01598	Message Profile Identifier

6030 **MSH-1 Field Separator**, required: This Integration Profile requires that applications support any ASCII value for field separator as specified in the HL7 standard. The value suggested by HL7 is | (ASCII 124).

MSH-2 Encoding Characters, required: This field contains the four characters in the following order: the component separator, repetition separator, escape character, and subcomponent separator. This Integration Profile requires that applications support any ASCII values for encoding characters as
6035 specified in the HL7 standard. The values suggested by HL7are ^~\& (ASCII 94, 126, 92, and 38, respectively).

MSH-3 Sending Application (HD) and **MSH-5 Receiving Application (HD)**, required. See the constrainable profile definition of data type HD.

MSH-4 Sending Facility (HD) and **MSH-6 Receiving Facility (HD)**, required. See the constrainable
6040 profile definition of data type HD.

MSH-9 Message Type (MSG), required:

Components: <Message Code (ID)> ^ <Trigger Event (ID)> ^ <Message Structure (ID)>

Definition: This field contains the message type, trigger event, and the message structure ID for the message. All three components are required.

6045 **MSH-10 Message Control Id (ST)**, required:

Definition: This field contains a number or other identifier that uniquely identifies the message in the context of exchange between trading partners. Each message should be given a unique identifier by the sending system. The receiving system will echo this ID back to the sending system in the Message Acknowledgment segment (MSA). The combination of this identifier and the name of the sending
6050 application (MSH-3) should be unique across the healthcare enterprise.

MSH-12 Version ID (VID), required:

Components: <Version ID (ID)> ^ <Internationalization Code (CE)> ^ <International Version ID (CE)>

Definition: This field is matched by the receiving system to its own version to be sure the message will
6055 be interpreted correctly.

The first component SHALL be populated with the value "2.5" representing HL7 Version 2.5.

MSH-15 Accept Acknowledgment Type (ID), not supported: IHE uses only the HL7 original acknowledgement mode.

MSH-16 Application Acknowledgment Type (ID), not supported: IHE uses only the HL7 original
6060 acknowledgement mode.

MSH-17 Country Code (ID), required if available.

Definition: This field contains the country of origin for the message. The values to be used are those of ISO 3166, using the 3-character alphabetic form. Refer to *HL7 Table 0399 - Country code*.

Examples of valid values:

6065   JPN = Japan, USA = United States, GBR = United Kingdom, ITA = Italy, FRA = France, NLD = Netherlands.

MSH-18   Character Set   (ID), conditional.

Definition: This field contains the character set for the entire message. Refer to *HL7 table 0211 - Alternate character sets* for valid values.

6070   Examples of valid values:

ASCII: The printable 7-bit ASCII character set.

8859/1: The printable characters from the ISO 8859/1 Character set used by Western Europe. This character set can still be used, but 8859/15 should be used by preference. This character set is the forward-compatible version of 8859/1 and includes new characters such as the Euro currency symbol.

6075   ISO IR87: Code for the Japanese Graphic Character set for information interchange (JIS X 0208-1990).

UNICODE UTF-8: UCS Transformation Format, 8-bit form.

Condition predicate: This field shall only be valued if the message uses a character set other than the 7-bit ASCII character set. Though the field is repeatable in HL7, IHE authorizes only one occurrence (i.e., one character set). The character set specified in this field is used for the encoding of all of the
6080   characters within the message.

MSH-19   Principal Language of Message (CE), required if available. Coded from ISO 639.

Examples: DE = German, EN = English, ES=Spanish, JA = Japanese, FR = French, NL = Dutch, IT = Italian

MSH-20   Alternate Character Set Handling Scheme   (ID), not supported: Character set switching is
6085   not allowed here..

MSH-21   Message Profile Identifier (EI), required if available.

This field shall be valued in the messages for which a Message Profile has been officially registered with HL7. When multiple message profiles are listed in this field, they should be vendor specific and/or country specific message profiles constraining the official one.

6090   **3.30.5.2 EVN – Event Type Segment**

Standard Reference: HL7 Version 2.5, Chapter 3, section 3.4.1

This segment is used to provide generic properties of the trigger event.

Table 3.30-2: EVN – Event Type segment

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	Element name
1	3	ID	X	[0..0]	0003	00099	Event Type Code
2	26	TS	R	[1..1]		00100	Recorded Date Time
3	26	TS	C	[0..1]		00101	Date/Time Planned Event
4	3	IS	O	[0..1]	0062	00102	Event Reason Code

5	250	XCN	O	[0..*]	0188	00103	Operator ID
6	26	TS	C	[0..1]		01278	Event Occurred
7	241	HD	RE	[0..1]		01534	Event Facility

EVN-1 Event Type Code (ID): Not supported (deprecated in HL7 2.5). The Event Type Code is given in MSH-9 of segment MSH.

EVN-2 Recorded Date Time (TS): Required. Date/time when the event was recorded.

EVN-3 Date/Time Planned Event (TS): Conditional. Date/time when the event was planned.

Condition predicate:

- This field shall be populated in events "Pending Transfer" (A15) and "Cancel Pending Transfer" (A26), which are supported by transaction ITI-31.

- The update of a pending transfer uses message A08 and leaves this field empty. The update of the planned date/time of the transfer is only possible through the ZBE segment in message Z99, when using the option "Historic Movement Management" of transaction ITI-31.

- Other planned events of transaction ITI-31, such as "Pending Admit", "Pending Discharge" and the cancels thereof, use a specific field of segment PV2 to give the date/time of the planned event. For consistency of use, IHE recommends that the content of the specific field of PV2 be also copied to EVN-3.

National extensions of this profile may extend the condition above.

EVN-6 Event Occurred (TS): Conditional. This field contains the date/time that the event really occurred.

Condition predicate:

- This field shall not be populated in messages communicating pending events and their cancellations.

- In messages communicating effective events (inserts and updates), this field shall be populated with the real date/time of the notified event.

- In messages communicating cancellations, this field shall be populated with the date/time that was sent in the message that originally communicated the event being cancelled.

EVN-7 Event Facility (HD): Required if known to the sender. This field identifies the actual facility where the event occurred as distinct from the sending facility (MSH-4).

3.30.5.3 PID - Patient Identification segment

Standard Reference: HL7 Version 2.5, Chapter 3 (Section 3.4.2)

The PID segment is used by all applications as the primary means of communicating patient identification information. This segment contains permanent patient identifying and demographic information that, for the most part, is not likely to change frequently.

Table 3.30-3 : PID - Patient Identification segment

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	Element name
1	4	SI	O	[0..1]		00104	Set ID - PID

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	Element name
2	20	CX	X	[0..0]		00105	Patient ID
3	250	CX	R	[1..*]		00106	Patient Identifier List
4	20	CX	X	[0..0]		00107	Alternate Patient ID - PID
5	250	XPN	R	[1..*]		00108	Patient Name
6	250	XPN	O	[0..1]		00109	Mother's Maiden Name
7	26	TS	CE	[0..1]		00110	Date/Time of Birth
8	1	IS	CE	[1..1]	0001	00111	Administrative Sex
9	250	XPN	X	[0..1]		00112	Patient Alias
10	250	CE	O	[0..1]	0005	00113	Race
11	250	XAD	CE	[0..*]		00114	Patient Address
12	4	IS	X	[0..1]	0289	00115	County Code
13	250	XTN	O	[0..*]		00116	Phone Number - Home
14	250	XTN	O	[0..*]		00117	Phone Number - Business
15	250	CE	O	[0..1]	0296	00118	Primary Language
16	250	CE	O	[0..1]	0002	00119	Marital Status
17	250	CE	O	[0..1]	0006	00120	Religion
18	250	CX	O	[0..1]		00121	Patient Account Number
19	16	ST	X	[0..1]		00122	SSN Number - Patient
20	25	DLN	X	[0..1]		00123	Driver's License Number - Patient
21	250	CX	O	[0..*]		00124	Mother's Identifier
22	250	CE	O	[0..1]	0189	00125	Ethnic Group
23	250	ST	O	[0..1]		00126	Birth Place
24	1	ID	O	[0..1]	0136	00127	Multiple Birth Indicator
25	2	NM	O	[0..1]		00128	Birth Order
26	250	CE	O	[0..1]	0171	00129	Citizenship
27	250	CE	O	[0..1]	0172	00130	Veterans Military Status
28	250	CE	X	[0..0]	0212	00739	Nationality
29	26	TS	C	[0..1]		00740	Patient Death Date and Time
30	1	ID	C	[0..1]	0136	00741	Patient Death Indicator
31	1	ID	CE	[0..1]	0136	01535	Identity Unknown Indicator
32	20	IS	CE	[0..*]	0445	01536	Identity Reliability Code
33	26	TS	CE	[0..1]		01537	Last Update Date/Time
34	241	HD	O	[0..1]		01538	Last Update Facility
35	250	CE	CE	[0..1]	0446	01539	Species Code
36	250	CE	C	[0..1]	0447	01540	Breed Code
37	80	ST	O	[0..1]		01541	Strain
38	250	CE	O	[0..2]		01542	Production Class Code
39	250	CWE	O	[0..*]		01840	Tribal Citizenship

In accord with the HL7 Version 2.5 usage of this segment, fields PID-2 (Patient ID), PID-4 (Alternate Patient ID), PID-19 (SSN patient number) and PID-20 (Driver's license number) are superseded by field PID-3, as shown below; field PID-28 (Nationality) is superseded by field PID-26 (Citizenship).

PID-3 – Patient Identifier List (CX), required. This field contains a list of identifiers (one or more)
6130 used by the healthcare facility to uniquely identify a patient.

As shown in the constrained profile definition of data type CX at the end of this supplement, subfields
CX-1 "ID number", CX-4 "Assigning authority", and CX-5 "Identifier Type Code" are required for each
identifier.

This field may be populated with various identifiers assigned to the patient by various assigning
6135 authorities.

The authorized values for subfield CX-5 "Identifier Type Code" are given in HL7 Table 0203 (HL7
Version 2.5, Chapter 2A, Section 2A.14.5).

Values commonly used for Identifier Type Code in the context of PID-3 are as follows:

BC	Bank card number. Assigning authority is the bank.
DL	Driver's licence number. Assigning authority is the state
NH	National Health Plan Identifier. Assigning authority at the national level.
PE	Living Subject Enterprise Number. Assigning authority is the enterprise.
PI	Patient Internal Identifier assigned by the healthcare organization.
PPN	Passport number.
PRC	Permanent Resident Card Number
SS	Social Security Number.

6140 (DL)

6145 (PRC)

PID-5 – Patient Name (XPN), required. This field contains one or more names for the patient. At least
one name must be provided, with at least the first subfield "Family Name" valued. See the constrained
6150 profile definition of data type XPN.

PID-7 – Date/Time of Birth (TS), conditional.

Condition predicate:

- This field is required if available (i.e., known to the sender) in the following messages: Creation
  of a new patient (A28 in ITI-30), inpatient admitted (A01 in ITI-31), registration of an outpatient
6155 (A04 in ITI-31), update patient demographics (A31 in ITI-30), update patient demographics in
  the context of an encounter (A08 in ITI-31).

- In all other messages, it is optional.

- If the exact date of birth is not known, it can be truncated to the year of birth (e.g. 1954) or to the
  year and month of birth (e.g. 195411).

6160 **PID-8 – Administrative Sex (IS)**, conditional.

Condition predicate:

- This field is required if available in the following messages: Creation of a new patient (A28 in
  ITI-30), inpatient admitted (A01 in ITI-31), registration of an outpatient (A04 in ITI-31), update
  patient demographics (A31 in ITI-30).

6165
- In all other messages, it is optional.

- The authorized values are these, taken from HL7 User-defined Table 0001:

User-defined Table 0001 - Administrative Sex

Value	Description	Comment
F	Female	
M	Male	
O	Other	
U	Unknown	
A	Ambiguous	
N	Not applicable	

PID-10 – Race (CE), optional: This field may be further constrained in national extensions of this PAM profile. For instance, it will be required if available (usage code RE) in the US extension, but will not be
6170   supported (usage code X) in the French extension.

PID-11 – Patient Address (XAD), conditional:

Condition predicate:

- This field is required if available (if known to the sender) in the following messages: Creation of a new patient (A28 in ITI-30), inpatient admitted (A01 in ITI-31), registration of an outpatient
6175   (A04 in ITI-31), update patient demographics (A31 in ITI-30).

- In all other messages, it is optional.

PID-18 – Patient Account Number (CX): Optional.

HL7 Definition: This field contains the patient account number assigned by accounting to which all charges, payments, etc., are recorded. It is used to identify the patient's account.

6180   Relationship to encounter: A patient account can span more than one enterprise encounter. At least one of the fields PID-18 "Patient Account Number" or PV1-19 "Visit Number" shall be valued in the messages of transaction ITI-31 that use the PV1 segment. Additional requirements for the presence of value in these fields may be documented in national extensions of this profile.

PID-29 – Patient Death Date and Time (TS), conditional:

6185   Condition predicate:

- This field is required in the Patient Discharge message of transaction ITI-31, in the case when the encounter is terminated by the patient's death. It provides the date/time of the patient's death.

- In all other messages, it is optional.

PID-30 – Patient Death Indicator (ID), conditional:

6190   Condition predicate:

- This field is required to be populated with value "Y" whenever PID-29 is populated.

PID-31 – Identity Unknown Indicator   (ID), conditional:

Condition predicate:

6195

- This field is required if available (i.e., known to the sender) in the following messages: Creation of a new patient (A28 in ITI-30), inpatient admitted (A01 in ITI-31), registration of an outpatient (A04 in ITI-31), update patient demographics (A31 in ITI-30) , update patient demographics in the context of an encounter (A08 in ITI-31).

- In all other messages, it is optional.

The possible values are "Y", and "N" which is the default.

6200 The value "Y" means that the patient identity is unknown. In this case the field PID-3 shall contain one single patient identifier, which is a temporary identifier, and the field PID-32 will contain the value "AL" indicating that the patient name is an alias.

PID-32 – Identity Reliability Code (IS), conditional:

Condition predicate:

6205

- This field is required if available (i.e., known to the sender) in the following messages: Creation of a new patient (A28 in ITI-30), inpatient admitted (A01 in ITI-31), registration of an outpatient (A04 in ITI-31), update patient demographics (A31 in ITI-30) , update patient demographics in the context of an encounter (A08 in ITI-31).

- In all other messages, it is optional.

6210 The field is repeatable. The possible values are taken from HL7 user-defined Table 0445:

User-defined Table 0445 - Identity Reliability Code

Value	Description	Comment (added by IHE for this profile)
US	Unknown/Default Social Security Number	
UD	Unknown/Default Date of Birth	
UA	Unknown/Default Address	
AL	Patient/Person Name is an Alias	Used in case of an unidentified patient (e.g. trauma case)

PID-33 – Last Update Date/Time (TS), conditional:

Condition predicate:

6215

- This field is required if available (i.e., known to the sender) in the following messages: Creation of a new patient (A28 in ITI-30), inpatient admitted (A01 in ITI-31), registration of an outpatient (A04 in ITI-31), update patient demographics (A31 in ITI-30), update patient demographics in the context of an encounter (A08 in ITI-31).

- In the cases of messages A08 and A31, the content of this field is equal to the value in EVN-6-event occurred.

6220 **PID-35 – Species Code (CE)** and **PID-36 – Breed Code (CE)**, conditional:

Condition predicate:

- Required if known to the sender, when the patient is a non-human living subject, in the following messages: Creation of a new patient (A28 in ITI-30), inpatient admitted (A01 in ITI-31), registration of an outpatient (A04 in ITI-31), update patient demographics (A31 in ITI-30),

6225 update patient demographics in the context of an encounter (A08 in ITI-31).

3.30.5.4 PV1 - Patient Visit segment

Standard Reference: HL7 Version 2.5, Chapter 3 (Section 3.4.3)

The PV1 segment is used by Registration/Patient Administration applications to communicate information on an account or visit-specific basis.

6230

Table 3.30-4: PV1 - Patient Visit segment

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	ELEMENT NAME
1	4	SI	O	[0..1]		00131	Set ID - PV1
2	1	IS	R	[1..1]	0004	00132	Patient Class
3	80	PL	C	[0..1]		00133	Assigned Patient Location
4	2	IS	O	[0..1]	0007	00134	Admission Type
5	250	CX	O	[0..1]		00135	Preadmit Number
6	80	PL	C	[0..1]		00136	Prior Patient Location
7	250	XCN	O	[0..*]	0010	00137	Attending Doctor
8	250	XCN	O	[0..*]	0010	00138	Referring Doctor
9	250	XCN	X	[0..0]	0010	00139	Consulting Doctor
10	3	IS	O	[0..1]	0069	00140	Hospital Service
11	80	PL	C	[0..1]		00141	Temporary Location
12	2	IS	O	[0..1]	0087	00142	Preadmit Test Indicator
13	2	IS	O	[0..1]	0092	00143	Re-admission Indicator
14	6	IS	O	[0..1]	0023	00144	Admit Supplier
15	2	IS	O	[0..*]	0009	00145	Ambulatory Status
16	2	IS	O	[0..1]	0099	00146	VIP Indicator
17	250	XCN	O	[0..*]	0010	00147	Admitting Doctor
18	2	IS	O	[0..1]	0018	00148	Patient Type
19	250	CX	O	[0..1]		00149	Visit Number
20	50	FC	O	[0..*]	0064	00150	Financial Class
21	2	IS	O	[0..1]	0032	00151	Charge Price Indicator
22	2	IS	O	[0..1]	0045	00152	Courtesy Code
23	2	IS	O	[0..1]	0046	00153	Credit Rating
24	2	IS	O	[0..*]	0044	00154	Contract Code
25	8	DT	O	[0..*]		00155	Contract Effective Date
26	12	NM	O	[0..*]		00156	Contract Amount
27	3	NM	O	[0..*]		00157	Contract Period
28	2	IS	O	[0..1]	0073	00158	Interest Code
29	4	IS	O	[0..1]	0110	00159	Transfer to Bad Debt Code
30	8	DT	O	[0..1]		00160	Transfer to Bad Debt Date
31	10	IS	O	[0..1]	0021	00161	Bad Debt Agency Code
32	12	NM	O	[0..1]		00162	Bad Debt Transfer Amount
33	12	NM	O	[0..1]		00163	Bad Debt Recovery Amount
34	1	IS	O	[0..1]	0111	00164	Delete Account Indicator
35	8	DT	O	[0..1]		00165	Delete Account Date
36	3	IS	O	[0..1]	0112	00166	Discharge Disposition
37	47	DLD	O	[0..1]	0113	00167	Discharged to Location
38	250	CE	O	[0..1]	0114	00168	Diet Type
39	2	IS	O	[0..1]	0115	00169	Servicing Facility

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	ELEMENT NAME
40	1	IS	X	[0..1]	0116	00170	Bed Status
41	2	IS	O	[0..1]	0117	00171	Account Status
42	80	PL	C	[0..1]		00172	Pending Location
43	80	PL	O	[0..1]		00173	Prior Temporary Location
44	26	TS	RE	[0..1]		00174	Admit Date/Time
45	26	TS	RE	[0..1]		00175	Discharge Date/Time
46	12	NM	O	[0..1]		00176	Current Patient Balance
47	12	NM	O	[0..1]		00177	Total Charges
48	12	NM	O	[0..1]		00178	Total Adjustments
49	12	NM	O	[0..1]		00179	Total Payments
50	250	CX	O	[0..1]	0203	00180	Alternate Visit ID
51	1	IS	O	[0..1]	0326	01226	Visit Indicator
52	250	XCN	X	[0..*]	0010	01274	Other Healthcare Provider

General conditions of use:

- All messages of transaction ITI-30 that use this segment, actually use a pseudo-PV1, which is empty. The only field populated is PV1-2 "Patient Class" values "N" (Not Applicable).

6235
- The condition predicates described below only apply to the use of this segment in the context of transaction ITI-31.

PV1-2 – Patient Class (IS), required:

Definition: This field is used by systems to categorize patients by site. It does not have a consistent industry-wide definition. It is subject to site-specific variations. Refer to *User-defined Table 0004 - Patient Class* for suggested values.

6240

User-defined Table 0004 - Patient Class

Value	Description	Comment
E	Emergency	
I	Inpatient	
O	Outpatient	
P	Preadmit	
R	Recurring patient	
B	Obstetrics	
C	Commercial Account	
N	Not Applicable	
U	Unknown	

National extensions of this PAM profile may add further values to this table.

Messages of transaction ITI-31 may use any of the above values. The four first values ("E" Emergency, "I" Inpatient, "O" Outpatient, "P" Preadmit) are in common use in most countries.

6245 **Conditions of use**:

- Transaction ITI-30 uses only the value "N" (Not Applicable) in all messages that contain the PV1 segment.

- In transaction ITI-31

    o Change to inpatient (A06) uses value I or another value representing an inpatient.

6250   o Change to outpatient (A07) uses value O or another value representing an outpatient (i.e. not assigned to an inpatient bed).

PV1-3 – Assigned Patient Location (PL), conditional:

Condition predicate:

- This field is required in the Transfer (A02) and Cancel Transfer (A12) messages.

6255   • In all other messages of transaction ITI-31, it is required if known to the sender.

PV1-6 – Prior Patient Location (PL), conditional:

Condition predicate:

- This field is required in the Transfer (A02)

- In all other messages of transaction ITI-31, it is optional.

6260   **PV1-7 – Attending Doctor (XCN)**, optional. It is recommended that when this field is populated, the segment PV1/PV2 be followed by a ROL segment containing the details on the role assumed by the attending doctor.

PV1-8 – Referring Doctor (XCN), optional. It is recommended that when this field is populated, the segment PV1/PV2 be followed by a ROL segment containing the details on the role assumed by the 6265   referring doctor.

PV1-9 – Consulting Doctor (XCN), not supported (deprecated by HL7). The consulting doctor(s) are entirely described in the appropriate ROL segments following the PV1/PV2.

PV1-11 – Temporary Location (PL), conditional:

Condition predicate: This field is used by the option "Temporary Patient Transfers Tracking" of 6270   transaction ITI-31 (messages A09, A10, A32, A33).

PV1-19 – Visit Number (CX), Optional. This fields contains the unique identifier assigned to the encounter. At least one of the fields PID-18 "Patient Account Number" or PV1-19 "Visit Number" shall be valued in the messages of transaction ITI-31 that use the PV1 segment. Additional requirements for the presence of values in these fields may be documented in national extensions of this profile.

6275   **PV1-42 – Pending Location (PL)**, conditional.

Condition predicate:

- This field is required in the Pending Transfer (A15) and Cancel Pending Transfer (A26) messages.

- In all other messages of transaction ITI-31, it is optional.

6280   **PV1-44 – Admit Date / Time (TS)**, required if available. This field contains the date/time of the beginning of the encounter.

PV1-45 – Discharge Date / Time (TS), required if available. This field contains the date/time of the discharge (end of the encounter).

3.30.5.5 MRG – Merge segment

6285   Standard Reference: HL7 Version 2.5, Chapter 3 (Section 3.4.9)

This segment contains the supplier patient identifiers list to be merged.

Table 3.30-5: MRG - Merge segment

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	Element name
1	250	CX	R	[1..*]		00211	Prior Patient Identifier List
2	250	CX	X	[0..0]		00212	Prior Alternate Patient ID
3	250	CX	O	[0..1]		00213	Prior Patient Account Number
4	250	CX	X	[0..0]		00214	Prior Patient ID
5	250	CX	X	[0..0]		01279	Prior Visit Number
6	250	CX	X	[0..0]		01280	Prior Alternate Visit ID
7	250	XPN	O	[0..*]		01281	Prior Patient Name

Each of the patient identifiers appearing in the MRG-1 is to be merged with a target patient identifier of the same type in the PID-3.

6290   The type of identifier is a code given by the 5th component of the CX data type. See the commonly used identifier types in the description of the PID segment above. See also the definition of data type CX in the "Common Data Types" section.

3.30.5.6 ROL – Role segment

Standard Reference: HL7 Version 2.5, Chapter 15 (Section 15.4.7)

6295   The ROL segment communicates information on persons related to the patient.

Table 3.30-6: ROL Segment

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM #	ELEMENT NAME
1	60	EI	C	[0..1]		01206	Role Instance ID
2	2	ID	R	[1..1]	0287	00816	Action Code
3	250	CE	R	[1..1]	0443	01197	Role-ROL
4	250	XCN	R	[1..*]		01198	Role Person
5	26	TS	O	[0..1]		01199	Role Begin Date/Time
6	26	TS	O	[0..1]		01200	Role End Date/Time
7	250	CE	O	[0..1]		01201	Role Duration
8	250	CE	O	[0..1]		01205	Role Action Reason
9	250	CE	O	[0..*]		01510	Provider Type
10	250	CE	O	[0..1]	0406	01461	Organization Unit Type
11	250	XAD	O	[0..*]		00679	Office/Home Address/Birthplace
12	250	XTN	O	[0..*]		00678	Phone

ROL-1 – Role Instance ID (EI), optional. This field is in fact optional in the context of ADT messages.

ROL-2 – Action Code (ID), required

6300 **ROL-3 – Role-ROL (CE)** , required. This field defines the functional involvement of the person. Values are given in *User-defined table 0443*:

User-defined Table 0443 - Provider role

Value	Description	Used with
AD	Admitting	PV1-17 Admitting doctor
AT	Attending	PV1-7 Attending doctor
CP	Consulting Provider	
FHCP	Family Health Care Professional	
PP	Primary Care Provider	
RP	Referring Provider	PV1-8 Referring doctor
RT	Referred to Provider	

ROL-4 – Role Person (XCN), required. Identification of the person playing the role.

3.30.5.7 OBX – Observation/Result segment

6305 Standard Reference: HL7 Version 2.5, Chapter 7 (Section 7.4.2)

In transactions ITI-30 and ITI-31, the OBX segment is primarily used to convey patient height and patient weight. For this reason, this segment is described in this section, although it always appears as optional in transactions ITI-30 and ITI-31.

Table 3.30-7: OBX Segment

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	Element name
1	4	SI	O	[0..1]		00569	Set ID – OBX
2	2	ID	R	[1..1]	0125	00570	Value Type
3	250	CE	R	[1..1]		00571	Observation Identifier
4	20	ST	O	[0..1]		00572	Observation Sub-ID
5	99999	Varies	R	[1..1]		00573	Observation Value
6	250	CE	O	[0..1]		00574	Units
7	60	ST	O	[0..1]		00575	References Range
8	5	IS	O	[0..1]	0078	00576	Abnormal Flags
9	5	NM	O	[0..1]		00577	Probability
10	2	ID	O	[0..1]	0080	00578	Nature of Abnormal Test
11	1	ID	R	[0..1]	0085	00579	Observation Result Status
12	26	TS	O	[0..1]		00580	Effective Date of Reference Range
13	20	ST	O	[0..1]		00581	User Defined Access Checks
14	26	TS	O	[0..1]		00582	Date/Time of the Observation
15	250	CE	O	[0..1]		00583	Producer's ID
16	250	XCN	O	[0..1]		00584	Responsible Observer
17	250	CE	O	[0..1]		00936	Observation Method
18	22	EI	O	[0..1]		01479	Equipment Instance Identifier
19	26	TS	O	[0..1]		01480	Date/Time of the Analysis

6310 **OBX-2 Value Type (ID)**, required.

This field contains the type of observation.

Example: "NM" for a numeric observation such as patient weight or patient height.

OBX-3 Observation Identifier (CE), required

The usage of LOINC® vocabulary is strongly recommended. Details of this free vocabulary can be found at http://www.loinc.org . The first and third sub-fields, "Identifier" and "Name of Coding System" are required in all transactions. The value of the "Name of Coding System" in the case of LOINC is "LN".

6315

Example of the code used with the patient weight: `3142-7^BODY WEIGHT (STATED)^LN`

OBX-5 Observation Value (Varies), required.

6320 This field contains the value of the observation itself.

OBX-11 Observation Result Status (ID), required.

This field contains the status of the results. In messages of transactions ITI-30 and ITI-31, this status is most commonly "F" (Final).

Example of use of the OBX segment to carry the patient weight and height:

6325

```
OBX|1|NM|3142-7^BODY WEIGHT (STATED)^LN||62|kg|||||F
OBX|2|NM|8303-0^BODY HEIGHT^LN||1.70|m|||||F
```

3.30.5.8 AL1 – Patient Allergy Information segment

6330 Standard Reference: HL7 Version 2.5, Chapter 3, Section 3.4.6

In transactions ITI-30 and ITI-31, the AL1 segment is used to inform the receiver of patient allergies. For this reason, this segment is described in this section, although it always appears as optional in transactions ITI-30 and ITI-31.

Table 3.30-8: AL1 Segment

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	Element name
1	4	SI	R	[1..1]		00203	Set ID – AL1
2	250	CE	O	[0..1]	0127	00204	Allergen Type Code
3	250	CE	R	[1..1]		00205	Allergen Code/Mnemonic/Description
4	250	CE	O	[0..1]	0128	00206	Allergen Severity Code
5	15	ST	O	[0..*]		00207	Allergen Reaction Code
6	8	DT	X	[0..0]		00208	Identification Date

6335 One or more AL1 segments may appear in the messages of transactions ITI-30 and ITI-31 if any allergies have been identified for the patient at time of registration.

3.30.6   Interactions

All messages of this transaction shall be acknowledged by the ACK message as stated in appendix C of ITI Technical Framework. For better readability, the acknowledgement messages are not shown on the interaction diagrams of this transaction.

6340

3.30.6.1 Interaction diagram
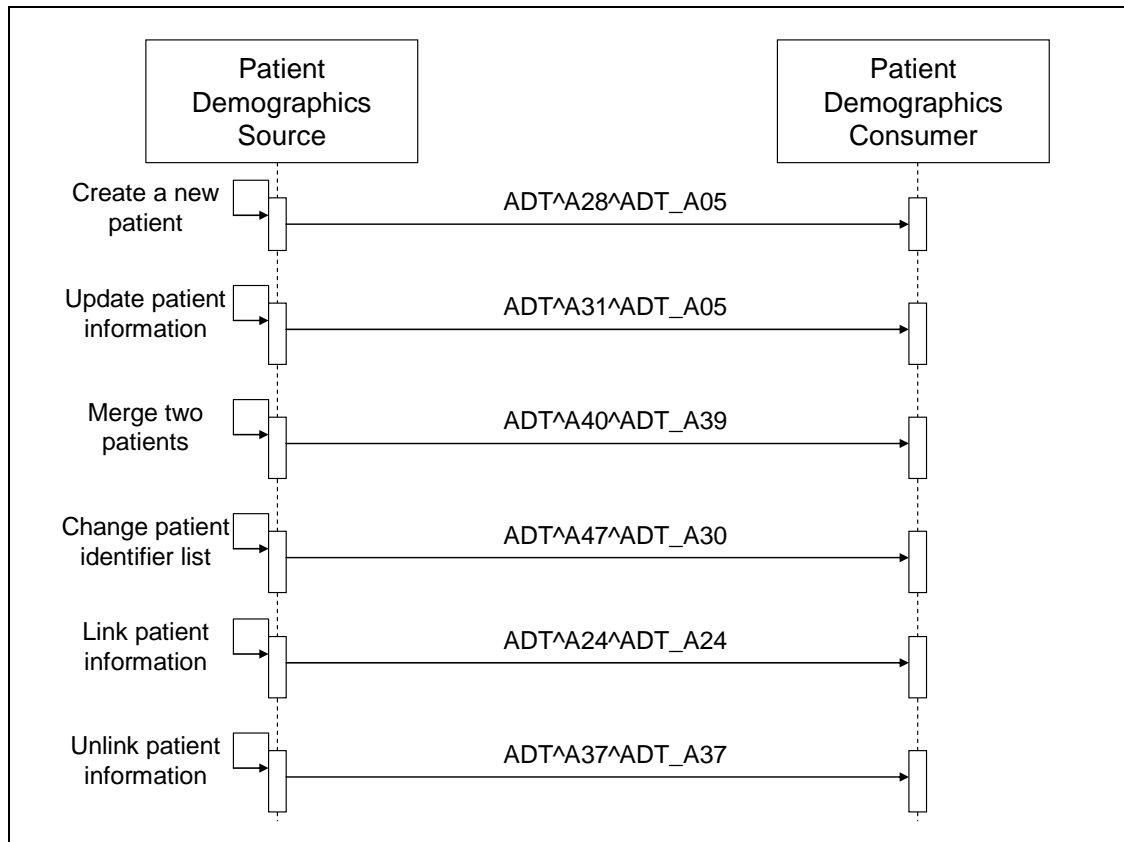
Figure 3.30-1: Interactions of transaction ITI-30

6345 **3.30.6.2 Create New Patient - ADT^A28^ADT_A05**

3.30.6.2.1   Trigger Event

This message is sent by a Patient Demographics Supplier to a Patient Demographics Consumer to communicate the demographics of a new patient, as well as related information.

MSH-9 is valued **ADT^A28^ADT_A05**.

6350 **3.30.6.2.2   Message Static Definition**

Table 3.30-9: Static definition of ADT^A28^ADT_A05

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15

NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	X	[0..0]	3
ROL	Role	X	[0..0]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6
UB2	Universal Bill 92 Information	O	[0..1]	6

3.30.6.2.3   Comments on segment usage

The ROL segment following the PID/PD1 segments is used to communicate "person level" providers having an ongoing relationship with the patient, such as "family health care provider" and "primary care provider".

The PV1 segment in this message is required in the HL7 message structure, but it is a pseudo PV1 carrying the only required field PV1-2 "Patient Class" with the value "N" meaning "Not applicable". This message does not convey any visit information.

The PV2 segment is not supported here, for the same reason.

The ROL segment following the PV1/PV2 segments is not supported here, for the same reason.

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

The ROL segment following the IN1/IN2/IN3 segments serves to communicate providers related to a specific insurance carrier.

3.30.6.2.4   Expected actions

The receiver shall add this new patient to its database, and shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

3.30.6.3 Update patient information - ADT^A31^ADT_A05

6370 **3.30.6.3.1   Trigger Event**

This message is sent by a Patient Demographics Supplier to a Patient Demographics Consumer to update the demographics of an existing patient.

MSH-9 is valued **ADT^A31^ADT_A05**.

3.30.6.3.2   Message Static Definition

6375 **Table 3.30-10: Static definition of ADT^A31^ADT_A05**

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	X	[0..0]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6

| UB2 | Universal Bill 92 Information | O | [0..1] | 6 |

3.30.6.3.3 Comments on segment usage

To accommodate the situation in which the receiver does not know the patient, this message is populated with complete up-to-date demographics for the patient.

The ROL segment following the PID/PD1 segments is used to communicate "person level" providers having an ongoing relationship with the patient, such as "family health care provider" and "primary care provider".

The PV1 segment in this message is required in the HL7 message structure, but it is a pseudo PV1 carrying the only required field PV1-2 "Patient Class" with the value "N" meaning "Not applicable". This message does not convey any visit information.

The PV2 segment is not supported here, for the same reason.

The ROL segment following the PV1/PV2 segments is not supported here, for the same reason.

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

The ROL segment following the IN1/IN2/IN3 segments serves to communicate providers related to a specific insurance carrier.

3.30.6.3.4 Expected actions

The receiver shall update the patient record in its database, and shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

If the receiver did not previously have a record for this patient, it shall insert this patient into its database.

3.30.6.4   Merge two patients - ADT^A40^ADT_A39

This message is to be supported with the "Merge" option of Transaction ITI-30.

3.30.6.4.1   Trigger Event

The Patient Demographics Supplier notifies to a Patient Demographics Consumer, the merge of records for a patient that was incorrectly filed under two different identifiers. This message is only used to merge two patient identifiers of the same type, or two lists of patient identifiers. It is not used to update other patient demographics information. The A31 trigger event should be used for this purpose.

MSH-9 is valued **ADT^A40^ADT_A39**.

3.30.6.4.2   Message Static Definition

Table 3.30-11: Static definition of ADT^A40^ADT_A39

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2

---	--- PATIENT begin	R	[1..1]	
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
MRG	Merge Information	R	[1..1]	3
PV1	Patient Visit	X	[0..0]	3

3.30.6.4.3 Comments on segment usage

This profile makes unrepeatable the PATIENT segment group: The message can communicate only one merge operation for one patient.

6410   The "incorrect supplier identifier" identified in the MRG segment (*MRG-1 - Prior Patient Identifier List*) is to be merged with the required "correct target identifier" of the same "identifier type code" component identified in the PID segment (*PID-3 - Patient Identifier List*). The "incorrect supplier identifier" would then logically never be referenced in future transactions.

The PV1 segment is not supported by IHE in this message.

3.30.6.4.4 Expected actions

6415   The receiver shall merge the two patients in its database, and shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

If the receiver does not recognize the target patient identifiers, it shall perform a Change Patient Identifier List instead of a Merge. This situation is not an error.

If the receiver does not recognize the supplier patient identifiers to be merged, it shall take no action.
6420   This situation is not an error.

If the receiver does not support the Merge option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.30.6.5 Change Patient Identifier List - ADT^A47^ADT_A30

3.30.6.5.1 Trigger Event

6425   The Patient Demographics Supplier notifies the change of a patient identifier list for a patient. That is, a single *PID-3-patient identifier list value* has been found to be incorrect and has been changed.

This message is not used to update other patient demographics information. The A31 trigger event should be used for this purpose.

MSH-9 is valued **ADT^A47^ADT_A30**.

6430   #### 3.30.6.5.2 Message Static Definition

Table 3.30-12: Static definition of ADT^A47^ADT_A30

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2

EVN	Event Type	R	[1..1]	2
---	--- PATIENT begin	R	[1..1]	
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
MRG	Merge Information	R	[1..1]	3

3.30.6.5.3   Comments on segment usage

The "incorrect supplier identifier" value is stored in the MRG segment (*MRG-1-Prior Patient Identifier List*) and is to be changed to the "correct target patient ID" value stored in the PID segment (*PID-3– Patient Identifier List*).

3.30.6.5.4   Expected actions

The receiver shall correct the identifier in its database, and shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

If the receiver already associates the target patient identifiers with another patient in its database, this is an error condition: A merge (A40) should have been sent instead of a change.

If the receiver does not recognize the supplier patient identifiers to be merged, no further action is required and no error condition exists.

3.30.6.6 Link Patient Information List - ADT^A24^ADT_A24

This message is to be supported with the "Link/Unlink" option of Transaction ITI-30.

3.30.6.6.1   Trigger Event

The Patient Demographics Supplier notifies the link of one patient identifier list (the first PID segment) to another one (the second PID segment). Linking two or more patients does not require the actual merging of patient information; following a link event, the affected patient data records should remain distinct.

This message is not used to update other patient demographics information. The A31 trigger event should be used for that purpose.

MSH-9 is valued to **ADT^A24^ADT_A24**.

3.30.6.6.2   Message Static Definition

Table 3.30-13: Static definition of ADT^A24^ADT_A24

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	X	[0..1]	3
PV1	Patient Visit	X	[0..1]	3

DB1	Disability Information	X	[0..1]	3
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	X	[0..1]	3
PV1	Patient Visit	X	[0..1]	3
DB1	Disability Information	X	[0..1]	3

6455 **3.30.6.6.3 Comments on segment usage**

The patient identifier list stored in the first PID segment (*PID-3–Patient Identifier List*) is to be linked with the patient identifier list stored in the second PID segment (*PID-3–Patient Identifier List*).

Transaction ITI-30 restricts the use of this message to only the purpose of linking two patient identifier lists. This is why segments PD1, PV1 and DB1 are not supported in this message.

6460 **3.30.6.6.4 Expected actions**

The receiver links the identifier lists in its database, and reports the result of this operation (success / error) in an acknowledgment message returned to the sender. In case of success, each patient record persists with all its associated information (encounter, clinical, care, insurance, next of kin, etc.).

6465 In case the receiver did not recognize one or both of the patient identifier lists, the linking is still performed (the receiver will record the link without creating any missing patient record) and no error condition exists.

If the receiver does not support the Link/Unlink option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.30.6.7 Unlink Patient Information List - ADT^A37^ADT_A37

6470 **3.30.6.7.1 Trigger Event**

The Patient Demographics Supplier notifies the receiving system of the unlinking of one patient identifier list (the first PID segment) from another one (the second PID segment).

MSH-9 is valued **ADT^A37^ADT_A37**.

3.30.6.7.2 Message Static Definition

6475 **Table 3.30-14: Static definition of ADT^A37^ADT_A37**

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	X	[0..1]	3
PV1	Patient Visit	X	[0..1]	3
DB1	Disability Information	X	[0..1]	3
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	X	[0..1]	3

PV1	Patient Visit	X	[0..1]	3
DB1	Disability Information	X	[0..1]	3

3.30.6.7.3   Comments on segment usage

The patient identifier lists stored in the two PID segments (*PID-3–Patient Identifier List*) are to be unlinked.

Transaction ITI-30 restricts the use of this message to only the purpose of unlinking two patient identifier lists. This is why segments PD1, PV1 and DB1 are not supported in this message.

3.30.6.7.4   Expected actions

The receiver unlinks the identifier lists in its database, and reports the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case of success the two patient records are unlinked, each of them keeping its own related information (encounter, clinical, next of kin, insurance…).

In case the receiver did not recognize the link between these two patient identifier lists, no action is performed and no error condition exists.

If the receiver does not support the Link/Unlink option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31 Patient Encounter Management

This section describes Transaction ITI-31 "Patient Encounter Management" of the IHE Patient Administration Management profile. Transaction ITI-31 is used by the actors Patient Encounter Supplier and Patient Encounter Consumer.

3.31.1 Scope

This transaction enables systems to share encounter information within acute care settings for both inpatients (i.e., those who are assigned an inpatient bed at the facility) and outpatients (i.e., those who are not assigned an inpatient bed at the facility)..

The transaction carries events for creating, updating, and canceling patient encounters as well as the movements that take place within these encounters.

The capabilities of this transaction are organized into several optional subsets to address a wide range of needs from the simplest one that only shares the basic encounter information to the most sophisticated one that tracks all patient temporary moves in the healthcare facility.

3.31.2 Use Case Roles
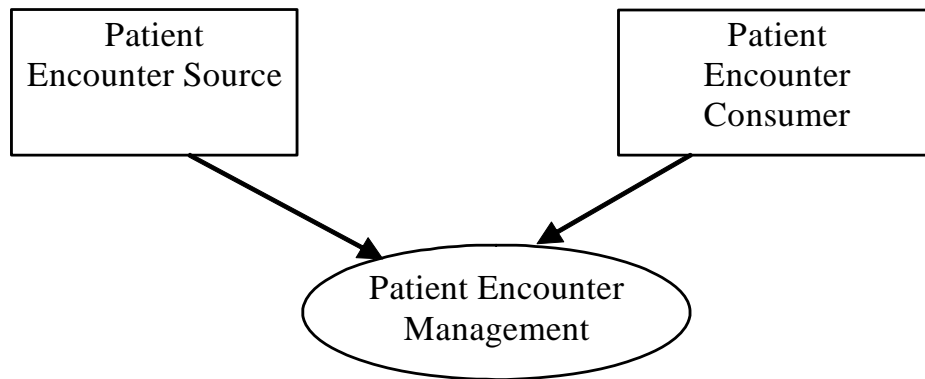
6505 **Actor**: Patient Encounter Supplier

Role: Sends inserts, cancels and updates of patient encounters and movements.

Actor: Patient Encounter Consumer

Role: Receives patient encounters and movement messages, and takes the appropriate actions.

3.31.3 Referenced Standards

6510 HL7 2.5 Chapters 2, 3, 6, 15

3.31.4 Definition of the concept "Movement"

As stated in Volume 1, a "Movement" is any change of the situation of the patient (location, patient class, attending doctor, etc.) in the context of the encounter.

The concept of "Movement" is a superset of the concept of "Transfer". Like a transfer, a movement is an
6515 event that can be planned (pending) and executed (effective). Errors detected in the recording of these pending and effective events can later be corrected through cancellations or updates, which are distinct events. Three actions are associated with Movements:

- **Insert**: This action is the first recording of the Movement.

- **Update**: This action corrects some attributes of a Movement formerly inserted. This action is
6520 possible only with the option "Historic Movement Management" of transaction ITI-30.

- **Cancel**: This action cancels a Movement that was erroneously recorded, and requests the receiver to delete this Movement from its database. Only the current Movement can be cancelled.

In some acute care settings, both the billing process and care provision process require precise knowledge of the movements of the inpatient during his or her stay in the hospital. Applications acting
6525 as Patient Encounter Supplier or Patient Encounter Consumer, divide the period of the encounter into "sub-encounters" delimited by the Movements. Each of these "sub-encounters" provides a specific context to record and invoice the acts produced within this period. However, if applications on both ends manage sub-encounters, which are periods of time, the messages of transaction ITI-31 communicate Movements as events. Hence, applications manage periods of time, but the messages carry the discrete
6530 events that delimit these periods of time.

Illustration:

1. Patient received at Emergency room by attending doctor U. (A04 / patient class E).

2. Doctor U admits the patient (A06 / patient class = I), into location BB, referring him to attending Doctor X .

6535   3. The patient is moved to location GG (A02Transfer), keeping X for attending doctor.

4. The patient is healed and leaves the hospital (A03: Discharge).

These 4 real world events are expressed with 5 trigger events / messages, two of which occur at the same time (step 2). Here the encounter will be divided into 3 sub-encounters:
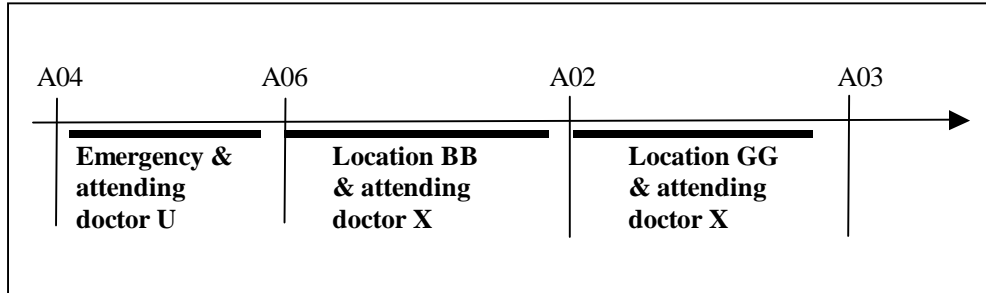
6540 **3.31.5 Message sets and options**

All messages of this transaction shall be acknowledged by the ACK message as described in Appendix C of the ITI IT Infrastructure Technical Framework. For better readability, the acknowledgement messages are not shown on the interaction diagrams of this transaction.

3.31.5.1 Basic subset

6545   **Table 3.31-1: Message basic subset for transaction ITI-31**

Category of event	Trigger / Action			
	insert		cancel	
Admit inpatient	A01	ADT^A01^ADT_A01	A11	ADT^A11^ADT_A09
Register outpatient	A04	ADT^A04^ADT_A01		
Discharge patient	A03	ADT^A03^ADT_A03	A13	ADT^A13^ADT_A01
Update patient information	A08	ADT^A08^ADT_A01		
Merge patient identifier list	A40	ADT^A40^ADT_A39		

The basic subset of transaction ITI-31 is composed of the above events and related messages. A system implementing either Patient Encounter Supplier or Patient Encounter Consumer, without any further option, shall support these 7 trigger events and messages.
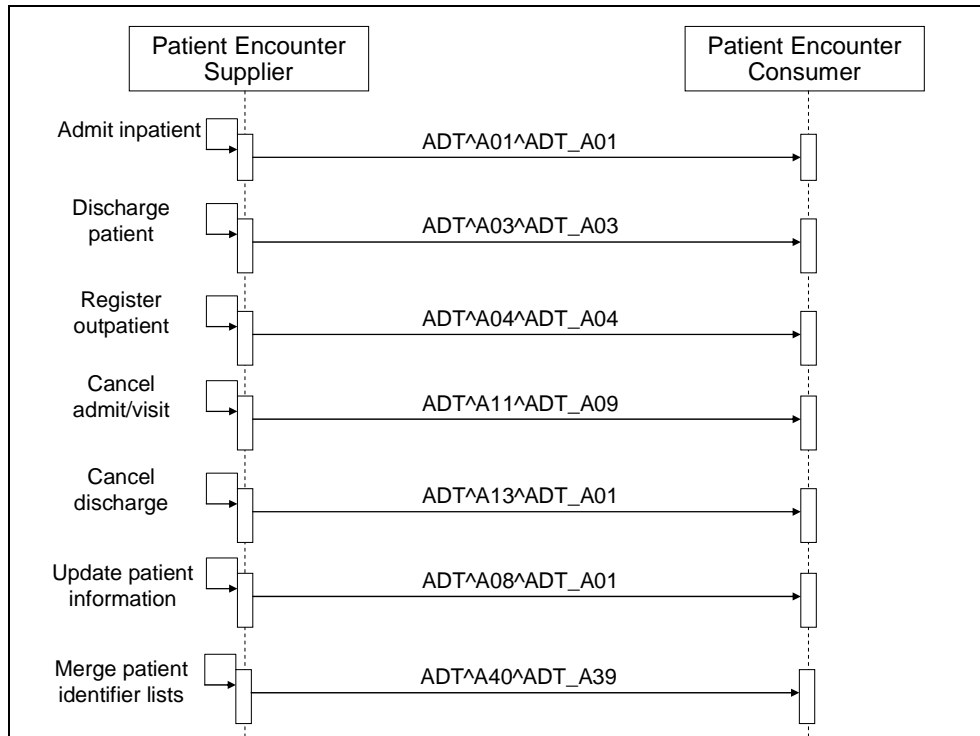
6550 **Figure 3.31-1: Interaction diagram for the basic subset**

3.31.5.2 Inpatient/Outpatient Encounter Management Option

This option adds support for management of patient class (Outpatient, Emergency, Inpatient, Pre-admitted, etc.) and of patient location (point of care, room, bed, etc.).

The following is the required message set to support the "Inpatient/Outpatient Encounter Management"
6555 option:

Table 3.31-2: Message subset for inpatient/outpatient encounter management option

Category of event	Trigger / Action			
	insert		cancel	
Admit inpatient	A01	ADT^A01^ADT_A01	A11	ADT^A11^ADT_A09
Register outpatient	A04	ADT^A04^ADT_A01		
Discharge patient	A03	ADT^A03^ADT_A03	A13	ADT^A13^ADT_A01
Update patient information	A08	ADT^A08^ADT_A01		
Merge patient identifier lists	A40	ADT^A40^ADT_A39		
Pre-admit patient	A05	ADT^A05^ADT_A05	A38	ADT^A38^ADT_A38
Change patient class to inpatient	A06	ADT^A06^ADT_A06		
Change patient class to outpatient	A07	ADT^A07^ADT_A06		
Transfer patient	A02	ADT^A02^ADT_A02	A12	ADT^A12^ADT_A12

A system implementing this option shall support these 13 trigger events and messages.

Figure 3.31-2 depicts the messages added by this option to the basic subset.
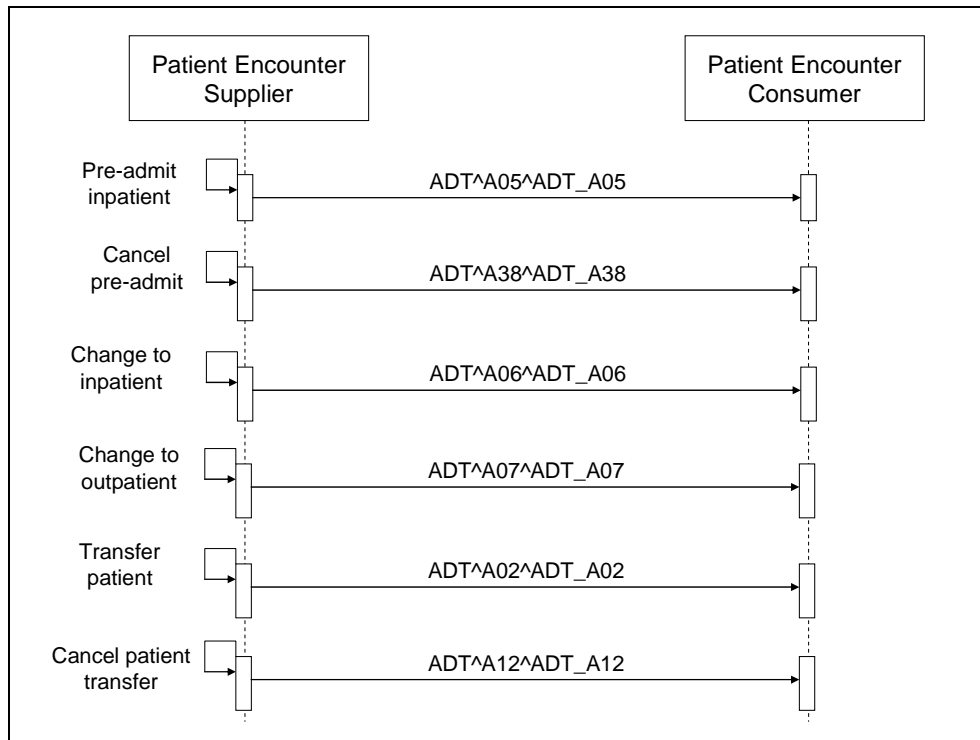
6560   **Figure 3.31-2: Additional interactions for "Inpatient/Outpatient Encounter Management" option**

3.31.5.3 Pending Event Management Option

This option adds support for management of pending events. This option also requires the "Inpatient/Outpatient Encounter Management" option.

The following is the required message set to support the "Pending Event Management" option:

6565   **Table 3.31-3: Message subset for Pending Event Management option**

Category of event	Trigger / Action			
	insert		cancel	
Admit inpatient	A01	ADT^A01^ADT_A01	A11	ADT^A11^ADT_A09
Register outpatient	A04	ADT^A04^ADT_A01		
Discharge patient	A03	ADT^A03^ADT_A03	A13	ADT^A13^ADT_A01
Update patient information	A08	ADT^A08^ADT_A01		
Merge patient identifier lists	A40	ADT^A40^ADT_A39		
Pre-admit patient	A05	ADT^A05^ADT_A05	A38	ADT^A38^ADT_A38
Change patient class to inpatient	A06	ADT^A06^ADT_A06		
Change patient class to outpatient	A07	ADT^A07^ADT_A06		
Transfer patient	A02	ADT^A02^ADT_A02	A12	ADT^A12^ADT_A12
Pending admit	A14	ADT^A14^ADT_A05	A27	ADT^A27^ADT_A21
Pending transfer	A15	ADT^A15^ADT_A15	A26	ADT^A26^ADT_A21
Pending discharge	A16	ADT^A16^ADT_A16	A25	ADT^A25^ADT_A21

A system implementing this option shall support these 19 trigger events and messages.

Figure 3.31-3 below depicts the messages added by this option to the basic subset and the Inpatient/Outpatient Encounter Management option.
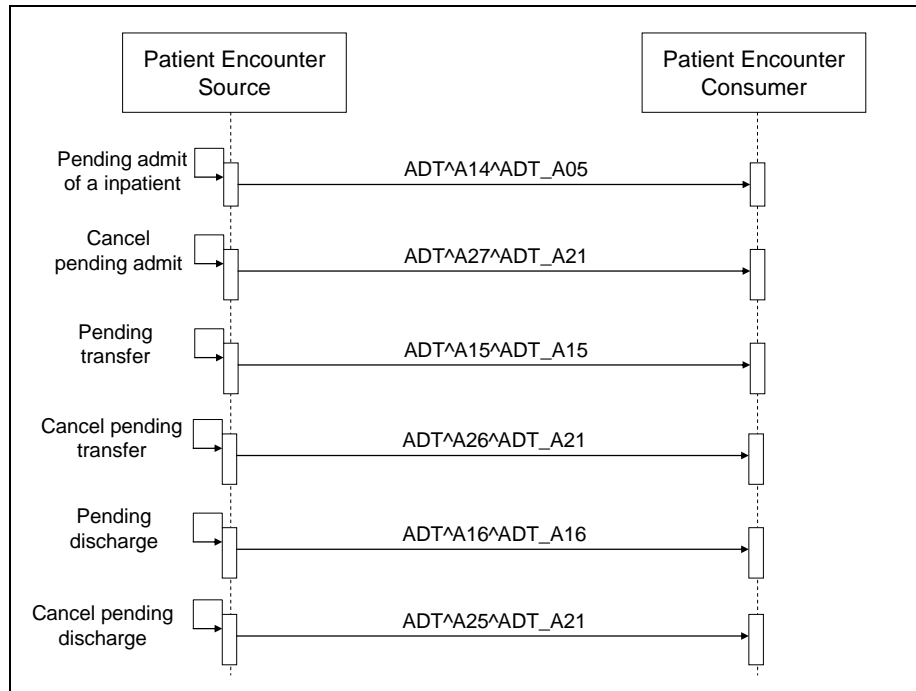
6570   **Figure 3.31-3: Additional interactions for "Pending Event Management" option**

3.31.5.4 Advanced Encounter Management Option

This option provides support to manage changes of attending doctor, leaves of absence, and accounts.

The following is the required message set to support the "Advanced Encounter Management" option:

Table 3.31-4: Message subset for Advanced Encounter Management option

Category of event	Trigger / Action			
	insert		cancel	
Admit inpatient	A01	ADT^A01^ADT_A01	A11	ADT^A11^ADT_A09
Register outpatient	A04	ADT^A04^ADT_A01		
Discharge patient	A03	ADT^A03^ADT_A03	A13	ADT^A13^ADT_A01
Update patient information	A08	ADT^A08^ADT_A01		
Merge patient identifier lists	A40	ADT^A40^ADT_A39		
Change attending doctor	A54	ADT^A54^ADT_A54	A55	ADT^A55^ADT_A52
Leave of absence	A21	ADT^A21^ADT_A21	A52	ADT^A52^ADT_A52
Return from leave of absence	A22	ADT^A22^ADT_A21	A53	ADT^A53^ADT_A52
Move account information	A44	ADT^A44^ADT_A43		

6575   A system implementing this option shall support these 15 trigger events and messages.

Figure 3.31-4 below depicts the messages added by this option to the basic subset.
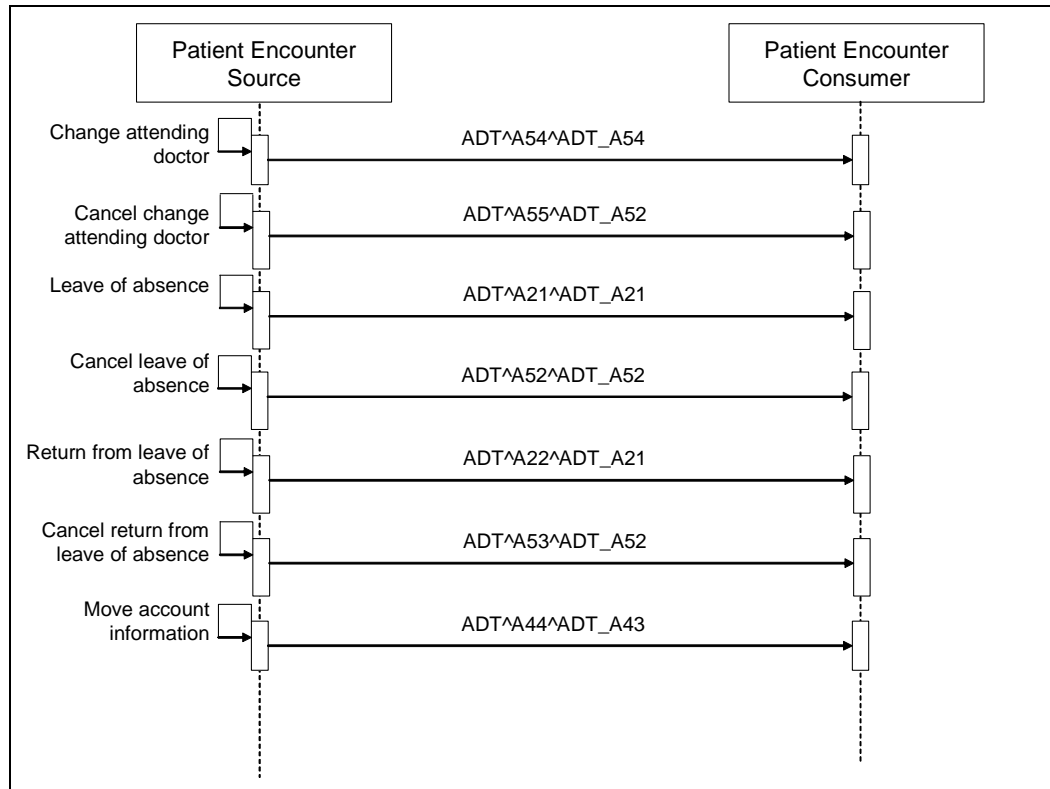
Figure 3.31-4: Additional interactions for "Advanced Encounter Management" option

6580 **3.31.5.5 Temporary Patient Transfers Tracking Option**

This option tracks patient moves to and from temporary locations such as radiotherapy, scanner, EKG, and dialysis.

The following is the required message set to support the "Temporary Patient Transfers Tracking" option:

Table 3.31-5: Message subset for Temporary Patient Transfers Tracking option

Category of event	Trigger / Action			
	insert		cancel	
Admit inpatient	A01	ADT^A01^ADT_A01	A11	ADT^A11^ADT_A09
Register outpatient	A04	ADT^A04^ADT_A01		
Discharge patient	A03	ADT^A03^ADT_A03	A13	ADT^A13^ADT_A01
Update patient information	A08	ADT^A08^ADT_A01		
Merge patient identifier lists	A40	ADT^A40^ADT_A39		
Patient departing - Tracking	A09	ADT^A09^ADT_A09	A33	ADT^A33^ADT_A21
Patient arriving - Tracking	A10	ADT^A10^ADT_A09	A32	ADT^A32^ADT_A21

6585 A system implementing this option shall support these 10 trigger events and messages.

Figure 3.31-5 below depicts the messages added by this option to the basic subset.

_____
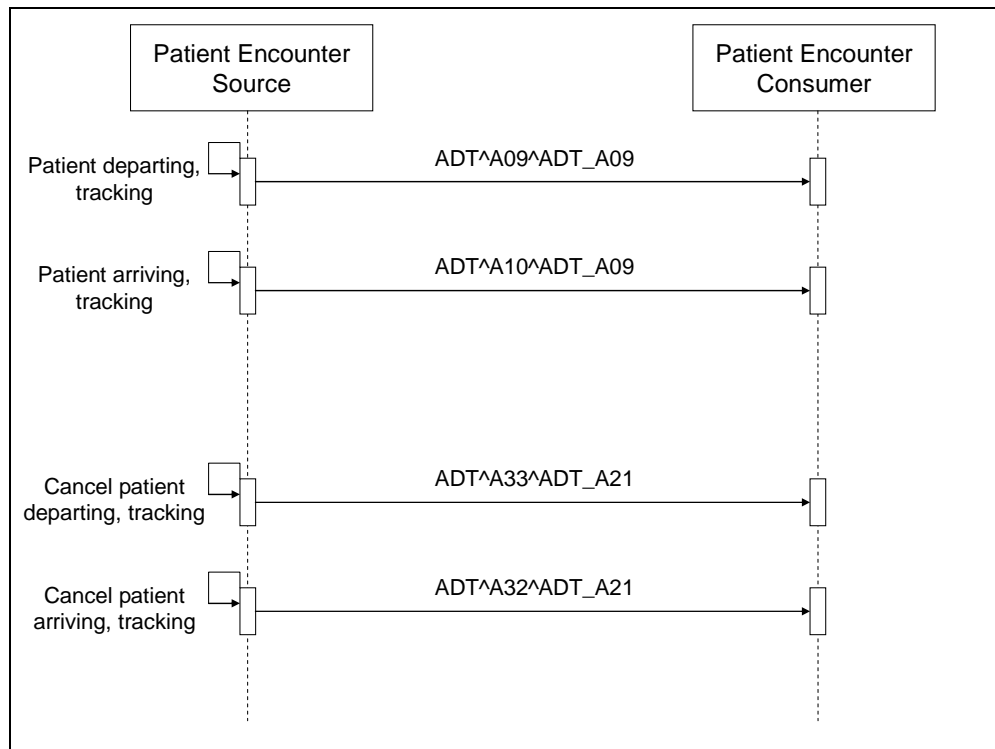
Figure 3.31-5: Additional interactions for "Temporary Patient Transfers Tracking" option

3.31.5.6 Historic Movement Management

6590   This option adds the capability to cancel or update safely any Movement.

The Movement updated can be the current Movement (currently active or pending) or a Movement in the past (i.e. historic Movement).

The Movement canceled can only be the current Movement (currently active or pending).

This capability is supported by the addition of segment ZBE below PV1/PV2. With this option, this ZBE
6595   segment is required at this position in the messages associated with the following trigger events: A01, A02, A03, A04, A05, A06, A07, A11, A12, A13, A14, A15, A16, A21, A22, A25, A26, A27, A38, A52, A53, A54, A55, Z99. In the following sections the ZBE segment is only shown in the message associated with trigger Z99 which is dedicated to the Historic Movement Management option. In the other messages, this segment will appear whenever this option is active.

6600   This segment ZBE brings the following features:

- It enables unique identification of the Movement (including admission and discharge).

- It carries an action code that describes the action to be performed on this Movement: The three possible actions are:

  o **INSERT**: The receiver must interpret the content of this message as a new Movement.

6605   o **CANCEL**: This action code is always associated with a "cancel" trigger event. The receiver shall delete the corresponding Movement (matched with its unique identifier). Only the current Movement can be cancelled.

_____

o **UPDATE**: This action code is associated with the dedicated trigger event Z99 described in section 3.31.7.30. The receiver shall update the corresponding Movement (matched
6610 with its unique identifier), which can be the current Movement or a historic Movement.

- In the case of UPDATE or CANCEL, the ZBE segment carries the code of the original trigger event that was associated with the action INSERT of the related Movement.

- It carries an indicator "Historic Movement" informing whether the action to perform is about the current Movement or a Historic one.

6615
- It provides the starting date/time of the "sub-encounter" that this Movement initiates.

- It carries the ward to which this patient is assigned during this sub-encounter.

This option may apply to any combination of the previous subsets, except Temporary Patient Transfers Tracking (Temporary Patient Transfers do not need to be uniquely identified).

Implementation note:

6620 The Patient Encounter Consumer must support transaction log update to maintain integrity of the Movement records.

3.31.6 Common HL7 Message Segments

Messages in Transaction 31 use the same common HL7 message segments as those in Transaction 30; refer to Section 3.30.5. In addition, messages in Transaction 31 use the ZBE segment, described below.

6625 **3.31.6.1 ZBE – Movement Action segment**

The ZBE segment was introduced in the German extension of the IHE Radiology Technical Framework. It is extended here with three additional fields: ZBE-5, ZBE-6 and ZBE-7. This ZBE segment is required with the "Historic Movement" option of transaction ITI-31.

The purpose of this segment is to uniquely identify any movement at creation time (action INSERT), so
6630 that any further correction brought to this movement (action UPDATE) or cancellation of it (action CANCEL) can be achieved safely and consistently between the two actors Patient Encounter Supplier and Patient Encounter Consumer.

Another security feature offered by this segment is to clearly distinguish current events from events that address a historic (past) movement to avoid any misinterpretation on the part of the receiving
6635 application.

Table 3.31-6: ZBE segment description

SEQ	LEN	DT	Usage	Card.	ELEMENT NAME
1		EI	R	[1..*]	Movement ID
2		TS	R	[1..1]	Start Movement Date/Time
3		TS	O	[0..1]	End Movement Date/Time
4		ID	R	[1..1]	Movement Action (INSERT / UPDATE / CANCEL)
5		ID	R	[1..1]	Historical Movement Indicator (values: Y / N)
6		ID	C	[0..1]	Original trigger event code [in the case of an UPDATE of the movement (trigger A08), this field conveys the original trigger event that was sent with the INSERT]
7		CWE	O	[0..1]	Responsible Ward (Medical or Nursing Ward, depending of the

SEQ	LEN	DT	Usage	Card.	ELEMENT NAME
					trigger event of the message)

ZBE-1 – Movement ID (EI): required and repeatable to support cooperative Movement Management. The Movement Identifier list is created with the action INSERT, and then recalled with further actions such as UPDATE or CANCEL.

6640 **ZBE-2 – Start Movement Date/Time (TS)**: Required. It is the date/time of the creation of the Movement, i.e. the effective date time of the event that used action INSERT with this Movement.

ZBE-3 – End Movement Date/Time (TS): Optional.

ZBE-4 – Action (ID): Required. Three possible values:

- INSERT: With any trigger event that inserts a movement.

6645 - UPDATE: With trigger event Z99

- CANCEL: With any "cancel" trigger event.

ZBE-5 –Historic Indicator (ID): Required. Values:

- 'Y' when the message is related to a Historic Movement.

- 'N' when the message is related to the current (last or next) movement.

6650 **ZBE-6 – Original Trigger (ID)**: Conditional.

Condition predicate: This field shall be populated when ZBE-4 contains action UPDATE or CANCEL. In this case, this field is populated with the trigger event that inserted (action INSERT) the movement being currently updated or canceled.

ZBE-7 – Responsible Ward (CWE): Optional. This field may be further constrained in national
6655 extensions of this profile. It will, for example, be associated with usage 'RE' in the French extension.

3.31.7 Interactions

The following sections contain the static definitions of the messages belonging to the various optional sets described above.

6660 The Historic Movement Management option is not shown in these message tables. The reader is reminded that this option adds the ZBE segment below PV1/PV2.

3.31.7.1 Admit/Visit Notification (ADT^A01^ADT_A01)

3.31.7.1.1   Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that a
6665 patient has arrived at a healthcare facility for an episode of care in which the patient is assigned to an inpatient bed. Such an episode is commonly referred to as "inpatient" care.

MSH-9 is valued **ADT^A01^ADT_A01**.

3.31.7.1.2   Message Static Definition

Table 3.31-7: Static definition of message ADT^A01^ADT_A01

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6
UB2	Universal Bill 92 Information	O	[0..1]	6
PDA	Patient Death and Autopsy	O	[0..1]	3

3.31.7.1.3   Comments on segment usage

Providers with an ongoing relationship with the patient may be communicated in ROL segments immediately following the PID/PD1 segments. Providers specific to an episode of care may be communicated in ROL segments immediately following the PV1/PV2 segments. Providers specific to a particular insurance carrier may be communicated in ROL segments immediately following the IN1/IN2/IN3 segments.

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.1.4   Expected actions

The receiver shall update the patient's status to indicate that the patient has been admitted.

6680   The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement (new admission) conflicts with an existing current movement for the patient (an admission is already opened for this patient) the message is discarded and an error condition is raised.

3.31.7.2 Cancel Admit/Visit Notification – ADT^A11^ADT_A09

6685   #### 3.31.7.2.1   Trigger Event

This message is sent by a Patient Encounter Supplier to cancel a previous notification to a Patient Encounter Consumer as a notification that a patient has been admitted for an inpatient stay (via trigger event A01) or registered for an outpatient visit (via trigger event A04). See Section 3.31.5.8 for the message to be used to cancel a pre-admit notification, and Section 3.31.5.14 for the message to be used
6690   to cancel a pending admit notification.

MSH-9 is valued **ADT^A11^ADT_A09**.

3.31.7.2.2   Message Static Definition

Table 3.31-8: Static definition of message ADT^A11^ADT_A09

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
DG1	Diagnosis Information	X	[0..0]	6

3.31.7.2.3   Comments on segment usage

6695   None.

3.31.7.2.4   Expected actions

The receiver shall reset the patient's status in its system to the value existing immediately before the admit or visit notification was received.

The receiver shall report the result of this operation (success / error) in an acknowledgment message
6700   returned to the sender.

In case this Movement conflicts with the current situation of the patient (i.e., no inpatient nor outpatient visit has been opened for this patient) the message is discarded but no error condition is raised.

3.31.7.3 Register a Patient (ADT^A04^ADT_A01)

3.31.7.3.1 Trigger Event

6705 This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that a patient has arrived at a healthcare facility for an episode of care in which the patient is not assigned to a bed. Examples of such episodes include outpatient visits, ambulatory care encounters, and emergency room visits.

MSH-9 is valued **ADT^A04^ADT_A01**.

6710 #### 3.31.7.3.2 Message Static Definition

Table 3.31-9: Static definition of message ADT^A04^ADT_A01

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6
UB2	Universal Bill 92 Information	O	[0..1]	6
PDA	Patient Death and Autopsy	O	[0..1]	3

3.31.7.3.3   Comments on segment usage

Field *PV1-44-admit date/time* is used to carry the date and time that the encounter started.

Providers with an ongoing relationship with the patient may be communicated in ROL segments
immediately following the PID/PD1 segments. Providers specific to an episode of care may be
communicated in ROL segments immediately following the PV1/PV2 segments. Providers specific to a
particular insurance carrier may be communicated in ROL segments immediately following the
IN1/IN2/IN3 segments.

One or more OBX segments may be present to carry "permanent observations" such as the patient
weight or height.

3.31.7.3.4   Expected actions

The receiver shall update the patient's status to indicate that the visit has started.

The receiver shall report the result of this operation (success / error) in an acknowledgment message
returned to the sender.

In case an inpatient encounter is already opened, the outpatient encounter is still recorded by the
receiver. This is not a situation of conflict and no error condition is raised.

3.31.7.4 Discharge/End Visit (ADT^A03^ADT_A03)

3.31.7.4.1   Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that a
patient's stay at a healthcare facility has ended. Inpatient encounters are generally closed by an A03.
Outpatient encounters may or may not be closed by an A03, depending on the healthcare organization
policies.

MSH-9 is valued **ADT^A03^ADT_A03**.

3.31.7.4.2   Message Static Definition

Table 3.31-10: Static definition of message ADT^A03^ADT_A03

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	X	[0..0]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
AL1	Allergy Information	O	[0..*]	3

DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
OBX	Observation/Result	O	[0..*]	7
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
PDA	Patient Death and Autopsy	O	[0..1]	3

3.31.7.4.3   Comments on segment usage

Field *PV1-3-assigned patient location* is used to indicate the patient's last location prior to discharge (or end of visit).

Field *PV1-45-discharge date/time* is used to carry either the date and time of discharge (for an inpatient) or the date and time that the visit ended (for an outpatient).

Providers with an ongoing relationship with the patient may be communicated in ROL segments immediately following the PID/PD1 segments. Providers specific to an episode of care may be communicated in ROL segments immediately following the PV1/PV2 segments. Providers specific to a particular insurance carrier may be communicated in ROL segments immediately following the IN1/IN2/IN3 segments.

If the patient is deceased, fields *PID-29-Patient Death Date and Time* and *PID-30-Patient Death Indicator* shall be populated.

3.31.7.4.4   Expected actions

The receiver shall update the patient's status to "discharged" (or "visit ended").

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no inpatient nor outpatient visit opened for this patient) the message is discarded but no error condition is raised.

3.31.7.5 Cancel Discharge/End Visit – ADT^A13^ADT_A01

6755 **3.31.7.5.1 Trigger Event**

This message is sent by a Patient Encounter Supplier to a Patient Encounter Consumer to cancel a previous notification (via trigger event A03) that a patient's stay at a healthcare facility had ended.

MSH-9 is valued **ADT^A13^ADT_A01**.

3.31.7.5.2 Message Static Definition

6760 **Table 3.31-11: Static definition of message ADT^A13^ADT_A01**

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6
UB2	Universal Bill 92 Information	O	[0..1]	6
PDA	Patient Death and Autopsy	O	[0..1]	3

3.31.7.5.3   Comments on segment usage

Field *PV1-3-patient location* shall contain the patient's location after the cancellation has been processed. This may be different from the patient's location prior to the discharge/end visit notification.

3.31.7.5.4   Expected actions

6765   The receiver shall reset the patient's status to its value prior to the receipt of the discharge/end visit message, and shall update the patient's location to the value in field PV1-3-patient location.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no prior discharge received) the
6770   message is discarded but no error condition is raised.

3.31.7.6 Update Patient Information (ADT^A08^ADT_A01)

3.31.7.6.1   Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that some
6775   non-movement-related information (such as address, date of birth, etc.) has changed for a patient. It is used when information about the patient has changed not related to any other trigger event.

MSH-9 is valued **ADT^A08^ADT_A01**.

3.31.7.6.2   Message Static Definition

Table 3.31-12: Static definition of message ADT^A08^ADT_A01

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6

___

Segment	Meaning	Usage	Card.	HL7 chapter
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6
UB2	Universal Bill 92 Information	O	[0..1]	6
PDA	Patient Death and Autopsy	O	[0..1]	3

3.31.7.6.3   Comments on segment usage

Providers with an ongoing relationship with the patient may be communicated in ROL segments immediately following the PID/PD1 segments. Providers specific to an episode of care may be communicated in ROL segments immediately following the PV1/PV2 segments. Providers specific to a particular insurance carrier may be communicated in ROL segments immediately following the IN1/IN2/IN3 segments.

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.6.4   Expected actions

The receiver shall update the patient record in its database to contain the information in the message.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no active encounter for this patient, or the patient is unknown) the message is discarded but no error condition is raised.

3.31.7.7 Pre-Admit (ADT^A05^ADT_A05)

3.31.7.7.1   Trigger Event

This message is sent by a Patient Encounter Supplier to a Patient Encounter Consumer to communicate information that has been collected about a patient to be admitted as an inpatient (or to be registered as an outpatient).

MSH-9 is valued **ADT^A05^ADT_A05**.

6800 ## 3.31.7.7.2   Message Static Definition

Table 3.31-13: Static definition of message ADT^A05^ADT_A05

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	X	[0..0]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6
UB2	Universal Bill 92 Information	O	[0..1]	6
PDA	Patient Death and Autopsy	O	[0..1]	3

3.31.7.7.3   Comments on segment usage

Field *PV2-8-expected admit date/time* is used to carry the expected date and time when the patient is to be admitted (or registered).

6805   Providers with an ongoing relationship with the patient may be communicated in ROL segments immediately following the PID/PD1 segments. Providers specific to an episode of care may be communicated in ROL segments immediately following the PV1/PV2 segments. Providers specific to a particular insurance carrier may be communicated in ROL segments immediately following the IN1/IN2/IN3 segments.

6810   One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.7.4   Expected actions

The receiver shall update the patient's status to pre-admitted.

6815   The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

There is no particular potential conflict between this Movement and any previously received message related to the same patient.

If the receiver does not support the Inpatient/Outpatient Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

6820   ## 3.31.7.8 Cancel Pre-Admit – ADT^A38^ADT_A38

3.31.7.8.1   Trigger Event

This message is sent by a Patient Encounter Supplier to a Patient Encounter Consumer to cancel a previous notification (via trigger event A08) that a patient was to be updated to pre-admitted (or pre-registered) status.

6825   MSH-9 is valued **ADT^A38^ADT_A38**.

3.31.7.8.2   Message Static Definition

Table 3.31-14: Static definition of message ADT^A38^ADT_A38

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..*]	6

3.31.7.8.3   Comments on segment usage

None.

6830   ### 3.31.7.8.4   Expected actions

The receiver shall reset the patient's status to its value prior to the receipt of the pre-admit message.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no pre-admit registered for this patient, or the patient is unknown) the message is discarded but no error condition is raised.

If the receiver does not support the Inpatient/Outpatient Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31.7.9 Change Outpatient to Inpatient (ADT^A06^ADT_A06)

3.31.7.9.1   Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that it has been decided to admit a patient that was formerly in a non-admitted status, such as Emergency.

MSH-9 is valued **ADT^A06^ADT_A06**.

3.31.7.9.2   Message Static Definition

Table 3.31-15: Static definition of message ADT^A06^ADT_A06

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
MRG	Merge Information	C	[0..1]	3
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	X	[0..0]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6

IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6
UB2	Universal Bill 92 Information	O	[0..1]	6

3.31.7.9.3   Comments on segment usage

The new patient location should appear in *PV1-3 - Assigned Patient Location* while the old patient location (if different) should appear in *PV1-6 - Prior Patient Location.*

Condition predicate on use of the segment MRG:

6850   A change from outpatient to inpatient status may be accompanied by the closing of the outpatient account and the opening of an inpatient account. This may be expressed by populating the outpatient account number into *MRG-3-prior account number* and the inpatient account number into *PID-18-patient account number.* The use of the MRG segment in this case is strictly conventional and is not intended to communicate an actual merge.

6855   Providers with an ongoing relationship with the patient may be communicated in ROL segments immediately following the PID/PD1 segments. Providers specific to an episode of care may be communicated in ROL segments immediately following the PV1/PV2 segments. Providers specific to a particular insurance carrier may be communicated in ROL segments immediately following the IN1/IN2/IN3 segments.

6860   One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.9.4   Expected actions

The receiver shall update the patient's class to "inpatient," and if necessary shall update the patient's location to the value in field *PV1-3-patient location.*

6865   If the MRG segment is included, the receiver shall update the patient's account number from the value in *MRG-3-prior account number* to the value in *PID-18-patient account number.*

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no active outpatient encounter
6870   is known for this patient, or the patient is unknown) the message is still processed and initiates a new inpatient encounter for a possibly new patient, and no error condition is raised.

If the receiver does not support the Inpatient/Outpatient Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

6875 **3.31.7.10 Change Inpatient to Outpatient (ADT^A07^ADT_A06)**

3.31.7.10.1 Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that a patient is no longer in an "admitted" status, but is still being seen for an episode of care.

MSH-9 is valued **ADT^A07^ADT_A06**.

6880 **3.31.7.10.2 Message Static Definition**

Table 3.31-16: Static definition of message ADT^A07^ADT_A06

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
MRG	Merge Information	C	[0..1]	3
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	X	[0..0]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6
UB2	Universal Bill 92 Information	O	[0..1]	6

3.31.7.10.3 Comments on segment usage

The new patient location should appear in *PV1-3 - Assigned Patient Location* while the old patient location (if different) should appear in *PV1-6 - Prior Patient Location*.

6885   Condition predicate on use of the segment MRG:

A change from inpatient to outpatient status may be accompanied by the closing of the inpatient account and the opening of an outpatient account. This may be expressed by populating the inpatient account number into *MRG-3-prior account number* and the outpatient account number into *PID-18-patient account number*. The use of the MRG segment in this case is strictly
6890   conventional and is not intended to communicate an actual merge.

Providers with an ongoing relationship with the patient may be communicated in ROL segments immediately following the PID/PD1 segments. Providers specific to an episode of care may be communicated in ROL segments immediately following the PV1/PV2 segments. Providers specific to a particular insurance carrier may be communicated in ROL segments immediately following the
6895   IN1/IN2/IN3 segments.

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.10.4 Expected actions

The receiver shall update the patient's class to "outpatient," and if necessary shall update the patient's
6900   location to the value in field *PV1-3-patient location*.

If the MRG segment is included, the receiver shall update the patient's account number from the value in *MRG-3-prior account number* to the value in *PID-18-patient account number*.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

6905   In case this Movement conflicts with the current situation of the patient (no active inpatient encounter is known for this patient, or the patient is unknown) the message is still processed and initiates a new outpatient encounter for a possibly new patient, and no error condition is raised.

If the receiver does not support the Inpatient/Outpatient Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

6910   ### 3.31.7.11   Transfer a Patient (ADT^A02^ADT_A02)

3.31.7.11.1 Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that a patient is being transferred from one location to another. The new location will be reflected in the institution's bed census.

6915   MSH-9 is valued **ADT^A02^ADT_A02**.

3.31.7.11.2 Message Static Definition

Table 3.31-17: Static definition of message ADT^A02^ADT_A02

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
PDA	Patient Death and Autopsy	O	[0..1]	3

3.31.7.11.3 Comments on segment usage

6920 The new patient location should appear in *PV1-3 - Assigned Patient Location* while the old patient location should appear in *PV1-6 - Prior Patient Location*.

Providers with an ongoing relationship with the patient may be communicated in ROL segments immediately following the PID/PD1 segments. Providers specific to an episode of care may be communicated in ROL segments immediately following the PV1/PV2 segments.

6925 One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

Segment DG1 should be used to communicate diagnosis information only if it is necessary to communicate with a receiver that is using a version of HL7 prior to V2.5.

3.31.7.11.4 Expected actions

The receiver shall update the patient's location to the value in field *PV1-3-patient location*.

6930 The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no active inpatient encounter is known for this patient, or the patient is unknown or the known patient location was not the one declared in PV1-6) the message is still processed, the new situation is registered (the encounter and the patient are
6935 created if needed) and no error condition is raised.

If the receiver does not support the Inpatient/Outpatient Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31.7.12 Cancel Transfer – ADT^A12^ADT_A12

3.31.7.12.1 Trigger Event

6940 This message is sent by a Patient Encounter Supplier to a Patient Encounter Consumer to cancel a previous notification (via trigger event A02) that a patient was being moved from one location to another.

MSH-9 is valued **ADT^A12^ADT_A12**.

3.31.7.12.2 Message Static Definition

6945 **Table 3.31-18: Static definition of message ADT^A12^ADT_A12**

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
DG1	Diagnosis Information	X	[0..0]	6

3.31.7.12.3 Comments on segment usage

Field *PV1-3-patient location* shall contain the patient's location prior to the transfer.

3.31.7.12.4 Expected actions

6950 The receiver shall reset the patient's location to the value in field *PV1-11-temporary location* or to the value in field *PV1-3-patient location*, as appropriate.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no transfer previously notified,
6955 or encounter unknown, or patient unknown) the message is discarded, and no error condition is raised.

If the receiver does not support the Inpatient/Outpatient Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

_____

3.31.7.13   Pending Admit (ADT^A14^ADT_A05)

6960   **3.31.7.13.1   Trigger Event**

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that it is planned to admit a patient.

MSH-9 is valued **ADT^A14^ADT_A05**.

3.31.7.13.2   Message Static Definition

6965   **Table 3.31-19: Static definition of message ADT^A14^ADT_A05**

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	X	[0..0]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6
UB2	Universal Bill 92 Information	O	[0..1]	6
PDA	Patient Death and Autopsy	O	[0..1]	3

_____

3.31.7.13.3 Comments on segment usage

Field *PV2-8-expected admit date/time* is used to carry the expected date and time when the patient is to be admitted.

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.13.4 Expected actions

The receiver shall update the patient's status to "pending admit".

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

There is no particular potential conflict between this Movement and any previously received message related to the same patient.

If the receiver does not support the Pending Event Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31.7.14 Cancel Pending Admit – ADT^A27^ADT_A21

3.31.7.14.1 Trigger Event

This message is sent by a Patient Encounter Supplier to a Patient Encounter Consumer to cancel a previous notification (via trigger event A14) that a patient was expected to be admitted.

MSH-9 is valued **ADT^A27^ADT_A21**.

3.31.7.14.2 Message Static Definition

Table 3.31-20: Static definition of message ADT^A27^ADT_A21

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7

3.31.7.14.3 Comments on segment usage

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.14.4 Expected actions

6990 The receiver shall reset the patient's status to its value prior to the receipt of the "pending admit" message.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no pending admit previously
6995 notified, or patient unknown) the message is discarded, and no error condition is raised.

If the receiver does not support the Pending Event Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31.7.15   Pending Transfer (ADT^A15^ADT_A15)

3.31.7.15.1 Trigger Event

7000 This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that it is planned to transfer a patient.

MSH-9 is valued **ADT^A15^ADT_A15**.

3.31.7.15.2 Message Static Definition

Table 3.31-21: Static definition of message ADT^A15^ADT_A15

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
DG1	Diagnosis Information	O	[0..*]	6

7005 ### 3.31.7.15.3 Comments on segment usage

Providers with an ongoing relationship may be communicated in ROL segments immediately following the PID/PD1 segments. Providers specific to an episode of care may be communicated in ROL segments immediately following the PV1/PV2 segments.

One or more OBX segments may be present to carry "permanent observations" such as the patient
7010 weight or height.

Segment DG1 should be used to communicate diagnosis information only if it is necessary to communicate with a receiver that is using a version of HL7 prior to V2.5.

The planned date for this pending transfer is given in field EVN-3 of segment EVN. See section 3.30.5.2.

3.31.7.15.4 Expected actions

The receiver shall record that a transfer is pending for this patient.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no active inpatient encounter, or patient unknown) the message is discarded, and no error condition is raised.

If the receiver does not support the Pending Event Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31.7.16   Cancel Pending Transfer – ADT^A26^ADT_A21

3.31.7.16.1 Trigger Event

This message is sent by a Patient Encounter Supplier to a Patient Encounter Consumer to cancel a previous notification (via trigger event A25) that it was planned to transfer a patient.

MSH-9 is valued **ADT^A26^ADT_A21**.

3.31.7.16.2 Message Static Definition

Table 3.31-22: Static definition of message ADT^A26^ADT_A21

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7

3.31.7.16.3 Comments on segment usage

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

The planned date for the pending transfer that is cancelled, is given in field EVN-3 of segment EVN. See section 3.30.5.2.

3.31.7.16.4 Expected actions

The receiver shall reset the patient's status to the value immediately before the Pending Transfer message was received.

_____

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

7040 In case this Movement conflicts with the current situation of the patient (no pending transfer known, or no active inpatient encounter, or patient unknown) the message is discarded, and no error condition is raised.

If the receiver does not support the Pending Event Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

7045 ### 3.31.7.17 Pending Discharge (ADT^A16^ADT_A16)

3.31.7.17.1 Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that it is planned to discharge a patient.

MSH-9 is valued **ADT^A16^ADT_A16**.

7050 ### 3.31.7.17.2 Message Static Definition

Table 3.31-23: Static definition of message ADT^A16^ADT_A16

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	RE	[0..1]	3
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6

_____

ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6

3.31.7.17.3 Comments on segment usage

Field *PV2-9-expected discharge date/time* is used to carry the expected date and time when the patient is to be discharged.

7055 One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.17.4 Expected actions

The receiver shall update the patient's status to "pending discharge".

The receiver shall report the result of this operation (success / error) in an acknowledgment message
7060 returned to the sender.

In case this Movement conflicts with the current situation of the patient (no active inpatient encounter, or patient unknown) the message is discarded, and no error condition is raised.

If the receiver does not support the Pending Event Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

7065 ## 3.31.7.18   Cancel Pending Discharge – ADT^A25^ADT_A21

3.31.7.18.1 Trigger Event

This message is sent by a Patient Encounter Supplier to a Patient Encounter Consumer to cancel a previous notification (via trigger event A16) that a patient was expected to be discharged.

MSH-9 is valued **ADT^A25^ADT_A21**.

7070 ### 3.31.7.18.2 Message Static Definition

Table 3.31-24: Static definition of message ADT^A25^ADT_A21

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7

3.31.7.18.3   Comments on segment usage

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.18.4   Expected actions

The receiver shall reset the patient's status to its value prior to the receipt of the "pending discharge" message.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no pending discharge known, or no active inpatient encounter, or patient unknown) the message is discarded, and no error condition is raised.

If the receiver does not support the Pending Event Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31.7.19   Change Attending Doctor – ADT^A54^ADT_A54

3.31.7.19.1   Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that there has been a change in the doctor responsible for the patient's treatment.

MSH-9 is valued **ADT^A54^ADT_A54**.

3.31.7.19.2   Message Static Definition

Table 3.31-25: Static definition of message ADT^A54^ADT_A54

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
ROL	Role	O	[0..*]	15

3.31.7.19.3   Comments on segment usage

Field *PV1-7-attending doctor* shall contain the new attending doctor.

Providers with an ongoing relationship may be communicated in ROL segments immediately following the PID/PD1 segments. Providers specific to an episode of care may be communicated in ROL segments immediately following the PV1/PV2 segments.

_____

Field *ROL-4-role begin date/time* and *ROL-5-role end date/time* are used to communicate the begin and end date and time of the attending doctor (or of the admitting, consulting, and/or referring doctor, as appropriate and as designated in *ROL-7-role code*). When segment ROL is used to communicate this
7100   information, field *ROL-2-action code* should be valued UP.

3.31.7.19.4 Expected actions

The receiver shall record the patient's new attending doctor.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

7105   In case this Movement conflicts with the current situation of the patient (no active inpatient or outpatient encounter, or patient unknown) the message is discarded, but no error condition is raised. If the receiver does not support the Advanced Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31.7.20   Cancel Change Attending Doctor – ADT^A55^ADT_A52

7110   ### 3.31.7.20.1 Trigger Event

This message is sent by a Patient Encounter Supplier to cancel a previous notification to a Patient Encounter Consumer of a change to the patient's attending doctor.

MSH-9 is valued **ADT^A55^ADT_A52**.

3.31.7.20.2 Message Static Definition

7115   **Table 3.31-26: Static definition of message ADT^A55^ADT_A52**

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3

3.31.7.20.3 Comments on segment usage

Field *PV1-7-attending doctor* shall contain the patient's attending doctor prior to the notification of change.

3.31.7.20.4 Expected actions

7120   The receiver shall reset the patient's attending doctor to the value in field *PV1-7-attending doctor*.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

_____

In case this Movement conflicts with the current situation of the patient (no active inpatient or outpatient encounter, or patient unknown) the message is discarded, but no error condition is raised.

7125   If the receiver does not support the Advanced Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31.7.21   Patient Goes on a Leave of Absence – ADT^A21^ADT_A21

3.31.7.21.1 Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that a
7130   patient has left the healthcare institution temporarily.

MSH-9 is valued **ADT^A21^ADT_A21**.

3.31.7.21.2 Message Static Definition

Table 3.31-27: Static definition of message ADT^A21^ADT_A21

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7

3.31.7.21.3 Comments on segment usage

7135   Field *EVN-6-event occurred* shall contain the date and time that the patient actually left the institution. *PV2-47-expected LOA return* shall contain the date and time that the patient is expected to return from the leave of absence.

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

7140   ### 3.31.7.21.4 Expected actions

The receiver shall record that the patient has left the institution on a leave of absence.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no active encounter, or patient
7145   unknown) the message is discarded, but no error condition is raised.

If the receiver does not support the Advanced Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31.7.22 Cancel Leave of Absence for a Patient – ADT^A52^ADT_A52

3.31.7.22.1 Trigger Event

7150 This message is sent by a Patient Encounter Supplier to cancel a previous notification to a Patient Encounter Consumer that a patient had left the healthcare institution temporarily.

MSH-9 is valued **ADT^A52^ADT_A52.**

3.31.7.22.2 Message Static Definition

Table 3.31-28: Static definition of message ADT^A52^ADT_A52

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3

7155 #### 3.31.7.22.3 Comments on segment usage

Field *EVN-6-event occurred* shall contain the date and time that the leave of absence was cancelled.

3.31.7.22.4 Expected actions

The receiver shall cancel the patient's leave of absence.

The receiver shall report the result of this operation (success / error) in an acknowledgment message
7160 returned to the sender.

In case this Movement conflicts with the current situation of the patient (no leave of absence previously notified, or no active encounter, or patient unknown) the message is discarded, but no error condition is raised.

If the receiver does not support the Advanced Encounter Management option of this transaction, it shall
7165 application-reject the message (see Appendix C.2.3).

3.31.7.23 Patient Returns from a Leave of Absence – ADT^A22^ADT_A21

3.31.7.23.1 Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that a patient has returned from a leave of absence.

7170 MSH-9 is valued **ADT^A22^ADT_A21**.

___

3.31.7.23.2 Message Static Definition

Table 3.31-29: Static definition of message ADT^A22^ADT_A21

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7

3.31.7.23.3 Comments on segment usage

Field *EVN-6-event occurred* shall contain the date and time that the patient actually returned from the leave of absence. *PV2-47-expected LOA return* shall contain the date and time that the patient was expected to return from the leave of absence.

One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.23.4 Expected actions

The receiver shall record that the patient has returned from the leave of absence.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no leave of absence previously notified, or no active encounter, or patient unknown) the message is discarded, but no error condition is raised.

If the receiver does not support the Advanced Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

3.31.7.24 Cancel Patient Return from a Leave of Absence – ADT^A53^ADT_A52

3.31.7.24.1 Trigger Event

This message is sent by a Patient Encounter Supplier to cancel a previous notification to a Patient Encounter Consumer that a patient had returned from a leave of absence.

MSH-9 is valued **ADT^A53^ADT_A52**.

3.31.7.24.2 Message Static Definition

7195
Table 3.31-30: Static definition of message ADT^A53^ADT_A52

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3

3.31.7.24.3 Comments on segment usage

Field *EVN-6-event occurred* shall contain the date and time that the return from leave of absence was cancelled. *PV2-47-expected LOA return* shall contain the date and time that the patient is expected to return from the leave of absence.

7200 ### 3.31.7.24.4 Expected actions

The receiver shall cancel the patient's return from leave of absence.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this Movement conflicts with the current situation of the patient (no return from leave of absence
7205 previously notified, or no active encounter, or patient unknown) the message is discarded, but no error condition is raised.

If the receiver does not support the Advanced Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

7210 ## 3.31.7.25 Move account information – ADT^A44^ADT_A43

3.31.7.25.1 Trigger Event

This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that an account previously associated with one patient is now associated with another patient.

MSH-9 is valued **ADT^A44^ADT_A43**.

7215 ### 3.31.7.25.2 Message Static Definition

Table 3.31-31: Static definition of message ADT^A44^ADT_A43

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2

Segment	Meaning	Usage	Card.	HL7 chapter
---	--- PATIENT begin	R	[1..*]	
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
MRG	Merge Information	R	[1..1]	3
---	--- PATIENT end			

3.31.7.25.3 Comments on segment usage

None.

3.31.7.25.4 Expected actions

7220 The receiver shall associate the account in *MRG-3-prior patient account number* with the patient in *PID-3-patient identifier list*, and shall remove associations of that account with the patient in *MRG-1-prior patient identifier list*.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

7225 In case this message conflicts with the current situation (account unknown or supplier patient unknown) the message is discarded, but no error condition is raised.

If the receiver does not support the Advanced Encounter Management option of this transaction, it shall application-reject the message (see Appendix C.2.3).

7230

3.31.7.26   Patient Departing – Tracking (ADT^A09^ADT_A09)

3.31.7.26.1 Trigger Event

This message is only used within the context of the "Temporary Patient Transfers Tracking" option.

7235 This message is sent by a Patient Encounter Supplier to notify a Patient Encounter Consumer that a patient has departed a location without the patient's official bed census location having changed. The HL7 standard describes three situations that qualify as non-census location changes: (a) patient tracking (i.e., pre-notification before an official transfer), (b) the patient is in transit between locations for some time, (c) a notification of temporary location change. This IHE transaction only uses the latter: notification of temporary location change.

7240 MSH-9 is valued **ADT^A09^ADT_A09**.

3.31.7.26.2 Message Static Definition

Table 3.31-32: Static definition of message ADT^A09^ADT_A09

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2

Segment	Meaning	Usage	Card.	HL7 chapter
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
DG1	Diagnosis Information	O	[0..*]	6

3.31.7.26.3   Comments on segment usage

If the patient has left for a non-temporary location (tracking), then field *PV1-3-patient location* shall
contain the patient's new location and field *PV1-6-prior patient location* shall contain the patient's old
location.

If the patient will be in transit for some time, then field *PV1-42-pending location* shall contain the new
location and field *PV1-6-prior patient location* shall contain the patient's old location.

If the patient is moving to a temporary location, then field *PV1-11-temporary location* shall contain the
new temporary location. If the patient is moving from a temporary location, then field *PV1-43-prior
temporary location* shall contain the old temporary location. If the patient is moving from a permanent
location, then field *PV1-6-prior patient location* shall contain the old permanent location.

One or more OBX segments may be present to carry "permanent observations" such as the patient
weight or height.

Segment DG1 should be used to communicate diagnosis information only if it is necessary to
communicate with a receiver that is using a version of HL7 prior to V2.5.

3.31.7.26.4   Expected actions

The receiver shall reset the patient's location to the value in field *PV1-11-temporary location*, field *PV1-
42-pending location*, or field *PV1-3-patient location*, as appropriate.

The receiver shall report the result of this operation (success / error) in an acknowledgment message
returned to the sender.

In case this message conflicts with the current situation the message is discarded, but no error condition
is raised.

If the receiver does not support the Temporary Patient Location Tracking option of this transaction, it
shall application-reject the message (see Appendix C.2.3).

3.31.7.27   Cancel Patient Departing – Tracking – ADT^A33^ADT_A21

3.31.7.27.1   Trigger Event

This message is only used within the context of the "Temporary Patient Transfers Tracking" option.
This message is sent by a Patient Encounter Supplier to a Patient Encounter Consumer to cancel a

7270 previous notification (via trigger event A09) that a patient has departed a location without the patient's official bed census location having changed.

MSH-9 is valued **ADT^A33^ADT_A21**.

3.31.7.27.2 Message Static Definition

Table 3.31-33: Static definition of message ADT^A33^ADT_A21

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7

7275 3.31.7.27.3 Comments on segment usage

If the patient was in a non-temporary location, then field *PV1-3-patient location* shall contain the patient's location prior to the erroneous A09 event. If the patient was in a temporary location, then field *PV1-11-temporary location* shall contain the patient's location prior to the erroneous A09 event.

One or more OBX segments may be present to carry "permanent observations" such as the patient
7280 weight or height.

3.31.7.27.4 Expected actions

The receiver shall reset the patient's location to the value in field *PV1-11-temporary location* or to the value in field *PV1-3-patient location*, as appropriate.

The receiver shall report the result of this operation (success / error) in an acknowledgment message
7285 returned to the sender.

In case this message conflicts with the current situation the message is discarded, but no error condition is raised.

If the receiver does not support the Temporary Patient Location Tracking option of this transaction, it shall application-reject the message (see Appendix C.2.3).

7290 3.31.7.28   Patient Arriving – Tracking – ADT^A10^ADT_A09

3.31.7.28.1 Trigger Event

This message is only used within the context of the "Temporary Patient Transfers Tracking" option.

This message is sent by a Patient Encounter Supplier to a Patient Encounter Consumer as a notification that a patient has arrived at a new location without the patient's official bed census location having
7295 changed. The HL7 standard describes three varieties of these non-census location changes involving

three different kinds of notification: (a) an unofficial notification of location change prior to the official notification of patient tracking, (b) the patient is in transit between locations for some time, (c) a notification of a temporary location change. This IHE transaction only uses the latter: notification of temporary location change.

7300   MSH-9 is valued **ADT^A10^ADT_A09**.

3.31.7.28.2   Message Static Definition

Table 3.31-34: Static definition of message ADT^A10^ADT_A09

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
DG1	Diagnosis Information	X	[0..0]	6

3.31.7.28.3   Comments on segment usage

If the patient is arriving at a temporary location, field *PV1-11-temporary location* shall indicate this
7305   temporary location. If the patient is moving from one temporary location to another, then field *PV1-43-prior temporary location* may also be used.

If the patient is arriving at a permanent location from a temporary location, field *PV1-3-patient location* shall be used for the new location and field *PV1-43-prior temporary location* shall be used for the old location.

7310   One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.28.4   Expected actions

The receiver shall update the patient's location to the value in field *PV1-11-temporary location* or to the value in field *PV1-3-patient location*, as appropriate.

7315   The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this message conflicts with the current situation the message is discarded, but no error condition is raised.

If the receiver does not support the Temporary Patient Location Tracking option of this transaction, it
7320   shall application-reject the message (see Appendix C.2.3).

_____

3.31.7.29   Cancel Patient Arriving – Tracking – ADT^A32^ADT_A21

3.31.7.29.1 Trigger Event

This message is sent by a Patient Encounter Supplier to a Patient Encounter Consumer to cancel a previous notification (via trigger event A10) that a patient arrived at a location without the patient's
7325   official bed census location having changed, as for example when the patient arrives at a diagnostic or treatment service.

MSH-9 is valued **ADT^A32^ADT_A21**.

3.31.7.29.2 Message Static Definition

Table 3.31-35: Static definition of message ADT^A32^ADT_A21

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7

7330   #### 3.31.7.29.3 Comments on segment usage

If the patient was in a non-temporary location, then field *PV1-3 - Assigned Patient Location* may contain (if known) the original patient location prior to the erroneous A10 (patient arriving-tracking) event. If the patient was in a temporary location, then field *PV1-11 - Temporary Location* may contain (if known) the original patient location prior to the erroneous A10 (patient arriving-tracking) event.

7335   One or more OBX segments may be present to carry "permanent observations" such as the patient weight or height.

3.31.7.29.4 Expected actions

If field *PV1-3 - Assigned Patient Location* is populated, the receiver shall reset the patient's permanent location to the value contained in that field. If field *PV1-11 - Temporary Location* is populated, the
7340   receiver shall reset the patient's permanent location to the value contained in that field.

The receiver shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

In case this message conflicts with the current situation the message is discarded, but no error condition is raised.

7345   If the receiver does not support the Temporary Patient Location Tracking option of this transaction, it shall application-reject the message (see Appendix C.2.3).

_____

3.31.7.30 Update Patient Movement Information – ADT^Z99^ADT_A01

3.31.7.30.1 Trigger Event

This message is only used within the context of the "Historic Movement Management" option.

7350   It is sent by a Patient Encounter Supplier to a Patient Encounter Consumer to communicate an update of a Movement, which can be the current Movement or a historic one.

MSH-9 is valued **ADT^Z99^ADT_A01**.

3.31.7.30.2 Message Static Definition

Table 3.31-36: Static definition of message ADT^Z99^ADT_A01

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
ROL	Role	O	[0..*]	15
NK1	Next of Kin / Associated Parties	O	[0..*]	3
PV1	Patient Visit	R	[1..1]	3
PV2	Patient Visit – Additional Info	O	[0..1]	3
ZBE	Movement segment	R	[1..1]	
ROL	Role	O	[0..*]	15
DB1	Disability Information	O	[0..*]	3
OBX	Observation/Result	O	[0..*]	7
AL1	Allergy Information	O	[0..*]	3
DG1	Diagnosis Information	O	[0..*]	6
DRG	Diagnosis Related Group	O	[0..1]	6
---	--- PROCEDURE begin	O	[0..*]	
PR1	Procedures	R	[1..1]	6
ROL	Role	O	[0..*]	15
---	--- PROCEDURE end			
GT1	Guarantor	O	[0..*]	6
---	--- INSURANCE begin	O	[0..*]	
IN1	Insurance	R	[1..1]	6
IN2	Insurance Additional Info.	O	[0..1]	6
IN3	Insurance Additional Info - Cert.	O	[0..1]	6
ROL	Role	O	[0..*]	15
---	--- INSURANCE end			
ACC	Accident Information	O	[0..1]	6
UB1	Universal Bill Information	O	[0..1]	6
UB2	Universal Bill 92 Information	O	[0..1]	6
PDA	Patient Death and Autopsy	O	[0..1]	3

3.31.7.30.3 Comments on segment usage

The ZBE segment is mandatory in this message. See the description of this segment in section 3.31.6.1.

3.31.7.30.4 Expected actions

Otherwise, the receiver shall update the Movement in its database, and shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

If the receiver does not know the Movement to be updated (identified by ZBE-3 in the ZBE segment), it discards the message and raises an error condition.

A receiver not supporting the Historic Movement Management option shall application-reject the message (see Appendix C.2.3).

3.31.7.31 Merge two patients - ADT^A40^ADT_A39

3.31.7.31.1 Trigger Event

The Patient Encounter Supplier notifies the merge of records for a patient that was incorrectly filed under two different identifiers. This message is only used to merge two patient identifiers of the same type, or two lists of patient identifiers, . It is not supposed to update other patient demographics information. The A08 trigger event should be used for this purpose.

MSH-9 is valued **ADT^A40^ADT_A39**.

3.31.7.31.2 Message Static Definition

Table 3.31-37: Static definition of message ADT^Z40^ADT_A39

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
SFT	Software Segment	O	[0..*]	2
EVN	Event Type	R	[1..1]	2
---	--- PATIENT begin	R	[1..1]	
PID	Patient Identification	R	[1..1]	3
PD1	Additional Demographics	O	[0..1]	3
MRG	Merge Information	R	[1..1]	3
PV1	Patient Visit	X	[0..0]	3

3.31.7.31.3 Comments on segment usage

This profile makes unrepeatable the PATIENT segment group: The message can communicate only one merge operation for one patient.

The "incorrect supplier identifier" identified in the MRG segment (*MRG-1-Prior Patient Identifier List*) is to be merged with the required "correct target identifier" of the same "identifier type code" component identified in the PID segment (*PID-3-Patient Identifier List*). The "incorrect supplier identifier" would then logically never be referenced in future transactions.

The PV1 segment is not supported by IHE in this message.

3.31.7.31.4   Expected actions

The receiver shall merge the two patients in its data base, and shall report the result of this operation (success / error) in an acknowledgment message returned to the sender.

7385   If the receiver does not recognize the target patient identifiers, it shall perform a Change Patient Identifier List instead of a Merge.

If the receiver does not recognize the supplier patient identifiers to be merged, it shall take no action. This situation is not an error.


7390   ## 3.32 Distribute Document Set on Media

This section corresponds to Transaction ITI-32 of the IHE Technical Framework. Transaction ITI-32 is used by the Portable Media Creator to create the media content and by Portable Media Importer to read the media content.

3.32.1 Scope

7395   In the Distribute Document Set on Media transaction the Portable Media Creator sends information to media reading actors by means of Interchange Media where it stores the information.

3.32.2 Use Case Roles
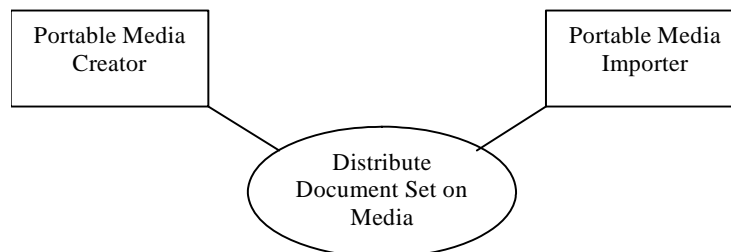
Actor: Portable Media Creator

7400   **Role:** Assemble the media content and store it on the media to be distributed.

Actor: Portable Media Importer

Role: Read the Document Submission Set content of distributed media in order to access the document(s) and the relevant metadata and perform import of the documents on the media.

3.32.3 Referenced Standard

7405   DICOM PS 3.10 Media Storage and File Format for Data Interchange (DICOM file format). http://dicom.nema.org/

DICOM PS 3.12 Media Formats and Physical Media for Data Interchange, Annex F - 120mm CD-R media, Annex R - USB Connected Removable Devices, Annex V - ZIP File Over Media, and Annex W - Email Media. http://dicom.nema.org/

7410   XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition). A Reformulation of HTML 4 in XML 1.0. W3C Recommendation 26 January 2000, revised 1 August 2002. http://www.w3.org/TR/xhtml1.

XHTML™ Basic. W3C Recommendation 19 December 2000. http://www.w3.org/TR/xhtm-basic.

MDN: RFC 3798 Message Disposition Notification. http://www.rfc-editor.org/rfc/rfc3798.txt

7415

3.32.4 Interaction Diagram
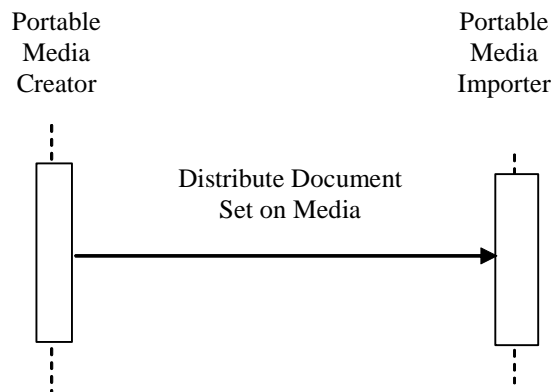
3.32.4.1 Distribute Document Set on Media

This transaction defines the interchange of XDS document submission sets on media. It specifies the requirements for a directory structure, and the physical media where stored.
7420

The file directory structure restrictions and file organization are specified below. These are based on industry standard file systems with restrictions chosen based on experience with demonstrated interoperability in the field of reliable exchange. These are defined in Part 10 of the DICOM standard and summarized below.

7425   The media that are supported are:

- CD-R media. The physical media specification used for the storage on CD-R is a restricted subset of the widely used CD-R media. The restrictions were chosen to ensure interoperability and media reliability. The standard directory and file structure can be recorded to the CD-R media by widely available software, but this software must be set to comply with the interoperability restrictions on
7430   recording format. This media specification relies on the healthcare experience gained by CD-R media widely used in radiology and cardiology. It is defined by Annex F in Part 12 of the DICOM standard and is also used in the IHE Radiology PDI profile for the interchange of images,

- USB Removable Devices. This media specification encompasses a wide range of USB connected flash media, removable storage devices, etc. The standard directory and file structure can be
7435   recorded onto any of these media by any system that supports the USB Removable Device type defined by the USB Implementers Forum. This specification is defined in Annex R in Part 12 of the DICOM standard.

- Email transport of ZIP files. This media specification defines the encoding of the directory and file structure as an ordinary ZIP file (maintaining the directory structure) and attaches that ZIP file to an

7440   email message. Some additional constraints are added to the email message header to facilitate recognizing the message. This specification is defined in the annexes to part 12 of the DICOM standard called: ZIP File Media and Email media. . The ZIP over Email Response option enables the Portable Media Importer to send an acknowledgment message to the Portable Media Importer.

3.32.4.1.1 Trigger Events

The user at the Portable Media Creator wishes to transport information by the creation and transport of interchange media. The Portable Media Creator assembles the Interchange Media content and stores it on the media.

If the ZIP over Email Response option is supported, the Portable Media Importer shall detect whether
7450   the Import was successful or not.

3.32.4.1.2 Message Semantics

The message semantics of this transaction are described in terms of content specifications for the media.

The Portable Media Creator shall be able to include one or multiple Submission Set(s), including document(s) and associated metadata. Additionally it shall include a ***README.TXT*** file and an
7455   ***INDEX.HTM*** and associated files for use to display the media content using a simple browser. It may include other files and directories that the Portable Media Importer will ignore.

3.32.4.1.2.1 Media File system and File Naming Restrictions

The following restrictions are needed to ensure broad interoperability:

- Strict ISO 9660 Level 1 compliance for filenames and directories, even on non-CDR media.
7460 - Strict ISO 9660 Level 1 compliance for recording methods on CDR media. This means no packet writing.
- Filenames should not be in lower case, nor have lower case equivalent file names encoded as Joliet or Rock Ridge extensions to the ISO 9660 file system.
- Only file and folder names referenced by the DICOMDIR file are restricted to 8 characters with no
7465   extension. Specifically, it is not permitted to name DICOM files based on their SOP Instance UID, since that would exceed the 8 character limit and use the illegal period character, and it is not permitted to add a ".dcm" extension or similar.

    Note: Refer to RAD TF-3: Appendix E of the IHE Radiology Technical Framework for a reference to common implementation misinterpretations and/or errors that are detrimental to interoperability.

7470 **3.32.4.1.2.2 Content Organization Overview**
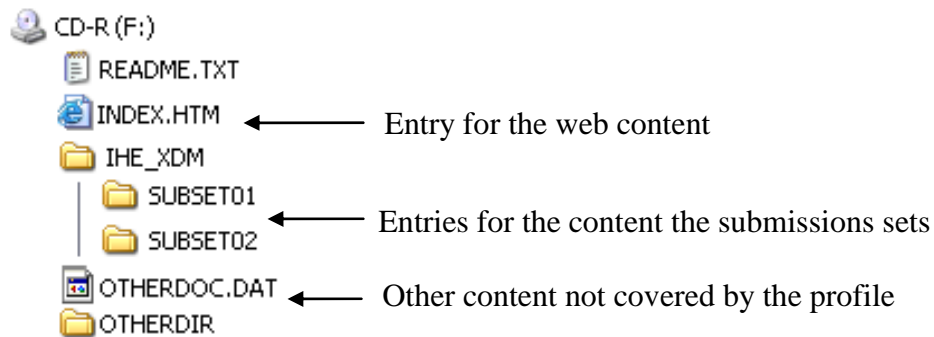
Figure 3.32.4.1-1 General structure of the media

The media shall contain at the "root" directory level, as shown in the figure above:

- An IHE_XDM directory.
7475 - Two files for helping to access the content of the media: *README.TXT* and *INDEX.HTM*
- An Autorun file or equivalent shall not be present in the root directory. Executable files may be present, but shall not be configured to start automatically.

As shown in the figure above, the *IHE_XDM* directory shall contain one sub-directory per submission set included on the media.

7480 There may be other files present on the media for other purposes, (e.g., use in compliance with the IHE Radiology PDI profile). The presence or absence of these files shall not affect performance of this transaction.
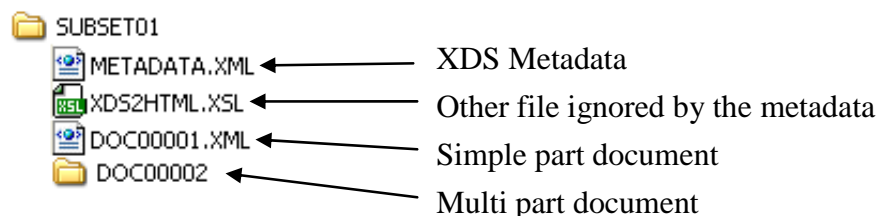
Figure 3.32.4.1-2 Structure of a submission set directory on the media

7485 As shown on the figure above, each submission set directory shall contain:

- A *METADATA.XML* file containing the XDS Registry metadata, as described in the section 4.1.7 Document Definition Metadata of the ITI TF-2 document. This shall include all of the metadata that is specified for a Register Document Set [ITI-14] or Register Document Set-b [ITI-42]. This may include XDSFolder objects, associations, and other metadata contents.
7490 There is no relationship between an XDSFolder and a media directory, although some people do call media directories "folders". The metadata for the submission set shall include unique and different submissionTime.

- One file for each "simple part" document referenced in the metadata as an XDSDocumentEntry
7495 - One sub-directory for each "multipart" document referenced in the metadata as an XDSDocumentEntry (see table 4.1-5, attribute mimeType set to "multipart/related")

- Potentially other files and directories that are ignored by the Portable Media Importer

The "multipart" document shall be structured as one sub-directory containing all the parts as file, including the "start" part corresponding to the main file to be open by the "multipart" document viewer.
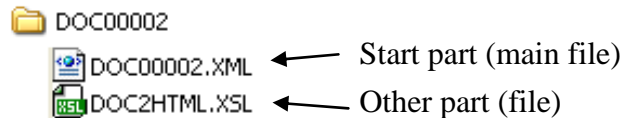7500 An example of "multipart" document is shown in the figure 3.32.4.1-3.

Figure 3.32.4.1-3 Structure on the media of a directory which is functionally equivalent to a "XDS multipart document"

The URI element of the metadata describing a file that is present on this media shall point to the file
7505 containing the document, through a relative URL which corresponds to the file name for simple part document and to the concatenation of the sub-directory and the main file name for "multipart" document (e.g. DOC00002/DOC00002.XML). Note that in cases where the files are not located within this media directory for the Submission Set, it is possible that the relative URL may begin with "../" so that a single copy the document can be present for multiple purposes.

7510 In Figure 3.32.4.1-2, the METADATA.XML file of the Submission Set stored in the SUBSET01 directory will contain many XDSDocumentEntry objects having their elements set as follows (see table 4.1-5, URI attribute for details):

```
<ExtrinsicObject id="Document1" mimeType="text/xml"... (with URI set to
"DOC00001.XML")
7515            <ExtrinsicObject id="Document2" mimeType="text/xml"... (with URI set to
"DOC00002/DOC00002.XML")
```

The file named *INDEX.HTM* in the root directory shall be encoded in compliance with the XHTML Basic recommendation from W3C. It may contain a description of the submission sets, including especially:

7520
- Patient ID and demographics
- Source Facility information

Note: XDM Distribute Document Set on Media Transaction does not require that all the submission sets included in the media are relative to the same patient.

It may also describe other content which is on the media, including the means to launch any executable
7525 that may be present on the media.

There shall also be a *README.TXT* file located in the root directory, that shall contain:

- Contact information regarding the Institution that created the media.
- Information regarding the Application that created the media.
    - Name of the product application and software version
7530   - Contact information of the vendor of the application that created the media
- General information about the overall organization of the interchange media. This is not intended to be specific to the content stored on this instance of interchange media, which if necessary should be placed in the *INDEX.HTM* file.
- Information regarding the Media Viewer application (if a Media Viewer is contained)

7535   -   Operating system(s) supported

                    -   Name of the product application and software version

                    -   Contact information of vendor that provided the Media Viewer application

                    -   Disclaimer statement about the intended usage of the application

                    -   List of minimum requirements

7540   -   Additional information regarding the usage of the application

Note that generally the *README.TXT* file is independent of the clinical content of the media, i.e. the same *README.TXT* may be included on all media created by that application at that institution. Experience has shown that this kind of *README.TXT* file is very valuable for resolving problems.

In addition, if the Portable Media Creator implements support for the Web Content Option of the PDI
7545 Profile then the *INDEX.HTM* file must meet the requirements of the PDI Profile Web Content Option.

The *INDEX.HTM* file located in the root directory shall contain:

- An informative header containing:
- Identification of the institution that created the interchange media
- Optionally, a disclaimer statement about privacy/security from the institution that created the
7550   interchange media
- a link to an entry point for accessing the web content of the IHE_PDI directory
- a link to the *README.TXT* file
- a link to additional non-constrained data (if it exists)
- a manifest which lists the data that can be imported by a Portable Media Importer Actor. (i.e.,
7555   all DICOM content on the media)
- a manifest which lists any patient-related data contained on the CD that cannot be imported (i.e., additional non-constrained content that doesn't have an importable DICOM equivalent on the media).
- a link to a launch point for a DICOM viewer, if present on the interchange media

7560

3.32.4.1.2.3 Response message

If the ZIP over Email Response option is supported and a response was requested, the Portable Media Importer shall send a response, based on the [MDN] mechanism, depending of the success of the Import operation:

7565   - Success: the MDN "disposition-type" field is set to "displayed"
- Error: the MDN "disposition-type" field is set to "deleted" and the MDN "disposition-modifier" is set to "Error: xxxx" where "xxxx" is the text detailing the error.

Note 1:   Older implementations of MDN might use "processed" instead of "display". The current RFC has removed this option but Portable Media Creator should be prepared to receive it. If they receive it, they have to look in the error field to see whether
7570   there is an error.

Note 2:   The general mechanism for use of eMail is described in the Appendix T (Informative)

3.32.4.1.3 Media Identification

The Portable Media Creator actor may add a human-readable identification on the outside of the physical medium, reflecting the originating institution, the time of the creation and content of the media. 7575   The method of media marking is outside the scope of this integration profile.

If the ZIP over Email Response option is supported, Portable Media Creator shall be configurable to include in its message header the request for a response:

- "Disposition-Notification-To:", followed by the email address to which Portable Media Importer shall send the response

7580   Then, the Portable Media Importer shall acknowledge this operation by sending a MDN response to the email address included in the message.

And finally, the Portable Media Creator shall consider that the import is successful unless:

- the disposition-modifier contains the word "error" or "failure", case insensitive.

Note: This profile does not specify how errors should be processed because the variety of appropriate 7585   responses is too great.

In the case the media used is the ZIP file over Email, the subject line shall contain the phrase:

- XDM/1.0/DDM

    Note: In case the same Email complies also with the DICOM Email, it is recommended that the subject contains the phrase:
    XDM/1.0/DDM+DICOM-ZIP

7590   ### 3.32.4.1.4 Expected Actions

The Portable Media Importer shall verify the integrity of the media by comparing their size and hash with the value of the corresponding entries in the METADATA.XML file of the relevant submission set directory. Mismatching documents shall be indicated to the user. Media faults shall be indicated to the user.

7595   The hash and the size of a "multipart" document implemented as a sub-directory containing the different "part" files, shall be calculated as described in the Register Document Set transaction [ITI-14] for multipart documents. See Open Issues Section 2.3.

The Portable Media Importer shall be grouped with a Content Consumer of one or more IHE Content Profiles.   This other actor performs some form of processing of medical data. When the Portable Media 7600   Importer is grouped with another processing actor, that actor shall be able to perform its processing on the documents it is designed to support.

    Note: This awkward phrasing means that an ability of process data on portable media is described by saying that the processing
    actor is grouped with a Portable Media Importer actor.

3.32.2.1.1.1 Basic Patient Privacy Enforcement Option

7605   If the Basic Patient Privacy Enforcement Option is implemented:

1. The Portable Media Creator actor shall populate the confidentialityCode in the document metadata with the list of Patient Privacy Consent Policy Identifiers (OID) values that identify the

Patient Privacy Consent Policies that apply to the associated document. All documents submitted shall have confidentiality codes. The confidentiality codes for different documents in the same submission may be different.

2. The Portable Media Creator actor shall be able to be configured with the Patient Privacy Consent Policies, Patient Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the policies. The details of this are product specific and not specified by IHE.

3. The Portable Media Creator actor may have user interface or business rule capabilities to determine the appropriate confidentiality codes for each document. The details of this are product specific and not specified by IHE.

4. The Portable Media Importer actor shall be able to be configured with the Patient Privacy Consent Policies, Patient Privacy Consent Policy Identifiers (OIDs) and associated information necessary to understand and enforce the policies. The meanings of the codes on the media must be provided out of band, e.g., by telephone, fax, or email. The detail of how this is done is product specific and not specified by IHE. If the documents are transferred internally within the organization or to other members of the recipient's affinity domain, appropriate internal confidentiality codes shall be applied.

5. The Portable Media Creator actor shall be able to publish the consent documents and any applicable digital signatures that apply to the collection of content that it has created on portable media.

6. The Portable Media Importer actor shall have the ability to coerce the confidentiality code in the metadata associated with the document from the codes used by the Exporter to the codes used by the Importer.

The Portable Media Importer actor shall abide by the XDS Affinity Domain Policies represented by the confidentialityCode in the metadata associated with the document. The Portable Media Creator actor likely will have user access controls or business rule capabilities to determine the details of how confidentiality codes apply to query results. The details of this are product specific and not specified by IHE. These rules shall reduce the query results to only those that are appropriate to the current situation for that actor and user.

3.32.4.1.5 Security considerations

In the case of physical media, encryption of the CD-R or USB shall not be used.

In the case the media used is the ZIP file over Email, the transaction shall be secured by S/MIME (see IHE ATNA) and comply with the security process as defined in the DICOM Part 15 Appendix (Secure Use of ZIP File Media over Email). The security process requires the use of S/MIME to both encrypt and sign the message. The encryption is used to maintain confidentiality during the transport. The signature is used to maintain integrity during transport and indicates that the sender is authorized to send the message.

Portable Media Creators that create media shall generate one or more ATNA "Export" events into the audit trail to describe the media creation event. These events shall describe each submission set and/or study that is exported.

___

Portable Media Importers that import media shall generate one or more ATNA "Import" events into the audit trail to describe the media import event. These events shall describe each submission set and/or study that is imported.

7650

> Note: It is easy to build a partial implementation of actors in the XDM profile that lack the auditing capability. For example, a person can manually create media that comply with the requirements of the XDM media. It is possible that the manual process omits the generation of audit records for their activity. This would not be a compliant or complete implementation of the actors, but it is easy to make this kind of mistake.

7655 The Portable Media Importer shall check the hash value and size as found in the XDS metadata to detect corruption within the metadata or media. The Portable Media Importer shall notify the user if any errors are detected.

3.33 Intentionally Left Blank

3.34 Intentionally Left Blank

7660 ## 3.35 Intentionally Left Blank

3.36 Intentionally Left Blank

3.37 Intentionally Left Blank

3.38 Intentionally Left Blank

3.39 Intentionally Left Blank

7665

3.40 Provide X-User Assertion

This section corresponds to Transaction ITI-40 of the IHE IT Infrastructure Technical Framework.

3.40.1 Scope

Transaction ITI-40 is used by the **X-Service User** to pass a claimed identity assertion to the **X-Service**
7670 **Provider**. The **X-Service User** and **X-Service Provider** use the '**X-Assertion Provider'** as the third party issuer of the claimed identity assertion.

3.40.2 Use Case Roles
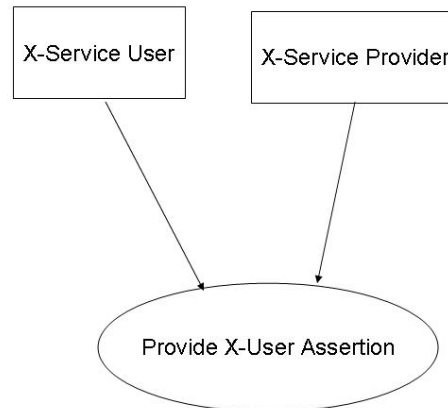
7675   **Actor:** X-Service User

Role: User of a transaction that requires a Cross-Enterprise User Assertion

Actor: X-Service Provider

Role: Service provider on a transaction that requires a Cross-Enterprise User Assertion

3.40.3 Referenced Standards

7680   **3.40.3.1 Normative -- required to use this profile**

- OASIS http://www.oasis-open.org/committees/security/.

  - o SAMLCore SAML V2.0 Core standard

  - WSS10 OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", March 2004.
7685 - WSS11 OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", February 2006.
  - WSS:SAMLTokenProfile1.0 OASIS Standard, "Web Services Security: SAML Token Profile", December 2004
  - WSS:SAMLTokenProfile1.1 OASIS Standard, "Web Services Security: SAML Token
7690   Profile 1.1", February 2006

3.40.3.2 Informative -- assist with understanding or implementing this profile

- IHE Profiles
  - o Personnel White Pages Profile
  - o Enterprise User Authentication Profile
  - o Basic Patient Privacy Consents Profile
  - o OASIS-OPEN
  - SAML V2.0 Standards http://www.oasis-open.org/committees/security/.
    - o SAMLTechOvw SAML V2.0 Technical Overview (a work in progress currently at revision 10)
    - o SAML Tutorial presentation by Eve Maler of Sun Microsystems
    - o SAML Metadata Version 2.0
  - WS-Trust OASIS Committee Draft, "WS-Trust 1.3", September 2006
  - WS-SecureConversation OASIS Committee Draft, "WS-SecureConversation 1.3", September 2006
- WS-I
  - o WS-I Conformance Claim
  - o WS-I Basic Security Profile Version 1.1 (Doesn't use SAML 2.0)
  - o WS-I Basic Profile Version 1.2 (Doesn't use SOAP 1.2)
- W3C
  - o WS-Policy Version 1.2
  - o SOAP Version 1.2
  - o SOAP W3C Note, "SOAP: Simple Object Access Protocol 1.1", 08 May 2000.
  - o SOAP 1.2 W3C Recommendation, "SOAP 1.2 Part 1: Messaging Framework", 24 June 2003.
  - o SOAPNorm W3C Working Group Note, "SOAP Version 1.2 Message Normalization", 8 October 2003.
- ISO
  - o ISO/TS 21091 Health informatics — Directory services for security, communications and identification of professionals and patients
  - o ISO 17090 Health informatics - Digital Certificates in Healthcare

7695

7700

7705

7710

7715

7720

___

3.40.4 Interaction Diagram
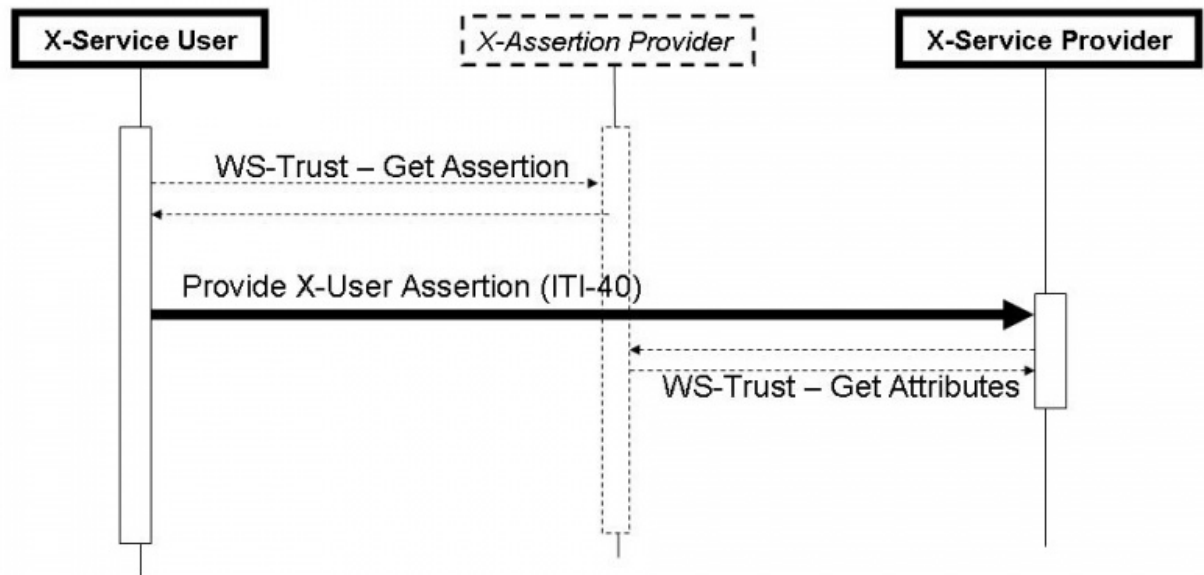
Figure 40.1-1 X-User Assertion Messages

3.40.4.1 Provide X-User Assertion

7725   The Provide X-User Assertion is profiled to assure interoperability between an X-Service User and an X-Service Provider that need an Assertion about the entity requesting the service. There are many ways to provide an Assertion that are all acceptable and may be used by parties that have agreed to their use.

The Provide X-User Assertion transaction sets some minimal interoperability profiling for this use-case. The Provide X-User Assertion transaction shall be used when there is no other agreed upon policy that 7730   would assure User Assertion interoperability (e.g. WS-SecurityPolicy).

3.40.4.1.1 Trigger

Configuration of the X-Service Provider and X-Service User indicates when the X-User Assertion transaction is necessary.

3.40.4.1.2 Message Semantics

7735   The X-User Assertion must be protected at all times against confidentiality exposure, malicious modification, and trust relationship between those communicating it. The IHE Actors that are grouped

with XUA may already require IHE-ATNA and thus TLS Mutual-Authentication, Integrity, and Confidentiality.

The X-Service User shall include the OASIS Web Services Security (WSS) Header, and shall include a
7740   SAML 2.0 Assertion as the security token.

Any ATNA Audit Messages that the X-Service User records in relationship to a transaction protected by the XUA (e.g., XDS.b Registry Stored Query, and XDS.b Retrieve Document Set), shall have the user identity recorded according to the XUA specific ATNA encoding rules (See 3.40.4.2 ATNA Audit encoding). This assures that the X-Service User and X-Service Provider ATNA Audit messages can be
7745   correlated at the ATNA Audit Repository.

Any ATNA Audit Messages recorded by Actor grouped with the X-Service User Actor, shall have the user identity recorded according to the XUA specific ATNA encoding rules (See 3.40.4.2 ATNA Audit encoding). For example: The XDS.b Document Consumer Actor records the Query event, this event record will include the identity provided in the XUA Identity Assertion. This assures that the X-Service
7750   User and X-Service Provider ATNA Audit messages can be correlated at the ATNA Audit Repository.

The SAML 2.0 **Assertion** is profiled as follows (**bold** is used when SAML 2.0 terms are used):

- The Assertion shall contain a **Subject**. The Subject contains the logical identifier of the principal performing the original service request (person, application, etc.) and remains unchanged through operations acting on the assertion (e.g. proxying the Assertion).

7755
  - The **Subject** shall contain a **SubjectConfirmation** element. The bearer confirmation method shall be supported; the holder-of-key method may be supported. These methods are defined in the SAML 2.0 Profile specification, section 3.

- The SAML Assertion **Conditions** are profiled as:

  - **NotBefore** shall be populated with the issue instant of the Assertion
7760
  - **NotOnOrAfter** is not specified by XUA because reasonable time limits are not clear at the IHE Profile level. The Expiration is provided by the X-Assertion Provider and would be variable on an Affinity Domain and/or System level.

  - The assertion shall contain an **AudienceRestriction** containing an **Audience** whose value is a URI identifying the X-Service Provider (e.g. XDS Registry, XDS Repository). It may
7765   contain an Audience whose value is a URI identifying the Affinity Domain.

  - The Assertion may contain **ProxyRestriction** and **OneTimeUser** conditions but XUA actors may ignore these conditions.

- The Assertion shall contain an AuthnStatement specify the AuthnContextClassRef or AuthnContextDeclRef
7770
- The Assertion may contain other statements (e.g. Attributes)

- The Assertion shall be signed by the X-Assertion Provider as defined in SAML Core.

The interface between the X-Service User and the X-Assertion Provider is not specified by XUA. This interface needs to be protected against risks (e.g. exposure of the SAML Token to interception for malicious use). Assertions need to be carefully managed in the X-Service User to ensure they are not
7775   exposed in the application code or any subsequent use of the Assertion.

3.40.4.1.3 Expected Actions

The X-Service Provider shall validate the Identity Assertion by processing the Web-Services Security header in accordance with the Web-Services Security Standard, and SAML 2.0 Standard processing rules (e.g., check the digital signature is valid and chains to an X-Identity Provider that is configured as trusted). If this validation fails, then the grouped Actor's associated transaction shall return with an error code as described in WS-Security core specification section 12 (Error Handling, using the SOAP Fault mechanism), and the ATNA Audit event for Authentication Failure shall be recorded according to ATNA rules.

Any ATNA Audit Messages recorded by Actor grouped with the X-Service Provider Actor, shall have the user identity recorded according to the XUA specific ATNA encoding rules (See 3.40.4.2 ATNA Audit encoding). For example: The XDS.b Registry Stored Query Actor records the Query event, this event record will include the identity provided in the XUA Identity Assertion. This assures that the X-Service User and X-Service Provider ATNA Audit messages can be correlated at the ATNA Audit Repository.

The X-Service Provider may use standards transactions to communicate with the X-Assertion Provider (e.g., WS-Trust, SAML 2.0 Protocol) to obtain information not included in the assertion provided (e.g. Attributes that might be related to structural roles).

The X-Service Provider may utilize the identity in access control decisions. Appropriate error messages, not defined here, shall be returned. The X-Service Provider may ignore any other statements (e.g. Attributes).

The X-Service Provider may use the authentication class references to determine the method that was used to authenticate the user. For example the X-Service Provider may have a configurable list of authentication class references that it is willing to recognize as authentication methods that are acceptable, thus treating other authentication class references as not authorized.

Assertions need to be carefully managed inside the X-Service Provider to ensure they are not exposed in the application code or any subsequent use of the Assertion.

3.40.4.2 ATNA Audit encoding

When an ATNA Audit message needs to be generated and the user is authenticated by way of an X-User Assertion, the ATNA Audit message **UserName** element shall record the X-User Assertion using the following encoding:

alias"<"user"@"issuer">"

where:

- **alias** is the optional string within the SAML Assertion's Subject element SPProvidedID attribute

- **user** is the required content of the SAML Assertion's Subject element

- **issuer** is the X-Assertion Provider entity ID contained with the content of SAML Assertion's Issuer element

3.40.4.3 Informative Material on WS-Trust

If the X-Service Provider uses WS-Trust in order to obtain a SAML assertion from an X-Identity Provider, it is suggested to use the version 1.3 of the WS-Trust specification, as described in [WS-Trust].

3.41 Provide and Register Document Set-b

This transaction is specified for Trial Implementation by the IHE XDS.b Supplement (www.IHE.net/Technical _Frameworks).

3.42 Register Document Set-b

This transaction is specified for Trial Implementation by the IHE XDS.b Supplement (www.IHE.net/Technical _Frameworks).

3.43 Retrieve Document Set

This transaction is specified for Trial Implementation by the IHE XDS.b Supplement (www.IHE.net/Technical _Frameworks).

_____

7825 ## 4 Cross-Transaction Specifications

4.1 XDS Metadata

The following sections specify the mapping of XDS concepts to ebRS and ebRIM semantics:

XDS Document

XDS Submission Request

7830   XDS Submission Set

XDS Folder

Document Relationships

The next sections specify the metadata definitions to support the above concepts. The following are discussed:

7835   XDS Document

XDS Submission Request

XDS Submission Set

XDS Folder

The remaining two sections discuss the following topics:

7840   XDS Registry Adaptor function

General metadata issues

Transaction that Reference this Section 4.1	
Register Document Set	ITI-14
Provide and Register Document Set	ITI-15
Query Registry	ITI-16
Registry Stored Query	ITI-18

Transactions that reference specific subsections of this Section 4.1	
Distribute Document Set on Media (4.1.1, 4.1.7, 4.1.8, 4.1.12)	ITI-32

4.1.1 Class Diagram
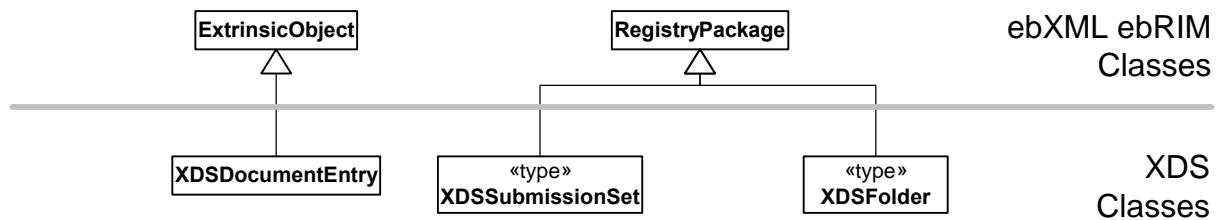
7845

Figure 4.1-1 ebXML Class Diagram of the Register Document Metadata

The XDSDocumentEntry class is derived from the ebXML ExtrinsicObject class. The XDSSubmissionSet and XDSFolder classes are derived from the ebXML5 RegistryPackage class. Since the ebXML Registry standard does not allow for subclassing the RegistryPackage class, these two
7850   classes are implemented as ebXML RegistryPackages. Type information (submission set vs. folder) is coded as an ebXML Classification against two object types created by the XDS profile, XDSSubmissionSet and XDSFolder.

4.1.2 Document Specification

A new registry object type is declared as a subclass of ebXML ExtrinsicObject. Its name is
7855   XDSDocumentEntry. An object of this type in the XDS registry is used to represent a document in an XDS repository.

An XDSDocumentEntry object in the registry contains a reference to a single document in a single repository.

> Note: A repository may hold documents that are not indexed in the registry.

7860   Appendix H defines the metadata to initialize an ebXML registry to serve as an XDS Document Registry.

4.1.3 XDS Submission Request Specification

A Submission Request is the collection of information that is transferred to an XDS Document Registry or Repository.

7865   There are two types of submission requests: XDS Registry Submission Request and XDS Repository Submission Request. Both are described below.

Appropriate protocol bindings are used to transfer this content between systems when the actors are not implemented together on the same system. The bindings are described in "Protocol Selection" section of the appropriate transaction.

7870   The two types of XDS Submission Requests are described next.

---

5   ebXML Registry terms such as RegistryPackage are shown with an ebXML prefix to help distinguish ebXML Registry terms from XDS terms. Unless otherwise indicated, references to 'ebXML' in XDS refer to the ebXML Registry specifications as opposed to other ebXML specifications. The short term is used for readability.

4.1.3.1 XDS Registry Submission Request

An XDS Registry Submission Request is the collection of metadata transferred between a Document Repository and a Document Registry in a single ebXML SubmitObjectsRequest. This request contains:

7875 • A collection of metadata to be stored in the registry including:

Metadata for new documents

Folders to be created

Documents to be added to folders

• A single XDS Submission Set, contained within the metadata, organizing the metadata

7880 This request is part of the Register Document Set transaction.

4.1.3.2 XDS Repository Submission Request

An XDS Repository Submission Request is the collection of metadata and documents transferred between a Document Source and a Document Repository using a single ebXML SubmitObjectsRequest. This request contains:

7885 Metadata

Zero or more documents; each document is represented by an XDSDocumentEntry object in the metadata. Submissions that add metadata to the registry without adding documents to the repository are possible.

This request is the information payload of the Provide and Register Document Set message of the 7890 Provide and Register Document Set transaction ITI-15.

Unless otherwise stated, the XDS Submission Set requirements specified hereafter apply to both types of XDS Submission Requests

4.1.3.3 Atomicity Requirements for XDS Submission Requests

XDS Submission requests shall be atomic operations. The result of a Submission Request is to update 7895 either:

a Registry or

a Registry and a Repository.

All changes requested are successfully applied or no net changes are made. More specifically:

1. Atomicity shall be managed by an XDS registry adaptor. (see section 4.1.11 for details on registry 7900 adaptor.addressing the fact that the ebXML Registry specification does not guarantee that a SubmitObjectsRequest is atomic). XDS specifies the mechanism through which atomicity is to be implemented and where it is needed.

2. All objects shall have their Status attribute set to Submitted when the objects are first created in the ebXML registry. An ebXML ApproveObjectsRequest, shall be issued within the XDS Registry Adaptor 7905 to change the Status attribute to Approved. This completes the transaction.

3. The following types of objects shall be have their status set to Approved to be considered publicly available:

XDSSubmissionSet (ebXML RegistryPackage)

XDSFolder (ebXML RegistryPackage)

7910   XDSDocumentEntry (subclass of ebXML ExtrinsicObject)

If an error occurs storing documents in the repository then all documents stored as part of the Repository Submission Request shall be removed.

If an error occurs storing metadata in the registry, then the following actions are performed:

7915   All metadata stored as part of the Registry Submission Request shall be removed from the registry

All documents stored as part of the Repository Submission Request shall be removed. This only applies if the Registry Submission Request is a result of a Repository Submission Request.

7920 Registry queries from the Registry Query transaction shall not find XDS Submission Sets, XDS Folders or XDSDocumentEntry objects until after the above atomic operation that creates them has completed successfully and the status attributes have been set to Approved.

4.1.3.4 Other Properties of Submission Requests

A Submission Request may contain metadata beyond the XDS Submission Set, XDS Folder, and XDSDocumentEntry objects. These are:

7925 ebXML Associations linking XDSDocumentEntry objects to XDSFolder objects. There are no restrictions on whether the XDSDocumentEntry objects or XDSFolder objects are in this Submission Request. Such an Association is the ebXML mechanism for including objects in an ebXML RegistryPackage (the basis of XDSFolder). Each of these Associations shall be accompanied by another association that links it with the XDSSubmissionSet object. This additional association

7930 allows for the identification of the Document Source actor which linked a particular document with a particular folder. See 4.1.5 for more information.

Associations linking existing (already contained in the registry) XDSDocumentEntry objects to the XDSSubmissionSet RegistryPackage contained in this Submission Request. This option is discussed in the next section.

7935

4.1.3.5 Attribute Value Length

4.1.3.5.1 Transactions using ebRIM 2.1

All attribute values shall conform to the size specification of ebRIM version 2.1 that is detailed in section 7.2 Data Types of that specification. More specifically, all Slots shall conform to the

7940 specification of ebRIM version 2.1, which is detailed in section 7.6.1 of that specification. The version 2.0-ebRIM specification is overly limiting in this respect. Without adopting the newer size limits, many typical patient record values could not be encoded.

4.1.3.5.2 Transactions using ebRIM 3.0

All attribute values shall conform to the size specification of ebRIM version 3.0 that is detailed in section 2.2 Data Types of that specification. More specifically, all Slots shall conform to the specification of ebRIM version 3.0, which is detailed in section 2.8.1 of that specification.

4.1.4 Submission Set Specifications

Submission Sets exist for two reasons:

> 1. To support atomic submission to the registry

> 2.To make a permanent record in the registry of

>> The existence and status of the submission

>> The XDS Folders and XDSDocumentEntry objects included in the submission.

Submission Sets, once shared, are immutable.

An XDS SubmissionSet is an ebXML RegistryPackage, classified as XDSSubmissionSet that is used to bundle XDSDocumentEntry, XDSFolder and Association objects for submission.

A Submission Set has a set of attributes that are described in section 4.1.8 Submission Set Metadata.

4.1.4.1 Inclusion of Documents in a SubmissionSet

Documents may be included in a Submission Set in two ways: inclusion by value and inclusion by reference.

Inclusion by value: A new document is being submitted to the registry. The Submission Set contains the XDSDocumentEntry object with associated attributes.

Inclusion by reference: Existing documents in the registry can be referenced by a Submission Set. These documents are included because of their clinical relevance to the rest of the Submission Set.

Linking document metadata to submission set: An XDSSubmissionSet shall be represented by an ebXML RegistryPackage. Document metadata (XDSDocumentEntry objects) shall be linked to the RegistryPackage via ebXML Associations according to the ebXML Registry standard.

For documents included by reference, the Submission Request shall include the Association object used to link the document. For documents included by value, the Submission Request shall include the XDSDocumentEntry object and the Association object used to link the document.

Submission Set Association labeling: Two types of association labels are defined: original (submission by value), or reference (Submission by reference). This allows finding the submission set that first submitted any document. It also supports proper rollback in case of a submission error. For document metadata included by value, a rollback of the submission shall delete the document metadata and the association. For document metadata included by reference, a rollback of the submission shall not delete the document metadata but shall still delete the association. (The document whose association is being deleted existed before this submission and shall be maintained.) The following labeling of the Associations is required.

Table 4.1-1 Submission Set Association Labeling

Inclusion type	Rollback	Association Labeling

| By Value | Yes | Slot: Name=SubmissionSetStatus
Value=Original |
| By Reference | No | Slot: Name=SubmissionSetStatus
Value=Reference |

Submission Sets and patients: A Submission Set is restricted in terms of mixing documents from different patients. All documents included by value in a Submission Set shall have their patientId attribute set to the same value. This restriction does not apply to documents included by reference.

Document metadata duplication: There are several conditions regarding the duplication of document metadata that can occur.

Duplicate registration of a document - A document and its metadata are submitted to the repository as part of a Repository Submission Request. This document already exists in one or more repositories and is already represented in the registry. It is submitted with a new (not previously used) UUID for the XDSDocumentEntry and associated ancillary objects. The registry shall accept such duplicate registration of the documents.

Duplicate document id submitted to repository - A document with its associated metadata is part of a Repository Submission Request. A document with the same XDSDocumentEntry.uniqueID is present in the repository but the XDSDocumentEntry.hash is different. This is an error and the Submission Request shall be rejected by the repository.

Note: There are two approaches to detecting this fault. First, this can be detected at the repository if repository logic can validate the hashes and has record of the document id to compare. Otherwise the request can be forwarded on to the registry and let the fault be detected by the registry (see next bullet). The repository then deals with the error returned by the registry.

Duplicate document ID submitted to registry - Metadata representing a document (XDSDocumentEntry) is part of a Registry Submission Request. An XDSDocumentEntry object with the same uniqueID is present in the registry but, the hash is different. This is an error and the Submission Request shall be rejected by the XDS registry adaptor.

A document, once generated outside of the XDS environment, can be registered by multiple Document Sources with the same uniqueId, same hash, different UUID, and with other metadata attributes not the same as described above. As a result, a Document Consumer may issue a GetDocuments Stored Query with a uniqueId parameter and have returned two or more XDSDocumentEntry objects with that same uniqueId.

4.1.4.2 Inclusion of Folders in a SubmissionSet

Linking folder metadata to submission set: An XDSSubmissionSet shall be represented by an ebXML RegistryPackage. Folder metadata (XDSFolder objects) shall be linked to the RegistryPackage via ebXML Associations according to the ebXML Registry standard.

Linking associations to a submission set: A document can be linked to a folder to indicate that this document is a member of a particular folder. This link shall be represented via an ebXML Association according to the ebXML Registry standard. Each of these Associations shall be accompanied by another 'HasMember' Association that links it with the XDSSubmissionSet object. This additional association allows for the identification of the Document Source actor which linked a particular document with a particular folder and shall be as follows:

- The targetObject shall contain the id of the Association that links the document and the folder.

▪ The sourceObject shall contain the id of the XDSSubmissionSet object.

It is not necessary that the XDSSubmissionSet object which links to this Association also contain the XDSDocumentEntry metadata or the XDSFolder metadata that correspond to the referenced document and folder. This allows for documents to be placed in folders at a later date and time. If the
8020 XDSSubmissionSet object does contain the corresponding XDSDocumentEntry or XDSFolder, then these should be linked to the XDSSubmissionSet object as previously described.

4.1.5 Folder Specification

An XDS Folder is an ebXML RegistryPackage classified as XDSFolder. This folder is used to bundle XDSDocumentEntry objects. Folders shall not be nested inside other folders. The patientId attribute of
8025 the XDSDocumentEntry objects it contains shall match the patientId attribute on the folder itself. This shall be enforced by the Registry Actor.

Note: The nesting of folders may be considered as a future extension to this transaction.

Linking documents to a folder: A document can be linked to a folder to indicate that this document is a member of a particular folder. This link shall be represented via an ebXML Association according to
8030 the ebXML Registry standard. This association shall have an id attribute which shall be a UUID. Each of these Associations shall be accompanied by another association that links it with the XDSSubmissionSet object. This additional association allows for the identification of the Document Source actor which linked a particular document with a particular folder. See 4.1.4.2 for more information regarding this accompanying Association object.

8035

4.1.6 Document Relationships and Associations

4.1.6.1 Document Relationships from HL7

Relationships between documents can be established with XDS. XDS adopts the document relationship semantics defined in HL7 CDA. The supported relationships are listed below in Table 4.1-2. The
8040 semantics behind each of these relationships are documented in HL7 CDA Release 2, Committee Ballot 2.

To create a document relationship in the registry, submit:

A new document (XDSDocumentEntry)

An Association linking the new document to an existing document.

8045 The association type defines the document relationship. The new document and the association must be submitted in the same Submission Set. The existing document must be an Approved object already in the registry. The identity (registry UUID) of the existing document must be discovered via registry query.

The association types used for document relationships are defined by XDS and an XDS Registry must
8050 be initialized with their definitions. See Appendix H for details.

Table 4.1-2 Document Relationships

Relationship	Definition

APND (append)	The current document is an addendum to the parent document.
RPLC (replace)	The current document is a replacement of the parent document.
XFRM (transform)	The current document is a transformation of the parent document.
XFRM_RPLC (transform with replace)	The current document is both a transformation and a replacement of the parent document.

Adapted from HL7 CDA Release 2, Committee Ballot 2

A Document Relationship refers to any of the relationships listed in Table 4.1-2 above. Section 3.15.5.1
8055   documents for the Document Source which of these operations are required and optional.

A Document Source actor creates a document relationship by submitting a Submission Set containing:

XDSDocumentEntry – this defines the new document being submitted

The uniqueId attribute must be unique.

The UUID must be unique or symbolic (the registry assigns)

8060   **Association** – this links the original XDSDocumentEntry (already in the registry) with the new XDSDocumentEntry being submitted.

The targetObject attribute of the Association object references the existing document in the registry.

The sourceObject attribute of the Association object references the XDSDocumentEntry
8065   contained in the Submission Set.

The Association Type is one of the relationships in table 4.1-2.

The targetObject attribute of the Association is the registry UUID representing the existing document in the registry. This UUID must be discovered via registry query.

The existing document shall be deprecated by the following rules (based on CDA R2):

8070   • The APND and XFRM relationships leave the original document with its status unchanged (Approved).

• The RPLC and XFRM_RPLC relationships change the status of the original document to Deprecated. All transformations (XFRM) and addenda (APND) of the original document shall also deprecated.

8075   Note to implementers: if you are doing a replace where original has addenda, you should be real careful - may have been important comment from another author.

The Registry Adaptor manages document deprecation. See section 4.1.11 XDS Registry Adaptor for details.

Only the most recent version of a document shall be replaceable. The most recent version of a document
8080   carries a status of Approved while older versions carry a status of Deprecated.

A transformation (connected to original document with XFRM Association) is an alternate form of an original document. Therefore, a transformation is permitted to be replaced (RPLC) but shall not be appended to (APND).

Associations of type XFRM, APND, RPLC, and XFRM_RPLC may include documentation describing
8085   the association (type of transformation, reason for replacement, etc.). If included, it shall be specified as

a Classification on the Association as shown in the example below. See also XDS Document Entry
attribute parentDocumentRelationshipCode.

Example (ebRIM 2.1):
```
<rim:Association id="ThisAssociation"
  associationType="XFRM"
  sourceObject="source"
  targetObject="target">
  <rim:Classification
      classificationScheme="urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3"
      classifiedObject="ThisAssociation"
      nodeRepresentation="French">
    <rim:Name>
      <rim:LocalizedString value="Translation into French"/>
    </rim:Name>
    <rim:Slot name="codingScheme">
      <rim:ValueList>
        <rim:Value>Connect-a-thon translation types</rim:Value>
      </rim:ValueList>
    </rim:Slot>
  </rim:Classification>
</rim:Association>
```

When a document is replaced and that document is a member of one or more folders, a new HasMember
Association shall be created by the Registry Adaptor connecting the replacement document to each
folder that held the original document as a member. The result is that a folder contains both the original
and replacement document differentiated by their status. The Document Registry actor shall detect this
condition and generate the necessary Associations.

Table 4.1-3 lists all metadata associated with XDSDocumentEntry objects. The attribute
XDSDocumentEntry.parentDocumentId is a reference to the targetObject attribute of the new
Association. The attribute XDSDocumentEntry.parentDocumentRelationship is a reference to the
Association Type. This represents two distinct naming conventions, HL7 CDA and ebXML Registry.

Document relationship metadata may coexist with other metadata in a Submission Set.

The new documents (related to original document by RPLC, APND, XFRM, or XFRM_RPLC
Associations) are assigned their own uniqueId attribute unrelated to the original document's.

See ITI Vol-1: 10.4.11.1 for further detail on the use and meaning of document relationships.

4.1.6.2 Association type signs

An ebRIM Association with associationType of *signs* shall be used to link an XDSDocumentEntry
representing a Digital Signature with the XDSDocumentEntry representing the document being signed.
Details of how Digital Signatures are represented in XDS are found in the Document Content Profile on
Digital Signatures. In constructing this association, the attributes are:

sourceObject: references the XDSDocumentEntry representing the Digital Signature

targetObject: references the XDSDocumentEntry representing the document being signed

associationType: signs

Other requirements on the use of this Association may exist in the Document Content Profile on Digital
Signatures.

4.1.6.3 Association Type formatting

OASIS ebRIM versions 2.1 and 3.0 (XDS.a and XDS.b) have different requirements for the formatting of Association Types. ebRIM 2.1 requires only the simple name (HasMember) while ebRIM 3.0 requires a namespace qualified name (urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember). The urn:oasis:names:tc:ebxml-regrep:AssociationType: namespace prefix only applies to Association Types defined by ebRIM 3.0 (HasMember only). Association Types defined by XDS and related profiles shall use the IHE specific namespace urn:ihe:iti:2007:AssociationType:.

Table 4.1-2.1 Association Types used in XDS and related profiles

ebRIM 2.1 Format	ebRIM 3.0 Format
HasMember	urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember
RPLC	urn:ihe:iti:2007:AssociationType:RPLC
XFRM	urn:ihe:iti:2007:AssociationType:XFRM
APND	urn:ihe:iti:2007:AssociationType:APND
XFRM_RPLC	urn:ihe:iti:2007:AssociationType:XFRM_RPLC
signs	urn:ihe:iti:2007:AssociationType:signs

4.1.7 Document Definition Metadata

Several data types are used in the tables below describing the document metadata. These data types are derived from other standards, and encoded in the registry as described in the following table. For entries where no Data Type is specified the entry is any string of bytes that fits within the length defined by the schema.

For the data types derived from HL7 standards, XDS requires that the default HL7 separators be used to represent the structure of HL7 V2 data types:

Field Separator	|
Component Separator	^
Subcomponent Separator	&
Repetition Separator	~

Table 4.1-3 Data Types

XDS Data Type	Source Standard	Encoding Specification
CX	HL7 V2 Identifier	This is an identifier. HL7 Identifier type CX consist of several components, but this specification restricts them to the use of two components, the ID Number, and the Assigning Authority (AA). The Assigning Authority identifies the "domain" over which the ID Number represents a unique entity. Furthermore, the AA is represented using a Universal ID and Universal ID Type. In XDS specification, ISO Object Identifiers (see OID below) must be used as Universal ID. Therefore,

		Universal ID Type is always ISO. The required format is: *IDNumber*^^^&*OIDofAA*&ISO
		No other values/modifications in other components or subcomponents are allowed. Specifically, components 2 and 3 shall be empty as listed above.
		An explicit example is:
		543797436^^^&1.2.840.113619.6.197&ISO
		Note that the '&' character must be properly encoded in the XML content. See the examples in the tables below for the appropriate representation.
DTM	HL7 V2 Date Time	This is a date/time value, represented as precisely as possible. All date time values in the registry are stored using universal coordinated time [UTC].
		"UTC" implies that the source and the consumer shall convert the time from/to the local time.
		The format of these values is defined as the following regular expression:
		YYYY[MM[DD[hh[mm[ss]]]]]
		Where:
		YYYY is the four digit year i.e. 2006
		MM is the two digit month 01-12, where Jan is 01, Feb is 02, etc.
		DD is the two digit day of the month 01-31
		HH is the two digit hour, 00-23, where 00 is midnight, 01 is 1 am, 12 is noon, 13 is 1 pm, etc.
		mm is the two digit minute, 00-59
		ss is the two digit seconds, 00-59
		The following are legal date time values with increasing precision representing the date and time January 2, 2005, 3:04:05am
		2005 200501 20050102 2005010203 200501020304 20050102030405
OID	ISO Object Identifier	An ISO Object identifier. Limited in length to 64 characters, and made up of characters from the set [0-9.]. It must start with an integer, and is followed by one or more additional integer values, separated by periods. Integers are represented without leading 0 digits unless the value is zero.
		1.3.6.1.4.1.21367.2005.3.7
		In the attribute tables below, when an OID format is specified, it shall follow the assignment and format rules defined for document UID in ITI TF-2 : Appendix B
Field	HL7 V2 Message Segment	Specified as the Field identifier, followed by a pipe (|) and then the data value represented with corresponding HL7 V2 data type as defined in HL7 standard. Note that if a HL7 data type is used to derive XDS data type (as shown in this table), the derived XDS data type shall be used to represent the value.
		An example of field Patient Identifier List (the third field of PID segment) is as follows:
		PID-3|DTP-1^^^&1.3.6.1.4.1.21367.2005.3.7& ISO
SHA1	Document hash calculated with SHA1 algorithm	See RFC 3174 US Secure Hash Algorithm 1 (SHA1), September 2001

URI	Uniform Resource Identifer	See RFC 2616
UUID	Universally Unique Identifier	A DCE Universally Unique Identifier, represented in registry attributes using the URN syntax for UUIDs: urn:uuid:9e0110f8-4748-4f1e-b0a8-cecae32209c7
XCN	HL7 V2 Extended Person Name	This data type describes a person along with the identifier by which he is known in some domain (either the source domain or the XDS affinity domain), using the HL7 v2.5 XCN data type. This data type contains, amongst others, Identifier Last Name First Name Second and Further Given Names Suffix Prefix Assigning Authority All of the HL7 v2.5 fields may be specified as optional components with the following restrictions: ▪ Either name or an identifier shall be present. Inclusion of other components is optional provided the slot value length restrictions imposed by ebXML2.1 and ebXML3.0, 64 and 256 bytes respectively, is not exceeded. ▪ If component 1 (ID Number) is specified, component 9 (Assigning Authority) shall be present if available. ▪ The XDS XCN Component 9 is subject to the same the restrictions as defined for the XDS CX data type component 4. Thus: the first subcomponent shall be empty, the second subcomponent must be an ISO OID (e.g., 1.2.840.113619.6.197), and the third subcomponent shall read 'ISO'. ▪ Any empty component shall be treated by the Document Registry as not specified. This is in compliance with HL7 v2.5. ▪ Trailing delimiters are recommended to be trimmed off. Document Registries shall ignore trailing delimiters. This is in compliance with HL7 v2.5.(Update registry validation table as well to note this.) A example of person name with ID number using this data type is as follows: 11375^Welby^Marcus^J^Jr. MD^Dr^^^&1.2.840.113619.6.197&ISO
XON	HL7 V2 Organization Name	This is the organization name, specified with the first component (XON.1) of the HL7 data type XON: Organization Name An example of organization name using this data type is as follows: Fairview Hospital

The source/query column indicates which attributes are required during submission, and whether the registry must support the ability to execute queries against them.

8150

Table 4.1-4 Codes for Source/Query Column

Code	Meaning
R	Required
R2	Required if Known

O	Optional
P	Registry is not required to support query of this attribute.
Cp	Computed/Assigned by Repository, required in register transaction.
Cg	Computed/Assigned by Registry

The XDSDocumentEntry object type is created in ebXML Registry by extending the ebXML Registry ObjectType Classification Scheme6.

The following metadata elements shall be used to describe an XDS Document. They shall be provided
8155 by the Document Repository Actor in the Register Document Set Transaction either directly if grouped with a Document Source Actor or forwarded from a Provide and Register Document Set Transaction.

The XDSDocumentEntry.URI shall be supplied by the Document Repository Actor. Its value is dependent on how the repository stores the document.

Each attribute shown below is an attribute on the XDSDocumentEntry object. The attribute name is
8160 defined with a prefix of the object type of XDSDocumentEntry when referenced by other objects, for example XDSDocumentEntry.patientId.

Table 4.1-5 Document Metadata Attribute Definition

---

6   The specific requirement in ebRIM that object types be user extendable was introduced after version 2.0.

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints	

author	Represents the humans and/or machines that authored the document. This attribute contains the following sub-attributes:
	• authorInstitution
	• authorPerson
	• authorRole
	• authorSpecialty
	which are individually defined below.
	
	The author attribute is defined as a Classification which contains the above sub-attributes. The author attribute itself does not have a simple value. It defines a structure to hold its sub-attributes. An instance of this Classification shall be considered a single value of the author attribute. If present, the author attribute shall have one or more values. Each instance of this Classification shall contain:
	• One instance of the authorPerson sub-attribute
	• Zero or more instances of the authorInstitution sub-attribute
	• Zero or more instances of the authorRole sub-attribute
	• Zero or more instances of the authorSpecialty sub-attribute
	
	The following example shows the definition of a single author. The classification shows the required authorPerson Slot holding the required single value. Single values are shown for authorInstitution, authorRole, and authorSpecialty. Multiple values for these three sub-attributes, if present, shall be coded as additional Value elements within the Slot/ValueList having the correct name.
	
	`<rim:Classification`
	`  classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d"`
	`  classifiedObject="theDocument"`
	`  nodeRepresentation="">`
	`<!-- nodeRepresentation intentionally left blank -->`
	
	`  <rim:Slot name="authorPerson">`
	`    <!-- shall be single valued -->`
	`    <rim:ValueList>`
	`      <rim:Value>name of author</rim:Value>`
	`    </rim:ValueList>`
	`  </rim:Slot>`
	
	`  <rim:Slot name="authorInstitution">`
	`    <!-- may be multivalued -->`
	`    <rim:ValueList>`
	`      <rim:Value>name of institution</rim:Value>`
	`    </rim:ValueList>`
	`  </rim:Slot>`
		R2/R	ebRIM	

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints
	``` <rim:Slot name="authorRole"> <!-- may be multivalued --> <rim:ValueList> <rim:Value>name of role</rim:Value> </rim:ValueList> </rim:Slot> <rim:Slot name="authorSpecialty"> <!-- may be multivalued --> <rim:ValueList> <rim:Value>specialty of author</rim:Value> </rim:ValueList> </rim:Slot> </rim:Classification> ```		
authorInstitution (sub-attribute of author)	Represents a specific healthcare facility under which the human and/or machines authored the document. A specific case is that of homecare. This is a sub-attribute of the author attribute. See the author attribute for definition of the requirements of usage. See author for example.	R2/R	XON
authorPerson (sub-attribute of author)	Represents the humans and/or machines that authored the document within the authorInstitution. The document author may be the patient itself. This is a sub-attribute of the author attribute. See the author attribute for definition of the requirements of usage. See author for example.	R2/R	XCN
authorRole (sub-attribute of author)	A code that represents the role of the author with respect to the patient when the document was created. This is a sub-attribute of the author attribute. See the author attribute for definition of the requirements of usage. See author for example.	R2/O	
authorSpecialty (sub-attribute of author)	Represents a specific specialty within a healthcare facility under which the human and/or machines authored the document. This is a sub-attribute of the author attribute. See the author attribute for definition of the requirements of usage. See author for example.	R2/O	
availabilityStatus	An XDS Document shall have one of two availability statuses: Approved available for patient care	Cg/R	

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints	

	Deprecated obsolete
	
	This attribute is always set to Approved as part of the submission of new XDS Documents. It may be changed to Deprecated under the primary responsibility of the Document Source with possible patient supervision.
	
	Although XDS supports the ability to delete documents, there is no such state as "the Document Entry is removed" (only an audit trail is kept if such a deletion is allowed).
	
	This list may be extended in the future. See section 4.1.3.3 Atomicity Requirements for XDS Submission Requests for additional details.
	
	If present, shall have a single value.
	
	The example below shows the status attribute, however, this attribute is only returned on query, not set during any registry or repository transaction.
	
	<pre><ExtrinsicObject
	  id="urn:uuid:fbeacdb7-5421-4474-9267-985007cd8855"
	  objectType=
	    "urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
	  status="Approved"
	  mimeType="application/octet-stream"
	> …</pre>			

classCode	The code specifying the particular kind of document (e.g. Prescription, Discharge Summary, Report). It is suggested that the XDS Affinity Domain draws these values from a coding scheme providing a coarse level of granularity (about 10 to 100 entries). Shall have a single value.
	
	<pre><rim:Classification
	  classificationScheme=
	    "urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
	  classifiedObject="theDocument"
	  nodeRepresentation="classCode"
	>
	  <rim:Name>
	  <rim:LocalizedString
	    value="classCodeDisplayName"/>
	  </rim:Name>
	  <rim:Slot name="codingScheme">
	    <rim:ValueList>
	      <rim:Value>XDS Affinity Domain Specific Value</rim:Value>
	    </rim:ValueList>
	  </rim:Slot>
	</rim:Classification></pre>
		R/R	XDS Affinity Domain specific	

classCode DisplayName	The name to be displayed for communicating to a human the meaning of the classCode. Shall have a single value for each value of classCode.	R/P	XDS Affinity Domain	

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints
	See classCode for example.		specific
comments	Comments associated with the Document. Free form text with an XDS Affinity Domain specified usage. ```<rim:Description>\n <rim:LocalizedString value = "comments"/>\n</rim:Description>```	O/P	XDS Affinity Domain specific
confidentialityCode	The code specifying the level of confidentiality of the XDS Document. These codes are specific to an XDS Affinity Domain. Enforcement and issues related to highly sensitive documents are beyond the scope of XDS (see security section). These issues are expected to be addressed in later years. confidentialityCode is part of a codification scheme and value set enforced by the Document Registry. Shall have one or more values. Code multiple values by creating multiple classification objects. ```<rim:Classification\n classificationScheme=\n "urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"\n classifiedObject="theDocument"\n nodeRepresentation="confidentialityCode"\n>\n <rim:Name>\n <rim:LocalizedString value="displayName"/>\n </rim:Name>\n <rim:Slot name="codingScheme">\n <rim:ValueList>\n <rim:Value>XDS Affinity Domain Specific Value</rim:Value>\n </rim:ValueList>\n </rim:Slot>\n</rim:Classification>```	R/P	XDS Affinity Domain specific
creationTime	Represents the time the author created the document in the Document Source. Shall have a single value. ```<rim:Slot name="creationTime">\n <rim:ValueList>\n <rim:Value>20041225212010</rim:Value>\n </rim:ValueList>\n</rim:Slot>```	R/R	DTM
entryUUID	The globally unique identifier (may be assigned by either by Source, Repository, or Registry) is primarily intended for use as a document registry management identifier. It is not meant to be an external reference for XDS Documents (e.g. in links within other documents). The uniqueId is meant for that purpose so that such links remain valid beyond the XDS Affinity Domain. If present, shall have a single value.	Cg/P	UUID

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints

	In the example below, the entryUUID is a6e06ca8-0c75-4064-9e5c-88b9045a96f6
	
	 ```<rim:ExtrinsicObject mimeType="application/pdf"```
	 ``` id="urn:uuid:a6e06ca8-0c75-4064-9e5c-88b9045a96f6"```
	 ``` objectType=```
	 ``` "urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"```
	
	 ```> …```		

eventCodeList	This list of codes represents the main clinical acts, such as a colonoscopy or an appendectomy, being documented. In some cases, the event is inherent in the typeCode, such as a "History and Physical Report" in which the procedure being documented is necessarily a "History and Physical" act.
	
	 An event can further specialize the act inherent in the typeCode, such as where it is simply "Procedure Report" and the procedure was a "colonoscopy". If one or more eventCodes are included, they shall not conflict with the values inherent in the classCode, practiceSettingCode or typeCode, as such a conflict would create an ambiguous situation.
	
	 This short list of codes is provided to be used as "key words" for certain types of queries. If present, shall have one or more values.
	
	 ```<rim:Classification```
	 ``` classificationScheme=```
	 ``` "urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4"```
	 ``` classifiedObject="theDocument"```
	 ``` nodeRepresentation="eventCode"```
	 ```>```
	 ``` <rim:Name>```
	 ``` <rim:LocalizedString value="eventCodeDisplayName"/>```
	 ``` </rim:Name>```
	 ``` <rim:Slot name="codingScheme">```
	 ``` <rim:ValueList>```
	 ``` <rim:Value>XDS Affinity Domain Specific Value</rim:Value>```
	 ``` </rim:ValueList>```
	 ``` </rim:Slot>```
	 ```</rim:Classification>```
		O/R	XDS Affinity Domain specific

eventCodeListDisplay Name	The list of names to be displayed for communicating to human reader the meaning of the eventCode. If present, shall have a single value corresponding to each value in eventCodeList. See eventCodeList for an example.	O7/P	XDS Affinity Domain specific
formatCode	Code globally uniquely specifying the format of the document.	R/R	XDS

---

7   Required if eventCode has a value.

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints

	Along with the typeCode, it should provide sufficient information to allow any potential XDS Document Consumer to know if it will be able to process the document. The formatCode shall be sufficiently specific to ensure processing/display by identifying a document encoding, structure and template (e.g. for a CDA Document, the fact that it complies with a CDA schema, possibly a template and the choice of a content-specific style sheet). Shall have a single value. Format codes may be specified by multiple organizations. Format codes defined by ITI shall have names with the prefix
	
	    urn:ihe:iti:
	
	Format codes defined by other IHE domains shall have names with the prefix
	
	    urn:ihe:'domain initials':
	
	Format codes defined by the Affinity Domain shall have names with the prefix
	
	    urn:ad:'name of affinity domain':
	
	Affinity Domains shall be unique.
	
	The prefixes described here are not assumed to be exhaustive.
	
	<pre><rim:Classification
	  classificationScheme=
	    "urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d"
	  classifiedObject="theDocument"
	  nodeRepresentation="formatCode"
	>
	  <rim:Name>
	    <rim:LocalizedString value="name"/>
	  </rim:Name>
	  <rim:Slot name="codingScheme">
	    <rim:ValueList>
	      <rim:Value>XDS Affinity Domain Specific Value</rim:Value>
	    </rim:ValueList>
	  </rim:Slot>
	</rim:Classification></pre>
			Affinity Domain specific

hash	Hash key of the XDS Document itself. This value is computed by the Document Repository and used by the Document Registry for detecting the improper resubmission of XDS Documents. If present, shall have a single value. If this attribute is received in a Provide & Register Document Set transaction, it shall be verified by the repository with the actual hash value of the submitted document; an error shall be	Cp/P	SHA1 hash See Section 3.15.4.1

XDSDocumentE ntry Attribute	Definition	Source/ Query	Constraints
	returned on mismatch. ```<rim:Slot name="hash">\n <rim:ValueList>\n <rim:Value>\n da39a3ee5e6b4b0d3255bfef95601890afd80709\n </rim:Value>\n </rim:ValueList>\n</rim:Slot>```		
healthcareFacilit y TypeCode	This code represents the type of organizational setting of the clinical encounter during which the documented act occurred. In some cases, the setting of the encounter is inherent in the typeCode, such as "Diabetes Clinic Progress Note". healthcareFacilityTypeCode shall be equivalent to or further specialize the value inherent in the typeCode; for example, where the typeCode is simply "Clinic Progress Note" and the value of healthcareFacilityTypeCode is "private clinic". The value shall not conflict with the value inherent in the typeCode, as such a conflict would create an ambiguous situation. Shall have a single value. ```<rim:Classification\n classificationScheme=\n "urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1"\n classifiedObject="theDocument"\n nodeRepresentation="healthcareFacilityTypeCode"\n>\n <rim:Name>\n <rim:LocalizedString\n value="healthcareFacilityTypeCodeDisplayName"/>\n </rim:Name>\n <rim:Slot name="codingScheme">\n <rim:ValueList>\n <rim:Value>XDS Affinity Domain Specific Value</rim:Value>\n </rim:ValueList>\n </rim:Slot>\n</rim:Classification>```	R/R	XDS Affinity Domain specific
healthcareFacilit y TypeCodeDispla y Name	The name to be displayed for communicating to a human the meaning of the healthcareFacilityTypeCode. Shall have a single value for each value of healthcareFacilityTypeCode. See healthcareFacilityTypeCode for an example.	R/P	XDS Affinity Domain specific
languageCode	Specifies the human language of character data in the document. The values of the attribute are language identifiers as described by the IETF (Internet Engineering Task Force) RFC 3066. This value may further be restricted by the registry according	R/P	

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints

	to XDS Affinity Domain specific policy. Shall have a single value.
	
	`<rim:Slot name="languageCode">`
	`  <rim:ValueList>`
	`    <rim:Value>en-us</rim:Value>`
	`  </rim:ValueList>`
	`</rim:Slot>`		

legalAuthenticator	Represents a participant who has legally authenticated or attested the document within the authorInstitution. Legal authentication implies that a document has been signed manually or electronically by the legalAuthenticator. This attribute may be absent if not applicable. If present, shall have a single value
	
	`<rim:Slot name="legalAuthenticator">`
	`  <rim:ValueList>`
	`    <rim:Value>^Welby^Marcus^^^Dr^MD</rim:Value>`
	`  </rim:ValueList>`
	`</rim:Slot>`
		O/O	XCN

mimeType	MIME type of the document in the Repository. Shall have a single value.
	
	`<rim:ExtrinsicObject mimeType="`**`application/pdf`**`"`
	`  id="theDocument"`
	`  objectType=  "urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"`
	`> …`
		R/P	

parentDocumentId	The identifier of the parentDocument entry that represents the source of a document replacement, addendum, transformation, or signs relationship. Not specified if no relationship will be specified.
	
	May identify a document which is unknown by the Document Registry. If present, shall have a single value.
	
	`<rim:ObjectRef`
	`  id="`**`urn:uuid:a6e06ca8-0c75-4064-9e5c-88b9045a96f6`**`"`
	`/>`
	`<rim:Association`
	`  associationType="`**`APND`**`"`
	`    sourceObject="theDocument"`
	`    targetObject="`**`urn:uuid:a6e06ca8-0c75-4064-9e5c-88b9045a96f6`**`"`
	`/>`
	
	If the parent document is in the registry then code as association to it, otherwise create a stub document object, and use its entryUUID as the value for the targetObject attribute.
	
	A document stub represents a document that is not in registry
		O/P	ebRIM Associaton

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints
	but is needed by another object to point at. This association is coded with a type from parentDocumentRelationship. A document may have a single relationship via the RPLC, APND, or XFRM association types. There is no restriction on the number of signs relationships that a document may be part of.		
parentDocument Relationship	The type of relationship that the document has with the parentDocument (e.g. replace, addendum, transformation, or signs). Shall be present if the parentDocumentId attribute is present. If present, shall have a single value. See parentDocumentID for an example.	O/P	Use one of the following values: APND RPLC XFRM signs

patientId	The patientId represents the subject of care of the document. This identifier shall be from the Assigning Authority Domain supporting the XDS Affinity Domain in which the Document Registry operates. It shall contain two parts:
	
	Authority Domain Id (enforced by the Registry)
	
	An Id in the above domain.
	
	No other values are allowed, as specified for the CX type in Table 4.1-3 above. Using HL7 terminology, no other values are allowed in the components of the coded value, nor are further subcomponents allowed.
	
	The value of the patientId shall be the same for all new documents of a Submission Set.
	
	Shall have a single value.
	
	`<rim:ExternalIdentifier`
	`  identificationScheme=`
	`    "urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446"`
	` value="6578946^^^&1.3.6.1.4.1.21367.2005.3.7&IS`
	`O"`
	`>`
	`  <rim:Name>`
	`   <rim:LocalizedString value = "XDSDocumentEntry.patientId"/>`
	`  </rim:Name>`
	`</rim:ExternalIdentifier>`
		R/R	CX

practiceSettingC ode	The code specifying the clinical specialty where the act that resulted in the document was performed (e.g. Familly Practice, Laboratory, Radiology). It is suggested that the XDS Affinity	R/R	XDS Affinity Domain

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints

	Domain draws these values from a coding scheme providing a coarse level of granularity (about 10 to 100 entries). Shall have a single value.
	
	``
	<rim:Classification
	  classificationScheme=
	    "urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead"
	  classifiedObject="theDocument"
	  nodeRepresentation="practiceSettingCode"
	>
	  <rim:Name>
	    <rim:LocalizedString
	      value="practiceSettingCodeDisplayName"
	    />
	  </rim:Name>
	  <rim:Slot name="codingScheme">
	    <rim:ValueList>
	      <rim:Value>XDS Affinity Domain Specific Value</rim:Value>
	    </rim:ValueList>
	  </rim:Slot>
	</rim:Classification>
	``
			specific

practiceSettingCode DisplayName	The name to be displayed for communicating to a human the meaning of the practiceSettingCode. Shall have a single value for each value of practiceSettingCode. See practiceSettingCode for an example.	R/P	XDS Affinity Domain specific
serviceStartTime	Represents the start time the service being documented took place (clinically significant, but not necessarily when the document was produced or approved). This may be the same as the encounter time in case the service was delivered during an encounter. Encounter time is not coded in XDS metadata but may be coded in documents managed by XDS. This time is expressed as (date/time/UTC). If present, shall have a single value. Note: Other times, such as document creation or approval are to be recorded, if needed, within the document. ``` <rim:Slot name="serviceStartTime"> <rim:ValueList> <rim:Value>20041225212010</rim:Value> </rim:ValueList> </rim:Slot> ```	R2/R	HL7 V2 DTM
serviceStopTime	Represents the stop time the service being documented took place (clinically significant, but not necessarily when the document was produced or approved). This may be the same as the encounter time in case the service was delivered during an encounter. Encounter time is not coded in XDS metadata but may be coded in documents managed by XDS. This time is expressed as (date/time/UTC). If the Service happens at a point in time, this attribute shall contain the same value as the	R2/R	HL7 V2 DTM

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints
	serviceStartTime. If present, shall have a single value. ```<rim:Slot name="serviceStopTime"> <rim:ValueList> <rim:Value>20041225232010</rim:Value> </rim:ValueList> </rim:Slot>```		
size	Size in bytes of the byte stream that was provided in the Register and Provide Transaction and stored by the XDS Document Repository. This value is computed by the Document Repository and included in the Register Documents Set Transaction. If present, shall have a single value. If this attribute is received in a Provide & Register Document Set transaction, it shall be verified by the repository with the actual size of the submitted document; an error may be returned on mismatch. ```<rim:Slot name="size"> <rim:ValueList> <rim:Value>3654</rim:Value> </rim:ValueList> </rim:Slot>```	Cp/P	Integer See Section 3.15.4.1
sourcePatientId	The sourcePatientId represents the subject of care medical record Identifier (e.g. Patient Id) in the local patient Identifier Domain of the Document Source. It shall contain two parts: Authority Domain Id An Id in the above domain (e.g. Patient Id). This sourcePatientId is not intended to be updated once the Document is registered (just as the Document content and metadata itself will not be updated without replacing the previous document). As this sourcePatientId may have been merged by the source actor, it may no longer be in use within the Document Source (EHR-CR). It is only intended as an audit/checking mechanism and has occasional use for Document Consumer Actors. There can be only one Slot named sourcePatientInfo. ```<rim:Slot name="sourcePatientId"> <rim:ValueList> <rim:Value>j98789^^^id.domain</rim:Value> </rim:ValueList> </rim:Slot>```	R/P	CX

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints	

sourcePatientInfo	This attribute should contain demographics information of the patient to whose medical record this document belongs, as the Document Source knew it at the time of Submission. This information typically includes: the patient first and last name, sex, and birth date. The Clinical XDS Affinity Domain policies may require more or less specific information and format. This patient information is not intended to be updated once the Document is registered (just as the Document content and metadata itself will not be updated without replacing the previous document). As sourcePatientInfo may have been updated by the source actor, it may no longer be in use within the Document Source (EHR-CR). It is only intended as an audit/checking mechanism and has occasional use for Document Consumer actors. Shall have a single value (only a single sourcePatientInfo slot may be present).
	
	`<rim:Slot name="sourcePatientInfo">`
	`  <rim:ValueList>`
	`<rim:Value>PID-3|DTP-1^^^&1.3.6.1.4.1.21367.2005.3.7&ISO</rim:Value>`
	`    <rim:Value>PID-5|DICTAPHONE^ONE^^^</rim:Value>`
	`    <rim:Value>PID-7|19650120</rim:Value>`
	`    <rim:Value>PID-8|M</rim:Value>`
	`    <rim:Value>PID-11|100 Main St^^BURLINGTON^MA^01803^USA</rim:Value>`
	`  </rim:ValueList>`
	`</rim:Slot>`
	
	PID-3 should include the source patient identifier.
	PID-5 should include the patient name.
	PID-8 should code the patient gender as
	        M – Male F – Female
	        O – Other U – Unknown
	PID-7 should include the patient date of birth.
	
	PID-11 should include the patient address.
	
	PID-2, PID-4, PID-12 and PID-19 should not be used.
		O/P		

title	Represents the title of the document. Clinical documents often do not have a title, and are collectively referred to by the display name of the classCode (e.g. a "consultation" or "progress note"). Where these display names are rendered to the clinician, or where the document has a unique title, the title component shall be used. Max length, 128 bytes, UTF-8. If	O/P		

XDSDocumentEntry Attribute	Definition	Source/Query	Constraints

	present, shall have a single value.
	
	``<rim:ExtrinsicObject
	  id="theDocument"
	  objectType=
	    "urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
	  mimeType="application/pdf"
	>
	  <rim:Name>
	      <rim:LocalizedString value="title"/>
	  </rim:Name>
	      …
	</rim:ExtrinsicObject>```		

typeCode	The code specifying the precise kind of document (e.g. Pulmonary History and Physical, Discharge Summary, Ultrasound Report). It is suggested that the XDS Affinity Domain draw these values from a coding scheme providing a fine level of granularity. Shall have a single value.
	
	``<rim:Classification
	  classificationScheme=
	    "urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
	  classifiedObject="theDocument"
	  nodeRepresentation="typeCode"
	>
	  <rim:Name>
	    <rim:LocalizedString
	      value="typeCodeDisplayName"
	    />
	  </rim:Name>
	  <rim:Slot name="codingScheme">
	      <rim:ValueList>
	      <rim:Value>XDS Affinity Domain Specific Value</rim:Value>
	    </rim:ValueList>
	  </rim:Slot>
	</rim:Classification>```
		R/R	XDS Affinity Domain specific

typeCodeDisplayName	The name to be displayed for communicating to a human the meaning of the typeCode. Shall have a single value for each value of typeCode. See typeCode for an example.	R/P	XDS Affinity Domain specific
uniqueId	The globally unique identifier assigned by the document creator to this document. This unique identifier may be used in the body of other XDS Documents to reference this document. The length of Unique Identifier shall not exceed 128 bytes. The structure and format of this Id shall be consistent with the specification corresponding to the format attribute. (e.g. for a DICOM standard document a 64 character numeric UID, for an HL7 CDA format a serialization of the CDA Document id extension and root in the form oid^extension, where OID is a 64 digits max, and the ID is a	R/R	See section 4.1.7.2

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints	
	16 UTF-8 char max). If the oid is coded without the extension then the '^' character shall not be included.			
	This uniqueId is intended to respond to the following types of usage:			
	The means to reference this XDS document from within the content of another document. Neither the XDS Registry nor the Repository is aware of such references, but the Document Sources and Consumers are.			
	The means to ensure that when a XDS Document is retrieved from the XDS Document Repository using the URI component, the selected XDS Document is the correct one.			
	Shall have a single value.			

	<pre><rim:ExternalIdentifier
	  identificationScheme=
	    "urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
	  value="*1.3.6.1.4.1.21367.2005.3.7^11379*"
	>
	  <rim:Name>
	    <rim:LocalizedString value="XDSDocumentEntry.uniqueId"/>
	  </rim:Name>
	</rim:ExternalIdentifier></pre>			

URI	When used in the Register Document Set transaction, this contains the URI of the XDS Document to be used for retrieval.	Cp/P	URI See sections 3.14.4.1. 2 3.15.4.1	
	If present, shall have a single value.			
	XDS does not constraint the format of this URI beyond RFC 2616. However, the IHE Retrieve Information for Display Integration Profile defined format may be used in cases where the Document repository is grouped with a RID Information Source Actor (See ITI TF-1:Appendix E.5)			
	RID links can be used only if they yield the document in full fidelity.			

	There are two formats for coding this attribute. If the string representing the URI is 128 characters or shorter, the short format may be used:
	<pre><rim:Slot name="URI">
	  <rim:ValueList>
	    <rim:Value>http://www.ihe.net</rim:Value>
	  </rim:ValueList>
	</rim:Slot></pre>			

	If the string is more than 128 characters long, the long format shall be used:			

XDSDocumentEntry Attribute	Definition	Source/ Query	Constraints
| | ```
<rim:Slot name="URI">
  <rim:ValueList>
    <rim:Value>1|http://www.ihe.net/IHERetrieveDocument?
    </rim:Value>
    <rim:Value>2|requestType=DOCUMENT&documentUID=1.2.3
    </rim:Value>
    <rim:Value>3|&preferredContentType=application%2fpdf
    </rim:Value>
  </rim:ValueList>
</rim:Slot>
```<br><br>Each Value is composed of an ordering prefix followed by a portion of the actual URI string. The ordering prefix shall be sequential starting at the value 1. When the long format is used, all Values shall have an ordering prefix.<br><br>Each value is ordered by its ordering prefix:<br>    ordering-prefix :== digit vertical-bar<br>    digit :== '1' \| '2' \| '3' \| '4' \| '5' \| '6' \| '7' \| '8' \| '9'<br>    vertical-bar :== '\|'<br><br>The long version may be used for URIs of less than 129 characters. This profile does not specify how a URI is to be broken up into pieces. The following example is valid.<br><br>```
<rim:Slot name="URI">
  <rim:ValueList>
    <rim:Value>1|http://www.ihe.net</rim:Value>
  </rim:ValueList>
</rim:Slot>
```<br><br>The long version is assembled into a URI by concatenating the Values without the ordering prefixes in the order specified by the ordering-prefixes. | | |

4.1.7.1 XDSDocumentEntry.formatCode

8165 In general, the repository holds an octet stream representing the document. The registry metadata describes, among other things, the format of the document. This is coded in XDSDocumentEntry.formatCode. This code will identify document format parameters necessary for interoperability. Rules about handling the formatCode are necessary but are not imposed by XDS. In the future IHE content specific Integration Profiles may be created that specify these rules.

8170   Note: Although only a small number of document standards may be used, a large number of code values may be defined to point to specific templates and archetypes structuring specific document content.

4.1.7.2 **XDSDocumentEntry.uniqueId**

The specification of the format and encoding for this attribute depends on the document standard defining the content of the XDS Document (*e.g.* OID with optional extension ID for HL7 CDA, UUID in some cases, SOP Instance UID for DICOM composite objects. Format is: OID^Extension). This attribute shall not exceed 128 bytes in size. It shall be used as an opaque and globally unique identifier for the XDS Document. Document Consumers, Registries, Repositories shall not attempt to interpret its content. When the Extension is not present, the '^' character shall not be included.

4.1.8 **Submission Set Metadata**

The following metadata elements shall be used to describe an XDS Submission Set. They shall be provided by the Document Source Actor in the Provide and Register Document Set transaction. They shall be provided by the Document Repository Actor in the Register Document Set Transaction either directly if grouped with a Document Source Actor or forwarded from a Provide and Register Document Set Transaction.

Each of the attributes listed below is an attribute on the RegistryPackage object defining the Submission Set. The attribute name is defined with a prefix of the object type of XDSSubmissionSet when referenced by other objects, for example XDSSubmissionSet.sourceId.

In the attribute tables below, when an OID format is specified, it shall follow the assignment and format rules defined for document UID in ITI TF-2 : Appendix B.

Table 4.1-6 Submission Set Metadata Attribute Definitions

XDSSubmission Set Attribute	Definition	Source/ Query	Constrains
author	Represents the humans and/or machines that authored the document. This attribute contains the following sub-attributes: • authorInstitution • authorPerson • authorRole • authorSpecialty which are individually defined below. The author attribute is defined as a Classification which contains the above sub-attributes. The author attribute itself does not have a simple value. It defines a structure to hold its sub-attributes. An instance of this Classification shall be considered a single value of the author attribute. If present, the author attribute shall have one or more values. Each instance of this Classification shall contain: • One instance of the authorPerson sub-attribute • Zero or more instances of the authorInstitution sub-attribute	R2/R	ebRIM

XDSSubmission Set Attribute	Definition	Source/ Query	Constrains

	• Zero or more instances of the authorRole sub-attribute
	• Zero or more instances of the authorSpecialty sub-attribute
	
	The following example shows the definition of a single author. The classification shows the required authorPerson Slot holding the required single value. Single values are shown for authorInstitution, authorRole, and authorSpecialty. Multiple values for these three sub-attributes, if present, shall be coded as additional Value elements within the Slot/ValueList having the correct name.
	
	`<rim:Classification`
	`  classificationScheme="urn:uuid:a7058bb9-b4e4-4307-ba5b-`
	`e3f0ab85e12d"`
	`  classifiedObject="theDocument"`
	`  nodeRepresentation="">`
	`<!-- nodeRepresentation intentionally left blank -->`
	
	`  <rim:Slot name="authorPerson">`
	`    <!-- shall be single valued -->`
	`    <rim:ValueList>`
	`      <rim:Value>name of author</rim:Value>`
	`    </rim:ValueList>`
	`  </rim:Slot>`
	
	`  <rim:Slot name="authorInstitution">`
	`    <!-- may be multivalued -->`
	`    <rim:ValueList>`
	`      <rim:Value>name of institution</rim:Value>`
	`    </rim:ValueList>`
	`  </rim:Slot>`
	
	`  <rim:Slot name="authorRole">`
	`    <!-- may be multivalued -->`
	`    <rim:ValueList>`
	`      <rim:Value>name of role</rim:Value>`
	`    </rim:ValueList>`
	`  </rim:Slot>`
	
	`  <rim:Slot name="authorSpecialty">`
	`    <!-- may be multivalued -->`
	`    <rim:ValueList>`
	`      <rim:Value>specialty of author</rim:Value>`
	`    </rim:ValueList>`
	`  </rim:Slot>`
	
	`</rim:Classification>`		

authorInstitution (sub-attribute of author)	Represents a specific healthcare facility under which the human and/or machines authored the Submission Set. This is a sub-attribute of the author attribute. See the author attribute for definition of the requirements of usage. `See author for example.`	R2/R	XON

XDSSubmission Set Attribute	Definition	Source/ Query	Constrains
authorPerson (sub-attribute of author)	Represents the human and/or machines that authored the Submission Set. The document author may be the patient itself. This is a sub-attribute of the author attribute. See the author attribute for definition of the requirements of usage. `See author for example.`	O/R	XCN
authorRole (sub-attribute of author)	A code that represents the role of the author with respect to the patient when the submission set was created. This is a sub-attribute of the author attribute. See the author attribute for definition of the requirements of usage. `See author for example.`	R2/O	
authorSpecialty (sub-attribute of author)	Represents a specific specialty within a healthcare facility under which the human and/or machines authored the submission set. This is a sub-attribute of the author attribute. See the author attribute for definition of the requirements of usage. `See author for example.`	R2/O	

availabilityStatus	An XDSSubmissionSet shall have one of two availability statuses:
	Submitted submission transaction not completed, not available for patient care
	Approved available for patient care
	This attribute is always set to Approved as part of a successful submission of new XDS Documents. XDS does not allow for the deprecation of Submission Sets.
	
	See section 4.1.3.3 Atomicity Requirements for XDS Submission Requests for additional details.
	
	If present, shall have a single value.
	
	The example below shows the status attribute, however, this attribute is only returned on query, not set during any registry or repository transaction.
	
	`<rim:RegistryPackage`
	` id="urn:uuid:fbeacdb7-5421-4474-9267-985007cd8855"`
	` status="Approved"`
	`> ...`
		Cg/R	

XDSSubmission Set Attribute	Definition	Source/ Query	Constrains

comments	Comments associated with the Submission Set. Free form text with an XDS Affinity Domain specified usage.
	
	`<rim:Description>`
	`  <rim:LocalizedString value = "comments"/>`
	`</rim:Description>`
		O/P	Use specific to XDS Affinity Domain.

contentTypeCode	The code specifying the type of clinical activity that resulted in placing these XDS Documents in this XDS-Submission Set. These values are to be drawn for a vocabulary defined by the XDS Affinity Domain. Shall have a single value.
	
	`<rim:Classification`
	`  classificationScheme=`
	`    "urn:uuid:aa543740-bdda-424e-8c96-df4873be8500"`
	`  classifiedObject="submissionSet"`
	`  nodeRepresentation="contentTypeCode"`
	`>`
	`  <rim:Name>`
	`    <rim:LocalizedString`
	`      value="contentTypeCodeDisplayName" />`
	`  </rim:Name>`
	`  <rim:Slot name="codingScheme">`
	`    <rim:ValueList>`
	`      <rim:Value>XDS Affinity Domain Specific Value</rim:Value>`
	`    </rim:ValueList>`
	`  </rim:Slot>`
	`</rim:Classification>`
		R/R	XDS Affinity Domain specific

contentTypeCode DisplayName	The name to be displayed for communicating to a human the meaning of the contentTypeCode. Shall have a single value for each value of contentTypeCode. See contentTypeCode for an example.	R/P	XDS Affinity Domain specific

entryUUID	The globally unique identifier (may be assigned by either by Source, Repository, or Registry) is primarily intended for use as a document registry management identifier. It is not meant to be an external reference for XDS Documents (e.g. in links within other documents). The uniqueId is meant for that purpose so that such links remain valid beyond the XDS Affinity Domain. If present, shall have a single value.
	
	In the example below, the entryUUID is
	
	`  urn:uuid:a6e06ca8-0c75-4064-9e5d-88b9045a9ab6`
	
	`<rim:RegistryPackage mimeType="application/pdf"`
	` id="urn:uuid:a6e06ca8-0c75-4064-9e5d-88b9045a9ab6"`
	`> ...`
		Cg/O	UUID

XDSSubmission Set Attribute	Definition	Source/ Query	Constrains

intendedRecipient	Represents the organization(s) or person(s) for whom the Submission set is intended. If present, shall have one or more values. Each entry should include one organization, one person, or both. Example below shows two doctors from the same organization, another doctor without precision of the organization and another organization without the precision of the person. If this attribute is received in a Provide and Register Document Set or Register Document Set transaction, it shall be ignored.
	
	Note: It is highly recommended to define the organization for all the persons, avoiding errors in the transmission of the documents internally at the Document Recipient side. There is a "|" character separator between the organization and the person, which is required when the person information is present.
	
	<pre><rim:Slot name="intendedRecipient">
	    <rim:ValueList>
	        <rim:Value>Fair
	Clinic^L^716|^Wel^Marcus^^^Dr^MD</rim:Value>
	        <rim:Value>Fair
	Clinic^L^716|^Al^Peter^^^Dr^MD</rim:Value>
	        <rim:Value>|12345^John^Smith^^^Dr^MD</rim:Value>
	        <rim:Value>Main Hospital</rim:Value>
	    </rim:ValueList></rim:Slot></pre>
		O/O	XON/X CN

patientId	The patientId represents the medical record identifier of subject of care whose longitudinal record is being maintained, as selected by the Document Source. Attaching an existing document for patient A to a folder for patient B is presumed in this case to be an update to the longitudinal record for patient B. In this case, the Submission Set patientId would be that of patient B. This identifier shall be from the Assigning Authority Domain supporting the XDS Affinity Domain in which the Document Registry operates. It shall contain two parts: Authority Domain Id (enforced by the Registry) An Id in the above domain. No other values are allowed, as specified for the CX type in Table 4.1-3 above. Using HL7 terminology, no other values are allowed in the components of the coded value, nor are further subcomponents allowed.	R/R	CX

XDSSubmission Set Attribute	Definition	Source/ Query	Constrains

	The value of the patientId shall be the same for all new documents of a Submission Set.
	
	Shall have a single value.
	
	``
	<rim:ExternalIdentifier
	  identificationScheme=
	    " urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446"
	  value="6578946^^^&1.3.6.1.4.1.21367.2005.3.7&ISO"
	>
	  <rim:Name>
	    <rim:LocalizedString value = "XDSSubmissionSet.patientId"/>
	  </rim:Name>
	</rim:ExternalIdentifier>
	``		

sourceId	OID identifying the instance of the Document Source that contributed the Submission Set. When a "broker" is involved in sending submission sets from a collection of client systems, it should use a different source ID for submissions from each separate system to allow for tracking. Shall have a single value.
	
	``
	<rim:ExternalIdentifier
	  identificationScheme=
	    "urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832"
	  value="1.3.6.1.4.1.21367.2005.3.7"
	>
	  <rim:Name>
	    <rim:LocalizedString value = "XDSSubmissionSet.sourceId"/>
	  </rim:Name>
	</rim:ExternalIdentifier>
	``
		R/R	OID

submissionTime	Point in Time at the Document Source when the Submission Set was created and issued for registration to the Document Registry. Shall have a single value. This shall be provided by the Document Source (in case of e-mail with significant delay). ``` <rim:Slot name="submissionTime"> <rim:ValueList> <rim:Value>20041225212010</rim:Value> </rim:ValueList> </rim:Slot> ```	R/R	DTM
title	Represents the title of the Submission Set. If present, shall have a single value. ``` <rim:Name> <rim:LocalizedString value="title"/> </rim:Name> ```	O/P	XDS Affinity Domain specific
uniqueId	Globally unique identifier for the submission-set instance assigned by the Document Source in OID format. Shall have a single value.	R/R	OID See

XDSSubmission Set Attribute	Definition	Source/ Query	Constrains
| | ```
<rim:ExternalIdentifier
  identificationScheme=
    " urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8"
  value="1.3.6.1.4.1.21367.2005.3.7.3670984664">
  <rim:Name>
    <rim:LocalizedString value = "XDSSubmissionSet.uniqueId"/>
  </rim:Name>
</rim:ExternalIdentifier>
``` | | Append ix B |

4.1.8.1 Creating an XDSSubmissionSet object from a RegistryPackage element

An XDSSubmissionSet object shall be created from a RegistryPackage element by labeling it with a
8195 Classification of type urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd. A receiver of metadata shall accept the Classification element coded within the RegistryPackage element or on the same level. The following XML example demonstrates these two valid approaches to coding the Classification.

Classification coded inside the RegistryPackage object

```
<…>
    <RegistryPackage id="SS">
        <!-- Classify registry package SS as being an XDSSubmissionSet -->
        <Classification classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-
b4633d873bdd" classifiedObject="SS"/>
    </RegistryPackage>
    <RegistryPackage id="Fol">
        <!-- Classify registry package Fol as being an XDSFolder -->
        <Classification classificationNode="urn:uuid:d9d542f3-6cc4-48b6-8870-
ea235fbc94c2" classifiedObject="Fol"/>
    </RegistryPackage>
<…>
```

8200

Classification coded outside the RegistryPackage object

```
<…>
    <RegistryPackage id="SS">
    </RegistryPackage>
    <!-- Classify registry package as XDSSubmissionSet -->
    <Classification classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-
b4633d873bdd" classifiedObject="SS"/>
    <RegistryPackage id="Fol">
```

_____

```
    </RegistryPackage>
    <!-- Classify registry package as XDSFolder  -->
    <Classification classificationNode="urn:uuid:d9d542f3-6cc4-48b6-8870-
ea235fbc94c2" classifiedObject="Fol"/>
<…>
```

The following UUIDs shall be used to label RegistryPackage elements as Submission Set or Folder

Object being coded	UUID used on the Classification
Submission Set	urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd
Folder	urn:uuid:d9d542f3-6cc4-48b6-8870-ea235fbc94c2

8205

4.1.9 Folder Metadata

The following metadata elements shall be used to describe an XDS Folder. They shall be provided by the Document Source Actor in the Provide and Register Document Set transaction. They shall be provided by the Document Repository Actor in the Register Document Set transaction if this transaction
8210   is used outside the context of a Provide and Register Document Set transaction.

Each of the attributes listed below is an attribute on the RegistryPackage object defining the Folder. The attribute name is defined with a prefix of the object type of XDSFolder when referenced by other objects, for example XDSFolder.patientId.

In the attribute tables below, when an OID format is specified, it shall follow the assignment and format
8215   rules defined for document UID in ITI TF-2 : Appendix B.

Note: Prior to the availability of this attribute the comments attribute might have been used to hold the title of the folder (folder name). With the addition of this attribute the comments attribute shall not be expected to hold the folder name.

8220   **Table 4.1-7 Folder Metadata Attribute Definitions**

XDSFolder Attribute	Definition	Source/ Query	Constrains
availabilityStatus	An XDSFolder shall have one of two availability statuses: Submitted submission transaction not completed, not available for patient care Approved available for patient care This attribute is always set to Approved as part of a successful submission of new XDS Folders. XDS does not allow for the deprecation of Folders. See section 4.1.3.3 Atomicity Requirements for XDS	Cg/R	

XDSFolder Attribute	Definition	Source/ Query	Constrains
	Submission Requests for additional details. If present, shall have a single value. The example below shows the status attribute, however, this attribute is only returned on query, not set during any registry or repository transaction. ``` <rim:RegistryPackage id="urn:uuid:fbeacdb7-5421-4474-9267-985007cd8855" status="Approved" > ... ```		

codeList	The list of codes specifying the type of clinical activity that resulted in placing these XDS Documents in this XDSFolder. These values are to be drawn for a vocabulary or coding scheme defined by the Clinical XDS Affinity Domain.
	
	When a new submission request associates XDS Documents (new submission or previously submitted) to an XDS Folder, the Code included in the codeList is appended to the existing list of codes for this Folder (if any) unless this code is already present in the list managed by the Registry for the same XDS-Folder.
	
	Only one code may be assigned to the Folder when an XDS Document is placed in a Folder. Shall have one or more values.
	
	``
	<rim:Classification
	  classificationScheme=
	    "urn:uuid:1ba97051-7806-41a8-a48b-8fce7af683c5"
	  classifiedObject="Folder"
	  nodeRepresentation="codeList"
	>
	  <rim:Name>
	    <rim:LocalizedString
	      value="codeListCodeDisplayName" />
	  </rim:Name>
	  <rim:Slot name="codingScheme">
	    <rim:ValueList>
	      <rim:Value>XDS Affinity Domain Specific Value</rim:Value>
	    </rim:ValueList>
	  </rim:Slot>
	</rim:Classification>
	``
		R/R	Multi-Valued. XDS Affinity Domain specific

codeListDisplay Name	The list of human readable descriptions of the meaning of each of the codes present in the codeList. Shall have a single value corresponding to each value in codeList. Only one code may be assigned to the Folder when an XDS Document is placed in such a Folder.	R/P	Multi-valued.

XDSFolder Attribute	Definition	Source/ Query	Constrains
	See codeList for an example.		

comments	Comments associated with the Folder. Free form text with an XDS Affinity Domain specified usage.
	
	`<rim:Description>`
	`  <rim:LocalizedString value = "`**`comments`**`"/>`
	`</rim:Description>`
		O/P	XDS Affinity Domain specific.

entryUUID	The globally unique identifier (may be assigned by either by Source, Repository, or Registry) is primarily intended for use as a document registry management identifier. It is not meant to be an external reference for XDS Documents (e.g. in links within other documents). The uniqueId is meant for that purpose so that such links remain valid beyond the XDS Affinity Domain. If present, shall have a single value.
	
	In the example below, the entryUUID is
	`     urn:uuid:a6e06ca8-0c75-4064-9e5c-88b9045a9ab6`
	
	`<rim:RegistryPackage mimeType="application/pdf"`
	` id="urn:uuid:a6e06ca8-0c75-4064-9e5c-88b9045a9ab6"`
	`> ...`
		Cg/O	UUID

lastUpdateTime	Point in time at the Document Registry when an XDS Document was registered and placed in the XDS Folder. If present, shall have a single value.
	
	`<rim:Slot name="lastUpdateTime">`
	`  <rim:ValueList>`
	`    <rim:Value>20041225212010</rim:Value>`
	`  </rim:ValueList>`
	`</rim:Slot>`
	
	The Document Registry shall set lastUpdateTime on submission of folder. The value in the submission request (if present), shall be ignored.
		Cg/R	DTM

patientId	The patientId represents the subject of care medical record Identifier as defined by the Document Source. This identifier shall be from the Assigning Authority Domain supporting the XDS Affinity Domain in which the Document Registry operates. It shall contain two parts: Authority Domain Id (enforced by the Registry) An Id in the above domain. No other values are allowed, as specified for the CX type in Table 4.1-3 above. Using HL7 terminology, no other values	R/R	CX

XDSFolder Attribute	Definition	Source/Query	Constrains
	are allowed in the components of the coded value, nor are further subcomponents allowed. The value of the patientId shall be the same for all new documents of a Folder. Shall have a single value. ```<rim:ExternalIdentifier identificationScheme= " urn:uuid:f64ffdf0-4b97-4e06-b79f-a52b38ec2f8a " value="6578946^^^&1.3.6.1.4.1.21367.2005.3.7&ISO" > <rim:Name> <rim:LocalizedString value = "XDSFolder.patientId"/> </rim:Name> </rim:ExternalIdentifier>```		
title	Represents the title of the Folder. If present, shall have a single value. ```<rim:Name> <rim:LocalizedString value="title"/> </rim:Name>```	O/P	XDS Affinity Domain specific
uniqueId	Globally unique identifier for the XDS-Folder in which one or more XDS Documents are placed. It is assigned by the Document Source at the time the XDS Folder is created in OID format. Shall have a single value. ```<rim:ExternalIdentifier identificationScheme= "urn:uuid:75df8f67-9973-4fbe-a900-df66cefecc5a" value="1.3.6.1.4.1.21367.2005.3.7.3670984664"> <rim:Name> <rim:LocalizedString value = "XDSFolder.uniqueId"/> </rim:Name> </rim:ExternalIdentifier>```	R/R	OID See Appendix B

4.1.9.1 Creating an XDSFolder object from a RegistryPackage element

An XDSFolder object shall be created from a RegistryPackage element by labeling it with a Classification of type urn:uuid:d9d542f3-6cc4-48b6-8870-ea235fbc94c2. A receiver of metadata shall
8225   accept the Classification element coded within the RegistryPackage element or on the same level. The following XML example demonstrates these two valid approaches to coding the Classification.

Classification coded inside the RegistryPackage object

```
<…>
    <RegistryPackage id="SS">
```

```
        <!-- Classify registry package SS as being an XDSSubmissionSet -->
        <Classification classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-
b4633d873bdd" classifiedObject="SS"/>
    </RegistryPackage>
    <RegistryPackage id="Fol">
        <!-- Classify registry package Fol as being an XDSFolder -->
        <Classification classificationNode="urn:uuid:d9d542f3-6cc4-48b6-8870-
ea235fbc94c2" classifiedObject="Fol"/>
    </RegistryPackage>
<…>
```

Classification coded outside the RegistryPackage object

```
<…>
    <RegistryPackage id="SS">
    </RegistryPackage>
    <!-- Classify registry package as XDSSubmissionSet -->
    <Classification classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-
b4633d873bdd" classifiedObject="SS"/>
    <RegistryPackage id="Fol">
    </RegistryPackage>
    <!-- Classify registry package as XDSFolder  -->
    <Classification classificationNode="urn:uuid:d9d542f3-6cc4-48b6-8870-
ea235fbc94c2" classifiedObject="Fol"/>
<…>
```

8230

The following UUIDs shall be used to label RegistryPackage elements as Submission Set or Folder

Object being coded	UUID used on the Classification
Submission Set	urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd
Folder	urn:uuid:d9d542f3-6cc4-48b6-8870-ea235fbc94c2

4.1.10 Registry Adaptor Enforcement of Attributes

ebRIM version 2.1 datatype Slot/ValueList/Value is limited to 128 characters by that standard. Many
8235 HL7 datatypes, which the attribute tables show as being encoded as a Slot, can be much larger. The
Document Source shall encoded these Slots so they fit into the 128 character space allocated to them.
This may require some information to be excluded. This profile gives no guidance as to how information
is to be excluded to make this coding limit.

The Registry Adaptor shall reject any submission which includes attribute values whose size exceeds the
8240 specification in the standard.

Table 4.1-8 Document Metadata Attribute Enforcement

XDSDocumentEntry Attribute	Registry Enforcement
availabilityStatus	No enforcement
authorInstitution	No enforcement
authorPerson	No enforcement
authorRole	No enforcement
authorSpecialty	No enforcement
classCode	Coding Scheme and Code Value.
classCodeDisplayName	Must match classCode
confidentialityCode	Coding Scheme and Code Value
confidentialityCodeDisplayName	Must match confidentialityCode
creationTime	No enforcement
entryUUID	No enforcement
eventCodeList	Coding Scheme and Code Value
eventCodeDisplayNameList	Must match eventCodeList
formatCode	Coding Scheme and Code Value
formatCodeDisplayName	Must match formatCode
hash	No enforcement
healthcareFacilityTypeCode	Coding Scheme and Code Value
healthcareFacilityTypeCodeDisplayName	Must match healthcareFacilityTypeCode
legalAuthenticator	No enforcement
languageCode	Optionally enforced by XDS Affinity Domain
mimeType	Code Value
parentDocumentRelationship	One of four values
parentDocumentId	Existing UUID
patientId	Authority Domain Id Patient Id (known from patient identity feed)
practiceSettingCode	Coding Scheme and Code Value
practiceSettingCode DisplayName	Must match practiceSettingCode
serviceStartTime	No enforcement
serviceStopTime	Verifies serviceStartTime <= serviceStopTime
size	No enforcement
sourcePatientId	No enforcement
sourcePatientInfo	Some parts required
title	No enforcement
typeCode	Coding Scheme and Code Value
typeCodeDisplayName	Must match typeCode
uniqueId	See section 4.1.7.2
URI	No enforcement

Table 4.1-9 SubmissionSet Metadata Attribute Enforcement

XDSSubmissionSet Attribute	Registry Enforcement
authorInstitution	No enforcement
authorPerson	No enforcement
authorRole	No enforcement
authorSpecialty	No enforcement
comments	No enforcement
contentTypeCode	Coding Scheme and Code value
contentTypeCodeDisplayName	Must match contentTypeCode
patientId	Authority Domain Id Patient Id (known from patient identity feed)
sourceId	No enforcement
submissionTime	No enforcement
uniqueId	No identical existing uniqueId in registry acording to rules in section 4.1.7.2

8245

Table 4.1-10 Folder Metadata Attribute Enforcement

XDSFolder Attribute	Registry Enforcement
codeList	Coding Scheme and Code value
codeListDisplayName	Must match codeList
comments	No enforcement
lastUpdateTime	Shall be set to the current time on submission of folder or folder content changes.
patientId	The value of the patientId shall be the same for all documents of a Folder.
uniqueId	No identical existing uniqueId in registry (assigned to XDSDocumentEntry, XDSSubmissionSet, or XDSFolder)

4.1.11 XDS Registry Adaptor

The XDS Registry Adaptor is a set of functionality that is not provided for in the ebXML registry
8250 standard, but is instead specified by XDS to support integration into the healthcare environment. This
adaptor has the following responsibility:

> **Validate patient ID** – patient IDs (XDSDocumentEntry.patientId attribute) shall be a known patient
> ID and registered against the Patient ID Domain of the XDS Affinity Domain managed by
> the patient Identity Source Actor.

8255 **Validate submitted metadata** – the adaptor shall verify that submitted metadata meets XDS
> Registry metadata specification

Verify coded values – the adaptor shall verify that coded fields (ebXML external classifications) contain valid XDS specified values or where the XDS Affinity Domain constrains code values, to verify them (See Section 4.1.10).

8260   **Ensure submissions are atomic** - The adaptor shall make submission to registry an atomic operation – see section 4.1.3.3 Atomicity Requirements for Submission Requests for atomicity requirements.

If the registry submission is successful then the adaptor shall label all Document Entry, Folder, and Submission Set objects as Approved. The ebRIM specification provides the
8265   ApproveObjectsRequest for this purpose.

If the registry submission fails then the adaptor shall remove from the registry all objects stored as part of this submission set. The ebRIM specification provides the RemoveObjectsRequest for this purpose.

Support document replacement - When a Submission Request includes a 'RPLC' or
8270   'XFRM_RPLC' association indicating that a document is being replaced, the following shall be true:

Document to be replaced must have status = Approved.

The association's sourceObject attribute shall contain the **id** (UUID or symbolic id) of an ExtrinsicObject representing an XDSDocumentEntry included in the Submission Set.

8275   The association's targetObject attribute shall contain the UUID of an ExtrinsicObject (XDSDocumentEntry) already in the registry.

When the 'RPLC' or 'XFRM_RPLC' association is detected by the Registry Adaptor it shall:

Verify the ExtrinsicObject pointed to by the Association's targetObject attribute is present in the registry and has status of `Approved`. The error `XDSReplaceFailed` shall be
8280   thrown if this object is not contained in the registry or has status other than `Approved`. This ensures that only the most recent version of a document can be replaced.

Submit the Submission Request to the registry.

If the submission is successful, label the replacement document as Approved and the replaced document as Deprecated. The ebRIM requests ApproveObjectsRequest and
8285   DeprecateObjectsRequest are available to do this.

If the Document being replaced is a member of one or more Folders, generate HasMember Associations connecting the replacement Document with each of the Folders holding the original Document. This makes the replacement Document a member of all Folders where the original Document is a member.

8290

parentdocumentRelat ionShip			

parentDocumentRela tionshipCode	A attribute that may be placed on an Association of type XFRM, APND, RPLC, or XFRM_RPLC to document the reason the relationship was created.
	
	`<rim:Association id="ThisAssociation"`
	`  associationType="XFRM"`
	`  sourceObject="source"`
	`  targetObject="target">`
	`  <rim:Classification`
	`      classificationScheme="urn:uuid:abd807a3-4432-4053-`
	`87b4-fd82c643d1f3"`
	`      classifiedObject="ThisAssociation"`
	`      nodeRepresentation="French">`
	`    <rim:Name>`
	`      <rim:LocalizedString value="Translation into French"/>`
	`    </rim:Name>`
	`    <rim:Slot name="codingScheme">`
	`      <rim:ValueList>`
	`        <rim:Value>Connect-a-thon translation types</`
	`rim:Value>`
	`      </rim:ValueList>`
	`    </rim:Slot>`
	`  </rim:Classification>`
	`</rim:Association>`
	The relationshipTypeCode is defined by the Classification scheme inside the Association object. Note the required structural issues:
	
	• The classficationScheme is defined by this profile
	
	• The association shall have an id attribute and the classifiedObject shall reference it
	
	• The nodeRepresentation, name, and coding scheme shall be specified as with any other classification object specified within XDS.
		O/P	

Validate patientIDs in Folders - The adaptor shall verify that all documents in a folder are for the same patient. Specifically, verify that the patientId attribute of the folder matches the
8295 patientId attribute of each document in the folder.

Validate MIME types - The adaptor shall validate that the mimeType document attribute for all documents received is on the approved list for this XDS Affinity Domain.

Maintain Folder attribute 'lastUpdateTime' - The XDS Folder attribute lastUpdateTime shall be updated by the adaptor every time a new document is added to an XDS Folder.

8300 **Validate patientID on documents being added to a Folder** - The patientId attribute of an XDSDocumentEntry object shall match the patientId attribute on any folder that holds it.

Validate coding - The adaptor shall enforce the number of classifications offered against a document. Code lists are allowed to be multiples. Codes are required to be singular.

Accept submissions containing multiple documents – The adapter shall be capable of accepting
8305 submissions containing multiple documents.

4.1.12 General Metadata Issues

This section documents ebXML Registry issues that are confusing, underdocumented, or are in conflict between various versions of the registry specification.

4.1.12.1 Association Type naming

8310 XDS requires that Association names be specified as text names and not UUIDs. This is consistent with version 2.0 and 2.1 of ebRIM. XDS requires the use of the following standard Associations:

HasMember – for linking RegistryPackage objects to their contents

In addition, XDS defines a collection of Association types defined in section 4.1.6 Document Relationships and Associations.

8315 ### 4.1.12.2 Assigning Codes to Documents

Many attributes of XDSDocumentEntry, XDSSubmissionSet, and XDSFolder (Tables 4.1-5, 4.1-6, and 4.1-7) are coded attributes defined as ebRIM Classifications. Three details are required to describe a coded value:

1. The value of the code

8320 2. The display name of the code (raw codes are not human-friendly)

3. The name of the coding scheme that the code comes from.

These three values combine to define a single coded element.

As described in ebXML Registry metadata, a coded attribute looks like:

8325

```
<!--+++++++++++++++++++++++++++++++++++++++++++++++++
   --
   --      XdsDocumentEntry.classCode
   --
8330 +++++++++++++++++++++++++++++++++++++++++++++++++ -->
<rim:Classification
   classificationScheme=
      "urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
   classifiedObject="theDocument"
8335 nodeRepresentation="My Class Code">

   <!-- +++++++++++++++++++++++++++++++++++++++++++++++
      XdsDocumentEntry.classCodeDisplayName
      +++++++++++++++++++++++++++++++++++++++++++++++ -->
8340 <rim:Name>
       <rim:LocalizedString value="Display Name for My Class Code"/>
   </rim:Name>

   <!-- +++++++++++++++++++++++++++++++++++++++++++++++
8345 Coding scheme for classCode
      +++++++++++++++++++++++++++++++++++++++++++++++ -->
   <rim:Slot name="codingScheme">
      <rim:ValueList>
         <rim:Value>Name of the Coding Scheme (LOINC for example)</rim:Value>
8350 </rim:ValueList>
   </rim:Slot>
</rim:Classification>
```

A code is constructed as a Classification object. The relevant parts of this classification are:

8355   **Classification** – this element wraps the definition

classificationScheme attribute – this UUID references a Classification Scheme object already present in the registry. This Classification Scheme object and its UUID are predefined by XDS and serve as the defining 'type' for the code.

classifiedObject attribute – this references the object in metadata being classified. This can be
8360   specified as a UUID or as a symbolic name as shown in the example above.

nodeRepresentation attribute – this is the value of the code.

Name element - this is the display name for the code.

codingScheme Slot (Value sub-element) - this is the name of the coding scheme.

The XDS Affinity Domain defines the local configuration for each coding scheme. Specifically, it
8365 defines:

Name of the coding scheme – which must be used in the codingScheme Slot

Values for the code – one of which must be used in the nodeRepresentation attribute

Name for each code – which must be used in the Name element and must match the value for the code.

8370 Some code types allow multiple values. EventCodeList is an example. These codes contain the letters 'List' in their name. These codes are XML coded identically to the above example with one exception. The entire Classification element may be repeated to specify additional values.

The Registry Adaptor Function is responsible for validating codes against the configuration of the XDS Affinity Domain.

8375   Note: the attribute XDSDocumentEntry.languageCode is not encoded as shown above. See Tables 4.1-5 for details.

4.1.12.3 Formatting of UUIDs

UUIDs shall be formatted according to RFC4122. Furthermore, values 10 through 15 shall be formatted in hexadecimal using lower case 'a'-'f'. An example of a properly formatted UUID is:

    urn:uuid:10b545ea-725c-446d-9b95-8aeb444eddf3

8380 Registries shall only accept and produce lowercase UUIDs.

4.1.12.4 XML Namespaces

The Register Document Set, Provide and Register Document Set, and Query Registry transactions are SOAP requests/responses containing valid XML. All elements shall be namespace qualified. Namespaces must be present in all elements. All referenced namespaces must be defined within the
8385 transmission.

4.1.13 Error Reporting

Registry Services schema (ebRS 2.1 or 3.0) defines the RegistryError element for reporting details of errors or warnings. RegistryError contains two required attributes, errorCode and codeContext. The Registry actor and Repository actor shall return these two attributes with each error reported. Codes

---

8390   reported in errorCode shall be taken from Table 4.1-11. The error codes XDSRegistryError or XDSRepositoryError shall be returned if and only if a more detailed code is not available from this table for the condition being reported. The attribute codeContext shall contain details of the error condition that may be implementation specific.

The following attributes are required on the RegistryError element when reporting errors or warnings:

8395
- **errorCode** shall be a value taken from table 4.1-11
- **codeContext** supplies additional detail for the errorCode
- **severity** supplies a coded indication of the severity of the error:

        For ebRS 3.0 transactions:

            urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error

8400   urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning

        For ebRS 2.1:

            Error

            Warning

The body of all RegistryError elements shall be empty.

8405   The following attributes on the RegistryError element are optional:

- **location** supplies the location of the error: module name and line number or stack trace if appropriate.
- **highestSeverity** – supplies the severity of the most severe error (this attribute is not available in ebRS 2.1)

8410   The value of the status attribute of either the RegistryResponse or AdHocQueryResponse elements shall be taken from the following lists. For Version 3.0 ebRIM/ebRS:

        urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure

        urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success

        urn:ihe:iti:2007:ResponseStatusType:PartialSuccess

8415   For version 2.1 ebRIM/ebRS:

        Failure

        Success

        PartialSuccess

Tables 4.1-12 through 4.1-15 control the reporting of errors for transactions that use the ebRS/ebRIM

8420   schemas.

An example of an error response reporting two errors using ebRS and ebRIM version 2.1 is:

```
<RegistryResponse
    xmlns="urn:oasis:names:tc:ebxml-regrep:registry:xsd:2.1"
    status="Failure">
  <RegistryErrorList>
```
8425

```
        <RegistryError
          errorCode="XDSPatientIdDoesNotMatch"
          codeContext="Patient ID in Document (Document1) does not match Submission Set"
8430      location=""
          severity="Error"/>
        <RegistryError
          errorCode="XDSRegistryMetadataError"
          codeContext="RegistryPackage (SubmissionSet) is not labeled as SubmissionSet or Folder"
8435      severity="Error"
          location="" />
      </RegistryErrorList>
    </RegistryResponse>
```

8440   An example of an error response reporting two errors using ebRS and ebRIM 3.0 is:

```
    <RegistryResponse
        xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
        status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">
8445     <RegistryErrorList
          highestSeverity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error">
        <RegistryError
          errorCode="XDSPatientIdDoesNotMatch"
          codeContext="Patient ID in Document (Document1) does not match Submission Set"
8450      location=""
          severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"/>
        <RegistryError
          errorCode="XDSRegistryMetadataError"
          codeContext="RegistryPackage (SubmissionSet) is not labeled as SubmissionSet or Folder"
8455      location=""
          severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"/>
      </RegistryErrorList>
    </RegistryResponse>
```

8460

Table 4.1-11 – Error Codes

Error Code	Discussion	Transaction P = Provide and Register R = Register Q= Query SQ=Stored Query
XDSMissingDocument	XDSDocumentEntry exists in metadata with no corresponding attached document	P
XDSMissingDocumentMetadata	MIME package contains MIME part with Content-Id header not found in metadata	P
XDSRegistryNotAvailable	Repository was unable to access the Registry	P
XDSRegistryError XDSRepositoryError	Internal Registry/Repository Error.	P,R P
XDSRegistryDuplicateUniqueIdInMessage XDSRepositoryDuplicateUniqueIdInMessage	A UniqueId value was found to be used more than once within the submission. Error code indicates where error was detected. CodeContext shall indicate the duplicate UniqueId.	P,R
XDSDuplicateUniqueIdInRegistry	UniqueId received was not unique within the Registry. UniqueId could have been attached to XDSSubmissionSet or XDSFolder. CodeContext shall indicate which and the value of the non-unique uniqueId. This error cannot be thrown for XDSDocumentEntry. See XdsNonIdenticalHash.	P,R P
XDSNonIdenticalHash	Document being registered was a duplicate (uniqueId already in registry) but hash does not match. CodeContext indicates UniqueId.	R
XDSRegistryBusy XDSRepositoryBusy	Too much activity	P,R,Q,SQ
XDSRegistryOutOfResources XDSRepositoryOutOfResources	Resources are low.	P,R,Q,SQ
XDSRegistryMetadataError XDSRepositoryMetadataError	Error detected in metadata. Actor name indicates where error was detected. CodeContext indicates nature of problem.	P,R
XDSTooManyResults		Q,SQ
XDSExtraMetadataNotSaved	This warning is returned if extra metadata was present but not saved in the registry.	P,R
XDSUnknownPatientId	Patient ID referenced in metadata is not known to the Registry actor via the Patient Identity Feed or is unknown because of patient identifier merge or other reasons. The codeContext shall include the value of	P,R

	patient ID in question.	
XDSPatientIdDoesNotMatch	XDS specifies where patient IDs must match between documents, submission sets, and folders. This error is thrown when the patient ID is required to match and does not. The codeContext shall indicate the value of the Patient Id and the nature of the conflict.	P,R
XDSUnknownStoredQuery	The Query ID provided in the request is not recognized.	SQ
XDSStoredQueryMissingParam	A required parameter to a stored query is missing.	SQ
XDSStoredQueryParamNumber	A parameter which only accepts a single value is coded with multiple values	SQ
XDSSqlError	All errors in executing an SQL query (Query Registry transaction [ITI-16] shall return this error code.	Q
XDSRegistryDeprecatedDocumentError	The Register transaction was rejected because it submitted an Association referencing a deprecated document.	P,R

The following tables explain the meaning of the status attribute in responses from the Registry or Repository.

8465   In the following tables, the values shown in the RegistryResponse Status and AdhocQueryResponse Status columns shall be prefixed by the namespace

urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:

or

urn:ihe:iti:2007:ResponseStatusType: (for PartialSuccess)

8470   when used with ebRS 3.0. The values shall be used as presented (no namespace) with ebRS 2.1.

Table 4.1-12 – Provide & Register Document Set Responses

RegistryResponse status	RegistryErrorList element	Result
Success	May be present. If present will contain one or more RegistryError elements with warning severity, none with error severity	All metadata and documents were successfully registered
Failure	Present, contains one or more RegistryError elements. At least one has error severity, others may have warning severity.	Metadata and documents not stored

Table 4.1-13 – Register Document Set Responses

RegistryResponse status	RegistryErrorList element	Result
Success	May be present. If present will contain one or	All metadata was successfully registered

	more RegistryError elements with warning severity, none with error severity	
Failure	Present, contains one or more RegistryError elements. At least one has error severity, others may have warning severity.	Metadata not stored

8475

Table 4.1-14 – Query Registry Responses

AdhocQueryResponse status	RegistryErrorList element	Result
Success	May be present. If present will contain one or more RegistryError elements with warning severity, none with error severity	Results returned
Failure	Present, contains one or more RegistryError elements. At least one has error severity, others may have warning severity.	Results not returned

Table 4.1-15 – Stored Query Responses

AdhocQueryResponse status	RegistryErrorList element	Result
Success	May be present. If present will contain one or more RegistryError elements with warning severity, none with error severity	Results shall be returned. Results may contain zero or more entries.
PartialSuccess	Present, contains one or more RegistryError elements. At least one has error severity, others may have warning severity.	Results shall be returned. Results may contain zero or more entries.
Failure	Present, contains one or more RegistryError elements. At least one has error severity, others may have warning severity.	Results not returned

8480 **4.1.14 Extra Metadata Elements**

XDS transactions may contain metadata not defined in the XDS Profile. This extra metadata may be ignored by the recipient but its presence shall not cause an error.

The following conditions shall apply.

1. All extra metadata content shall be in the form of Slots.

8485 2. These Slots may be attached to XDSSubmissionSet, XDSDocumentEntry, XDSFolder, or Association objects.

3. If the Document Registry actor is not capable of storing extra metadata and extra metadata is provided in a Register Document Set transaction, it shall return a warning with an error code of XdsExtraMetadataNotSaved. The XDS defined metadata shall be saved.

8490 4. Document Consumer actors shall ignore extra metadata elements they do not understand.

5. If a Document Registry actor accepts extra metadata Slots (no warning on submission) then it shall return these Slots in query results.

6. The Name attribute of extra Slots shall conform to the following rules:

   a. Name shall be a valid URN.

8495
   b. Name shall begin with 'urn:' prefix (formatted as a valid URN)

   c. The prefix 'urn:ihe' shall not be used

7. Note that ebRIM requires that the name of a Slot be unique within the containing object (Document Entry, Submission Set, Folder, Association).

4.2 Character String Comparisons

8500 All character string comparisons shall be done in conformance with the rules of the Unicode standard (http://www.unicode.org/versions/latest/) using the normalized form C defined in Unicode Techical Report 15 (http://unicode.org/reports/tr15).

> Note: Latin alphabet case-insensitive NFC matching corresponds to byte string matching. The primary impact of this is for non-Latin alphabets. They need to be converted into normalized form before comparison. The TR 15 approach is consistent
> 8505 with the working documents of W3C, although W3C has not yet issued a balloted recommendation that Unicode normalized form C be used. See http://www.w3.org/TR/WD-charreq, http://www.w3.org/International/charlint/, and the current W3C draft (http://www.w3.org/TR/charmod-norm).

See the following references for more details:

8510 Unicode Technical Report #15,   Unicode Consortium UAX #15: Unicode Normalization Forms (http://www.unicode.org/reports/tr15/)

Unicode Standard   Unicode Consortium. The Unicode Standard, (http://www.unicode.org/versions/latest/)

4.3 XDS Metadata Vocabulary

4.3.1 Metadata UUIDs

8515 The UUIDs in the following sections shall be used in constructing and interpreting XDS metadata. The assigning authority "IHE XDS Metadata" shall be used for these codes.

4.3.1.1 Submission Set Object

UUID	Use/meaning
urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd	ClassificationNode
urn:uuid:a7058bb9-b4e4-4307-ba5b-e3f0ab85e12d	author External Classification Scheme
urn:uuid:aa543740-bdda-424e-8c96-df4873be8500	contentTypeCode External Classification Scheme

urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446	patientId External Identifier
urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832	sourceId External Identifer
urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8	uniqueId External Identifer

4.3.1.2 Document Entry Object

UUID	Use/meaning
urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1	XDSDocumentEntry ClassificationNode
urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d	author External Classification Scheme
urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a	classCode External Classification Scheme
urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f	confidentialityCode External Classification Scheme
urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4	eventCodeList External Classification Scheme
urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d	formatCode External Classification Scheme
urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1	healthCareFacilityTypeCode External Classification Scheme
urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427	patientId ExternalIdentifier
urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead	practiceSettingCode External Classification Scheme
urn:uuid:f0306f51-975f-434e-a61c-c59651d33983	typeCode External Classification Scheme
urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab	uniqueId ExternalIdentifier

8520

4.3.1.3 Folder Object

UUID	Use/meaning
urn:uuid:d9d542f3-6cc4-48b6-8870-ea235fbc94c2	XDSFolder ClassificationNode
urn:uuid:1ba97051-7806-41a8-a48b-8fce7af683c5	codeList External Classification Scheme
urn:uuid:f64ffdf0-4b97-4e06-b79f-a52b38ec2f8a	patientId External Identifier
urn:uuid:75df8f67-9973-4fbe-a900-df66cefecc5a	uniqueId External Identifier

5   IHE Content Specifications

This section follows the documentation pattern found in the IHE PCC Technical Framework. The reader should be familiar with the IHE PCC Technical Framework.

8525

5.1   Basic Patient Privacy Consents Module

This section describes the encoding requirements for the Basic Patient Privacy Consents Document Content.

The BPPC document has two possible document templates, one without a scanned document part, and one with. Section 5.1.2 defines the requirements of the BPPC document without a scanned document part, Section 5.1.3 explains with a scanned document part.

8530

5.1.1 References

> o   [HL7 CDA Release 2.0](#) (denoted HL7 CDA R2, or just CDA, in subsequent text)

5.1.2 Patient Privacy Consent Acknowledgment Document Specification 1.3.6.1.4.1.19376.1.5.3.1.1.7 – With no Scanned Document Part

8535

A patient acknowledgement of a Patient Privacy Consent Policy is a document that contains machine readable indication. This specification describes the BPPC document without a scanned part. When the Patient Privacy Consent Acknowledgment Document contains a Scanned Document (XDS-SD), it will conform to IHE ITI TF-2:5.1.3.

8540   **5.1.2.1 XDS Metadata**

5.1.2.1.1 XDS DocumentEntry Metadata

BPPC leverages the XDS DocumentEntry Metadata requirements in the IHE PCC TF-2:5.1.1.1.1 unless otherwise specified below.

5.1.2.1.1.1 XDSDocumentEntry.classCode

8545
- classCode -- This attributes shall be set to the value "Consent".
- classCodeDisplayName -- This attributes shall be set to the value "Consent".

5.1.2.1.1.2 XDSDocumentEntry.eventCodeList

- eventCodeList -- the eventCodeList shall be populated using the Patient Privacy Consent Policy Identifiers that have been acknowledged to within the document.

8550
  - o   /ClinicalDocument/documentationOf/serviceEvent[templateId/@root='1.3.6.1.4.1.19376. 1.5.3.1.2.6']/code/@code
- eventCodeDisplayNameList -- The eventCodeDisplayNameList shall be populated using the display names for those policies.

o /ClinicalDocument/documentationOf/serviceEvent[templateId/@root='1.3.6.1.4.1.19376.
8555   1.5.3.1.2.6']/code/@displayName

5.1.2.1.1.3 XDSDocumentEntry.formatCode

The XDSDocumentEntry format code for this content shall be **urn:ihe:iti:bppc:2007.** The formatCode codeSystem shall be 1.3.6.1.4.1.19376.1.2.3.

5.1.2.1.1.4 XDSDocumentEntry.uniqueId

8560   This value shall be the `ClinicalDocument/id` in the HL7 CDA R2 header. The root attribute is required, and the extension attribute is optional. In accordance with the XDS.a profile, total length is limited to 128 characters; for XDS.b the limit is 256 characters. Additionally see IHE PCC TF-2:5.1.1.1.1, for further content specification.

5.1.2.1.2 XDS SubmissionSet Metadata

8565   No additional constraints. For more information, see IHE PCC TF-2:5.1.1.1.2

5.1.2.1.3 XDS Folder Metadata

No additional requirements. For more information, see IHE PCC TF-2:5.1.1.1.3

5.1.2.3 Specification

CDA Release 2.0 documents that conform to the requirements of this content module shall indicate their
8570   conformance by the inclusion of the appropriate <templateId> elements in the header of the document. This is shown in the sample document below. A CDA Document may conform to more than one template. This content module inherits from the Medical Document content module, and so must conform to the requirements of that template as well, thus all <templateId> elements shown in the example below shall be included.

8575
```
<ClinicalDocument xmlns='urn:hl7-org:v3'>
  <typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>
  <templateId root='1.3.6.1.4.1.19376.1.5.3.1.1.1'/>
  <templateId root='1.3.6.1.4.1.19376.1.5.3.1.1.7'/>
  <id root=' ' extension=' '/>
  <code code=' ' displayName=' '
    codeSystem='2.16.840.1.113883.6.1' codeSystemName='LOINC'/>
  <title>Consent to Share Information</title>
  <effectiveTime value='20070619012005'/>
  <confidentialityCode code='N' displayName='Normal'
    codeSystem='2.16.840.1.113883.5.25' codeSystemName='Confidentiality' />
  <languageCode code='en-US'/>
     :
  <component><structuredBody>

  </strucuredBody></component>
</ClinicalDocument>
```
8580

8585

8590

Figure 5.1.2.3-1 Sample Consent to Share Information Document

A Patient Privacy Consent Acknowledgement Document shall contain a text description of what the patient consented to, a list of codes indicating the policy(s) agreed to, and a time range indicating the
8595   effective time of the consent. It may be attested to using an electronic digital signature, conforming to the ITI Digital Signature Profile.

A consent shall have one or more <serviceEvent> elements in the header identifying the policies authorized by the document (see Section 4.2.3.4 of CDA R2). Each <serviceEvent> element indicates informed consent to one and only one XDS Affinity Domain policy. More than one policy may be agreed to within a given consent document.

8600

Data Element Name	Opt	Template ID
Consent Service Event At least one, and possibly more than one consent can be provided within the document.	R	1.3.6.1.4.1.19376.1.5.3.1.2.6
Authorization Consents may also be protected under a sharing publicity.	O	1.3.6.1.4.1.19376.1.5.3.1.2.5

5.1.2.3.1 Consent Service Events 1.3.6.1.4.1.19376.1.5.3.1.2.6

Within a Patient Privacy Consent Document, there shall be a Consent Service Event with the effective time of the consent shall be specified within the documentationOf/serviceEvent element.

8605

```
<documentationOf typeCode='DOC'>
  <serviceEvent classCode='ACT' moodCode='EVN'>
    <templateId root='1.3.6.1.4.1.19376.1.5.3.1.2.6'/>
    <id root=''/>
    <code code='' displayName='' codeSystem='' codeSystemName=''/>
    <effectiveTime>
      <low value=''/>
      <high value=''/>
    </effectiveTime>
  </serviceEvent>
</documentationOf>
```

8610

8615

Figure 5.1.2.3-2 Consent Service Events Example

5.1.2.3.2 <documentationOf typeCode='DOC'>

At least one <documentationOf> element shall exist within a consent to share information, describing the service event of provision of consent. This element shall have a typeCode attribute with the value DOC.

8620

5.1.2.3.3 <serviceEvent classCode='ACT' moodCode='EVN'>

One <serviceEvent> shall exist for each consent to share information given, describing the duration of the provision of consent. This element shall have a classCode attribute set to ACT, and a moodCode attribute of EVN.

8625

5.1.2.3.4 <templateId root='1.3.6.1.4.1.19376.1.5.3.1.2.6'/>

The <templateId> element shall be recorded exactly as shown above, and identifies this <serviceEvent> as recording consent to share information.

5.1.2.3.5 <id root=' ' />

8630 The service event shall have one <id> element, providing an identifier for the service event. The root attribute of this element shall be present, and shall be a GUID or OID. The extension attribute shall not be present.

5.1.2.3.6 <code code=' ' displayName=' ' codeSystem=' ' codeSystemName=' '/>

The <code> element shall be present, and shall indicate the consent given. The code attribute indicates the consent given, and the codeSystem attribute indicates the code system from which this consent is given. The displayName attribute may be present, and describes the consent given. The codeSystemName attribute may be present, and describes the code system.

5.1.2.3.7 <effectiveTime><low value=' '/><high value=' '/></effectiveTime>

The <effectiveTime> element shall be present, and shall indicate the effective time range over which consent is given. The low value must be provided . The high value may be present. If present, is shall indicate the maximum effective time of the consent.

5.1.3 Patient Privacy Consent Acknowledgment Document Specification 1.3.6.1.4.1.19376.1.5.3.1.1.7.1 – With Scanned Document

A patient acknowledgement of a Patient Privacy Consent Policy is a document that contains machine readable indication. This section specifies the BPPC document with a scanned document part.

5.1.3.1 XDS Metadata

The BPPC document shall conform to the requirements in section 5.1.2.1 with the formatCode exception listed below

5.1.3.1.1 XDS DocumentEntry Metadata

The BPPC document shall conform to the XDS DocumentEntry Metadata requirements in the IHE PCC TF-2:5.1.1.1.1 unless otherwise specified below.

5.1.3.1.1.1 XDSDocumentEntry.formatCode

The XDSDocumentEntry format code for this content is **urn:ihe:iti:bppc-sd:2007.** The formatCode codeSystem shall be 1.3.6.1.4.1.19376.1.2.3.

5.1.3.1.2 XDS SubmissionSet Metadata

No additional constraints. For more information, see IHE PCC TF-2:5.1.1.1.2

5.1.3.1.3 XDS Folder Metadata

No additional requirements. For more information, see IHE PCC TF-2:5.1.1.1.3

5.1.3.3 Specification

This BPPC document shall conform to the XDS-SD (ITI TF-2 Section 5.2) specification and shall have the additional requirements stated in Section 5.1.2.3.

5.1.3.4 Conformance

See section 5.1.2.4

8665 5.2 Scanned Documents Content Module

This section outlines the content of the HL7 CDA R2 constraints for the document. We note here that requirements specified below are to ensure the presence of a minimum amount of wrapper data in order to enhance description and facilitate sharing of the document. Implementers of this profile can and should make use of additional annotation within the CDA header to provide richer context. The 8670 examples in the following sections contain the minimal amount of wrapper data, as specified, and in many cases do make use of additional CDA header elements for enriched context.

Assumptions and Definitions: We assume that the scanning facility and equipment within it are assigned an OID and that the scanning facility assembles the wrapped scanned content. More information regarding the construction of OIDS can be found in the ITI Technical Framework, Volume 8675 2, Appendix B. We define the following nomenclature for entity roles concerned in forming the wrapper content.

Original content – Legacy paper or electronic document intended for wrapping.

Scanned content – Scanned or appropriately converted/encoded electronic version of the original content.

8680 *Original author* – Author of the original content.

(Scanner) Operator – Person assembling the scanned content.

5.2.1 Referenced Standards

- PDF RFC 3778, The application/pdf Media Type (informative)
- PDF/A ISO 19005-1b. Document management - Electronic document file format for long-term
8685 preservation - Part 1: Use of PDF (PDF/A)
- HL7 CDA Release 2.0 (denoted HL7 CDA R2, or just CDA, in subsequent text)
- RFC 3066, Tags for the identification of languages

5.2.1.1 Discussion of Content Standards

PDF and plaintext documents intended for wrapping can consist of multiple pages. Encoding of multiple 8690 page PDF documents are subject to the PDF/A standard. This ISO standard, PDF/A, is a subset of Adobe PDF version 1.4 intended to be suitable for long-term preservation of page-oriented documents. PDF/A attempts to maximize:

- Device independence
- Self-containment
8695 - Self-documentation

The constraints imposed by PDF/A include:

- Audio and video content are forbidden
- JavaScript and executable file launches are prohibited
- All fonts must be embedded and also must be legally embeddable for unlimited, universal
8700 rendering
- Colorspaces specified in a device-independent manner

- Encryption is disallowed (although the enclosing document and transport may provide encryption external to the PDF content)
- Compression methods are restricted to a standard list

8705 The PDF/A approach has several advantages over TIFF or JPEG. First, there are more image compressions and format flexibility in PDF, so that the image files sizes can be kept smaller. There are many simple programs available for converting TIFF and JPEG into PDF with various other features for improving compression or adding other information. The PDF/A enables devices that produce vectorized output. Unlike TIFF, JPEG, or BMP, a PDF/A image has the ability to provide several
8710 "layers" of information. This allows the creation of PDF searchable images.

A PDF searchable image is a PDF document with an exact bitmapped replica of the scanned paper pages and with text information stored behind the bitmap image of the page. This approach retains the look of the original pages while enabling text searchability and computer analysis. This approach is especially suitable for documents that have to be searchable while retaining the original scan details. The text layer
8715 is created by an Optical Character Recognition (OCR) application that scans the text on each page. It then creates a PDF file with the recognized text stored in a layer beneath the image of the text. Unrecognized graphics areas and annotations are preserved with full fidelity in the image. The text form may be incomplete or the OCR confused by some words, but the original image is preserved and available.

8720 Plaintext as well as PDF/A documents shall be base-64 encoded before wrapped in a HL7 CDA R2 header. The PDF/A docments shall conform to PDF/A-1b. Creators are encouraged to conform to PDF/A-1a to the maximum extent possible, but a simple document scanner may be unable to fully conform to PDF/A-1a. Other profiles may require PDF/A-1a conformance.

HL7 CDA R2 header schema is constrained so that pertinent metadata values and scanning facility,
8725 technology and operator information shall be present (see 5.2.3).

Medical imagery and photographs are outside the scope of this profile. Diagnostic or intervention medical imagery will be supported through DICOM (which includes the use of JPEG and MPEG). Additionally audio and video recorded content is not covered by this profile.

5.2.2 XDS Metadata

8730 XDS-SD is a CDA R2 document and thus conforms to the XDS Metadata requirements in the PCC TF-2:5 unless otherwise specified below.

5.2.2.1 XDS DocumentEntry Metadata

XDS-SD leverages the XDS DocumentEntry Metadata requirements in the PCC TF-2:5.1.1.1.1 unless otherwise specified below.

8735 #### 5.2.2.1.1 XDSDocumentEntry.formatCode

The XDSDocumentEntry.formatCode shall be **urn:ihe:iti:xds-sd:pdf:2008** when the document is scanned pdf and **urn:ihe:iti:xds-sd:text:2008** when the document is scanned text. The formatCode codeSystem shall be 1.3.6.1.4.1.19376.1.2.3.

5.2.2.1.2 XDSDocumentEntry.uniqueId

8740   This value shall be the `ClinicalDocument/id` in the HL7 CDA R2 header. The root attribute is required, and the extension attribute is optional. In accordance with the XDS.a profile, total length is limited to 128 characters; for XDS.b the limit is 256 characters. Additionally see PCC TF-2:5.1.1.1.1, for further content specification.

5.2.2.1.3 Relating instances of XDS-SD documents

8745   In general, most instances of XDS-SD will not have parent documents. It is possible, however, in some specific use cases that instances of XDS-SD documents are related. For example, for a particular document it may be the case that both the PDF scanned content and somewhat equivalent plaintext need to be wrapped and submitted. Each document would correspond to separate XDSDocumentEntries linked via an XFRM Association that indicates one document is a transform of the other. These can be
8750   submitted in a single submission set, or in separate ones. Other specific examples may exist and this profile does not preclude the notion of a parent document for these cases.

5.2.2.2 XDS SubmissionSet Metadata

No additional constraints. Particular to this profile, a legitimate use of submission sets would be to maintain a logical grouping of multiple XDS-SD documents. We encourage such usage. For more
8755   information, see PCC TF-2:5.1.1.1.2

5.2.2.3 XDS Folder Metadata

No additional requirements. For more information, see PCC TF-2:5.1.1.1.3

5.2.3 Specification

HL7 CDA R2 header element	CDA as constrained by XDS-SD	Section Number of Extended Discussion	Source Type	Source / Value
ClinicalDocument/typeId	R	5.2.3.1	FM	Fixed, per CDA R2 version in use.
ClinicalDocument/templateId	R	5.2.3.1	FM	Fixed, per this specification
ClinicalDocument/id	R	5.2.3.1	DS	Computable.
ClinicalDocument/code	R	5.2.3.1	O / FM	Entered by operator or appropriately fixed for scanned content
ClinicalDocument/title	R2	5.2.3.1	SA / O	Entered by operator, or possibly can be taken from the scanned content.
ClinicalDocument/confidentialityCode	R	5.2.3.1	O	Assigned by the operator
ClinicalDocument/effectiveTime	R	5.2.3.1	DS	Computed. This is the scan time.
ClinicalDocument/languageCode	R	5.2.3.1	O	Entered by operator
ClinicalDocument/recordTarget	R	5.2.3.2	SA / O	Taken from scanned content, supplemented by operator.
ClinicalDocument/author/assignedAuthor/assignedPerson	R2	5.2.3.3	SA / O	Taken from scanned content, supplemented by operator. This is the original author.
ClinicalDocument/author/assignedAuthor/authoringDevice	R	5.2.3.4	DS / FM / O	Can be computed or fixed based on the scanning device and software. This is the information about the scanning device.
ClinicalDocument/dataEnterer	R	5.2.3.5	DS / O	Can be computed by the scanner or supplemented by operator. This is the information about the scanner operator.
ClinicalDocument/custodian	R	5.2.3.6	DS / FM	Retains original HL7 CDA Context. To be computed or fixed appropriately to denote guardianship of the scanned and wrapped content.
ClinicalDocument/legalAuthenticator	O	5.2.3.7	O	Most likely supplemented by the operator, when applicable or mandated.
ClinicalDocument/documentationOf/serviceEvent/effectiveTime	R	5.2.3.8	SA / O	Denotes the time/date range of the original content.
ClinicalDocument/component/nonXMLBody	R	5.2.3.9	SA	The scanned/encoded content.

8760

5.2.3.1 ClinicalDocument child-less elements

In this section we further discuss `id`, `code`, `effectiveTime`, `confidentialityCode` and `languageCode` elements of the `ClinicalDocument`.

8765
- The ClinicalDocument/templateId element shall be present. The root attribute shall contain the oid, '1.3.6.1.4.1.19376.1.2.20', to indicate this document is an XDS-SD document.

- The ClinicalDocument/id element shall be present. The root attribute shall contain the oid for the document, in which case the extension attribute shall be empty, or an oid that scopes the set of possible unique values for the extension attribute, in which case the extension shall be populated with a globally unique identifier within the scope of the root oid.

8770
- The ClinicalDocument/code will in most cases be provided by the operator. Values for this code are dictated by the CDA R2 documentation, but are permissible to extend to fit the particular use case. Attributes code@code and code@codeSystem shall be present.

- The ClinicalDocument/title shall be present if known.

- The ClinicalDocument/effectiveTime shall denote the time at which the original content was
8775 scanned. At a minimum, the time shall be precise to the day and shall include the time zone offset from GMT.

- The ClinicalDocument/confidentialityCode shall be assigned by the operator in accordance with the scanning facility policy. The notion or level of confidentiality in the header may not be the same as that in the Affinity Domain, but in certain cases could be used to derive a confidentiality value
8780 among those specified by the Affinity Domain. Attributes confidentialityCode@code and confidentialityCode@codeSystem shall be present.

- The ClinicalDocument/languageCode, in accordance with the HL7 CDA R2 documentation, shall denote the language used in the character data of the wrapper CDA header. If the scanned content, when rendered, is in a language different than that of the header, the language context of the CDA
8785 will be overwritten at the body level (see 5.2.3.9 ClinicalDocument/component/nonXMLBody for an example). Attribute code@code shall be present. Attribute code@codeSystem shall be IETF (Internet Engineering Task Force) RFC 3066 in accordance with the HL7 CDA R2 documentation.

Example:

```
<ClinicalDocument xmlns="urn:hl7-org:v3">
  <typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>
  <templateId root="1.3.6.1.4.1.19376.1.2.20"/>
  <id root="1.3.6.4.1.4.1.2835.2.7777"/>
  <code code="34133-9"  codeSystem="2.16.840.1.113883.6.1"
      codeSystemName="LOINC" displayName="SUMMARIZATION OF EPISODE NOTE"/>
  <title>Good Health Clinic Care Record Summary</title>
  <effectiveTime value="20050329224411+0500"/>
  <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>
  <languageCode code="en-US"/>
```

8790

5.2.3.2 ClinicalDocument/recordTarget

The `ClinicalDocument/recordTarget` contains identifying information about the patient concerned in the original content. In many cases this will have to be supplied by the operator. All subelements retain their original definition as defined by the HL7 CDA R2 specification, unless noted below.

8795
- The ClinicalDocument/recordTarget/patientRole/id element shall include both the root and the extension attributes. Refer back to PCC TF-2:5.1.1.1.1 for more details.

- At least one ClinicalDocument/recordTarget/patientRole/addr element shall include at least the country subelement. The addr element has an unbounded upper limit on occurrences. It can, and should, be replicated to include additional addresses for a patient, each minimally specified by the
8800 country sub element.

- At least one ClinicalDocument/recordTarget/patientRole/ patient/name element shall be at least one given subelement and one family subelement.

- The ClinicalDocument/recordTarget/patientRole/patient/ administrativeGenderCode element shall be present.

8805
- The ClinicalDocument/recordTarget/patientRole/patient/ birthTime element shall be present with precision to the year.

Example:

```
<recordTarget>
  <patientRole>
    <id extension="12345" root="2.16.840.1.113883.3.933"/>
    <addr>
      <streetAddressLine>17 Daws Rd.</streetAddressLine>
      <city>Blue Bell</city>
      <state>MA</state>
      <postalCode>02368</postalCode>
      <country>USA</country>
    </addr>
    <patient>
      <name>
        <prefix>Mrs.</prefix>
        <given>Ellen</given>
        <family>Ross</family>
      </name>
      <administrativeGenderCode code="F"
          codeSystem="2.16.840.1.113883.5.1"/>
      <birthTime value="19600127"/>
    </patient>
  </patientRole>
</recordTarget>
```

5.2.3.3 ClinicalDocument/author (original)

8810 This ClinicalDocument/author element represents the author of the original content. It additionally can encode the original author's institution in the subelement representedOrganization. Information regarding the original author and his/her institution shall be included, if it is known. In many cases this

will have to be supplied by the operator. All subelements retain their original definition as defined by the HL7 CDA R2 specification, unless noted below.

8815 • The ClinicalDocument/author/templateId element shall be present. The root attribute shall contain the oid, '1.3.6.1.4.1.19376.1.2.20.1', to indicate this is the original author.

• The ClinicalDocument/author/time represents the day and time of the authoring of the original content. This value is not restricted beyond statements made in the HL7 CDA R2 documentation.

• The ClinicalDocument/author/assignedAuthor/id element if known shall include both the root and
8820 the extension attributes. Refer back to PCC TF-2:5.1.1.1.1 for more details.

• The ClinicalDocument/author/assignedAuthor/representedOrganization/id element if known shall include both the root and the extension attributes. Refer back to PCC TF-2:5.1.1.1.1for more details.

Example:

```
<author>
  <templateId root="1.3.6.1.4.1.19376.1.2.20.1"/>
  <time value="19990522"/>
  <assignedAuthor>
    <id extension="11111111" root="1.3.5.35.1.4436.7"/>
    <assignedPerson>
      <name>
        <prefix>Dr.</prefix>
        <given>Bernard</given>
        <family>Wiseman</family>
        <suffix>Sr.</suffix>
      </name>
    </assignedPerson>
    <representedOrganization>
      <id extension="aaaaabbbbb" root="1.3.5.35.1.4436.7"/>
      <name>Dr. Wiseman's Clinic</name>
    </representedOrganization>
  </assignedAuthor>
</author>
```

8825

5.2.3.4 ClinicalDocument/author (scanner)

This ClinicalDocument/author element shall be present and represent the scanning device and software used to produce the scanned content. All subelements retain their original definition as defined by the HL7 CDA R2 specification, unless noted below.

8830
- The ClinicalDocument/author/templateId element shall be present. The root attribute shall contain the oid, '1.3.6.1.4.1.19376.1.2.20.2', to indicate this author is the scanning device and software.

- The ClinicalDocument/author/time shall denote the time at which the original content was scanned. This value shall be equal to that of ClinicalDocument/effectiveTime. At a minimum, the time shall be precise to the day and shall include the time zone offset from GMT.

8835
- The ClinicalDocument/author/assignedAuthor/id element shall be at least the root oid of the scanning device.

- The ClinicalDocument/author/assignedAuthor/assignedAuthoringDevice/code element shall be present. The values set here are taken from appropriate DICOM vocabulary. The value of code@codeSystem shall be set to "1.2.840.10008.2.16.4". The value of code@code shall be set to
8840
"CAPTURE" for PDF scanned content and "WSD" for plaintext. The value of code@displayName shall be set to "Image Capture" for PDF scanned content and "Workstation" for plaintext.

- The ClinicalDocument/author/assignedAuthor/assignedAuthoringDevice/manufacturerModelName element shall be present. The mixed content shall contain string information that specifies the scanner product name and model number. From this information, features like bit depth and
8845
resolution can be inferred. In the case of virtually scanned documents (for example, print to PDF), the manufactureModelName referenced here refers to the makers of the technology that was used to produce the embedded content.

- The ClinicalDocument/author/assignedAuthor/assignedAuthoringDevice/softwareName element shall be present. The mixed content shall contain string information that specifies the scanning
8850 software name and version. In the case of virtually scanned documents, the softwareName referenced here refers to the technology that was used to produce the embedded content.

- The ClinicalDocument/author/assignedAuthor/representedOrganization/id element shall be present. The root attribute shall be set to the oid of the scanning facility.

Example:

```
 <author>
   <templateId root="1.3.6.1.4.1.19376.1.2.20.2"/>
   <time value="20050329224411+0500"/>
   <assignedAuthor>
     <id root="1.3.6.4.1.4.1.2835.2.1234"/>
     <assignedAuthoringDevice>
     <code code="CAPTURE" displayName="Image Capture" codeSystem="
     1.2.840.10008.2.16.4" />
        <manufacturerModelName>SOME SCANNER NAME AND MODEL
        </manufacturerModelName>
        <softwareName>SCAN SOFTWARE NAME v0.0</softwareName>
     </assignedAuthoringDevice>
     <representedOrganization>
        <id root="1.3.6.4.1.4.1.2835.2"/>
        <name>SOME Scanning Facility</name>
        <addr>
          <streetAddressLine>21 North Ave</streetAddressLine>
          <city>Burlington</city>
          <state>MA</state>
          <postalCode>01803</postalCode>
          <country>USA</country>
        </addr>
     </representedOrganization>
   </assignedAuthor>
 </author>
```

8855

5.2.3.5 ClinicalDocument/dataEnterer

This ClinicalDocument/dataEnterer element shall represent the scanner operator who produced the scanned content. All subelements retain their original definition as defined by the HL7 CDA R2 specification, unless noted below.

8860 • The ClinicalDocument/dataEnterer/templateId element shall be present. The root attribute shall contain the oid, '1.3.6.1.4.1.19376.1.2.20.3', to indicate this is the scanner operator.

- The ClinicalDocument/dataEnterer/time shall denote the time at which the original content was scanned. This value shall be equal to that of ClinicalDocument/effectiveTime. At a minimum, the time shall be precise to the day and shall include the time zone offset from GMT.

8865 • The ClinicalDocument/dataEnterer/assignedEntity/id element shall be both the root and the extension attributes the root shall be the oid of the scanning facility and the extension shall be an appropriately assigned, facility unique id of the operator.

Example:

```
   <dataEnterer>
     <templateId root="1.3.6.1.4.1.19376.1.2.20.3"/>
     <time value="20050329224411+0500"/>
     <assignedEntity>
       <id extension="22222222" root="1.3.6.4.1.4.1.2835.2"/>
       <assignedPerson>
         <name>
           <prefix>Mrs.</prefix>
           <given>Bernice</given>
           <family>Smith</family>
         </name>
       </assignedPerson>
     </assignedEntity>
   </dataEnterer>
```

8870   **5.2.3.6 ClinicalDocument/custodian**

The ClinicalDocument/custodian shall be present. Its context is left up to the scanning facility to refine in accordance with local policies and to reflect the entity responsible for the scanned content. In most cases this will be the scanning facility. All subelements retain their original definition as defined by the HL7 CDA R2 specification, unless noted below.

8875   • The ClinicalDocument/assignedCustodian/representedOrganization/name shall be present.

   • At least one ClinicalDocument/assignedCustodian/representedOrganization/addr element shall include at least the country sub element.

Example:

```
   <custodian>
     <assignedCustodian>
       <representedCustodianOrganization>
          <id root="1.3.6.4.1.4.1.2835.2"/>
          <name>SOME Scanning Facility</name>
          <addr>
            <streetAddressLine>21 North Ave</streetAddressLine>
            <city>Burlington</city>
            <state>MA</state>
            <postalCode>01803</postalCode>
            <country>USA</country>
          </addr>
       </representedCustodianOrganization>
     </assignedCustodian>
   </custodian>
```

8880 5.2.3.7 ClinicalDocument/legalAuthenticator

The `ClinicalDocument/legalAuthenticator` may be present and its context is left up to the scanning facility to refine in accordance with local policies. All subelements retain their original definition as defined by the HL7 CDA R2 specification, unless noted below.

- The ClinicalDocument/legalAuthenticator/assignedEntity/id element if known shall include both the

8885 root and the extension attributes. Refer back to PCC TF-2:5.1.1.1.1 for more details.

Example:

```
   <legalAuthenticator>
     <time value="19990522"/>
     <signatureCode code="S"/>
     <assignedEntity>
       <id extension="11111111" root="1.3.5.35.1.4436.7"/>
       <assignedPerson>
         <name>
           <prefix>Dr.</prefix>
           <given>Bernard</given>
           <family>Wiseman</family>
           <suffix>Sr.</suffix>
         </name>
       </assignedPerson>
     </assignedEntity>
   </legalAuthenticator>
```

5.2.3.8 ClinicalDocument/documentationOf

This `ClinicalDocument/documentationOf` element is used to encode the date/time range of the
8890 original content. If the original content is representative of a single point in time then the endpoints of the date/time range shall be the same. Information regarding this date/time range shall be included, if it

is known. In many cases this will have to be supplied by the operator. This profile does not restrict the `documentationOf` element beyond statements made in the HL7 CDA R2 documentation.

Example:

```
<documentationOf>
  <serviceEvent >
    <effectiveTime>
      <low value="19800127"/>
      <high value="19990522"/>
    </effectiveTime>
  </serviceEvent>
</documentationOf>
```

8895

5.2.3.9 ClinicalDocument/component/nonXMLBody

This ClinicalDocument/component/nonXMLBody element shall be present and used to wrap the scanned content. The nonXMLBody element is guaranteed to be unique; thus the x-path to recover the scanned content is essentially fixed. All subelements of the nonXMLBody retain their original definition

8900 as defined by the HL7 CDA R2 specification, unless noted below.

- If the human-readable language of the scanned content is different than that of the wrapper (specified in ClinicalDocument/languageCode), then ClinicalDocument/component/nonXMLBody/languageCode shall be present. Attribute code@code shall be present. Attribute code@codeSystem shall be IETF (Internet Engineering Task Force) RFC

8905 3066 in accordance with the HL7 CDA R2 documentation.

- The ClinicalDocument/component/nonXMLBody/text element shall be present and encoded using xs:base64Binary encoding. Its #CDATA will contain the scanned content.

    - ClinicalDocument/component/nonXMLBody/text@mediaType shall be "application/pdf" for PDF, or "text/plain" for plaintext.

8910

    - ClinicalDocument/component/nonXMLBody/text@representation shall be present. The @representation for both PDF and plaintext scanned content will be "B64", because this profile requires the base-64 encoding of both formats.

Example (PDF scanned content is in the *same* language as the wrapper):

```
   <component>
     <nonXMLBody>
       <text mediaType="application/pdf" representation="B64">
       JVBERi0xLjMKJcfsj6IKNSAwIG9iago8PC9MZW5ndGggNiAwIFIvRmlsdGVyIC9GbGF0
       ZURlY29kZT4+CnN0cmVhbQp4nGWPMWsDMQyFd/8KjfJwqmVbkr0GQqFbg7fQoSRNWuhB
       Q/4/1L67TEEYme+9J1s3CMQQRm39NLuXg8H17gK89nN1N8eLAbZ2mmHXuql2QDVUhnZx
       a5iBcyQtoMIUM7TZHbH5KZEVDgm//SSUswbFHx/JzBLeu5yYxOIzE8bPcRWqdaGDmcZO
       BWc/9bfUNOPfOte44O9jxtcIKskqp0JZouJ5deYqeBn58ZmKtIU+2ptjqWQRJpGyrHDu
       K7CXIe2be+/1DzXQP+RlbmRzdHJlYW0KZW5kb2JqCjYgMCBvYmoKMjAxCmVuZG9iago0
       ...
       SW5mbyAyIDAgUgovSUQggWzxGNENDN0FFQjU0QjM2RkIyODNNDNUMzMjQ3OUFFMjgzRj48
       RjRDQzdBRUI1NEIzNkZCMjgzQzVDMzI0NzlBRDI4M0Y+XQo+PgpzdGFydHhyZWYKMzAx
       MgolJUVPRgo=
       </text>
     </nonXMLBody>
   </component>
</ClinicalDocument>
```

8915

Example (PDF scanned content is in a *different* language than the wrapper):

```
   <component>
     <nonXMLBody>
       <languageCode code="zh-CN"/>
       <text mediaType="application/pdf" representation="B64">
       JVBERi0xLjMKJcfsj6IKNSAwIG9iago8PC9MZW5ndGggNiAwIFIvRmlsdGVyIC9GbGF0
       ZURlY29kZT4+CnN0cmVhbQp4nGWPMWsDMQyFd/8KjfJwqmVbkr0GQqFbg7fQoSRNWuhB
       Q/4/1L67TEEYme+9J1s3CMQQRm39NLuXg8H17gK89nN1N8eLAbZ2mmHXuql2QDVUhnZx
       a5iBcyQtoMIUM7TZHbH5KZEVDgm//SSUswbFHx/JzBLeu5yYxOIzE8bPcRWqdaGDmcZO
       BWc/9bfUNOPfOte44O9jxtcIKskqp0JZouJ5deYqeBn58ZmKtIU+2ptjqWQRJpGyrHDu
       K7CXIe2be+/1DzXQP+RlbmRzdHJlYW0KZW5kb2JqCjYgMCBvYmoKMjAxCmVuZG9iago0
       ...
       SW5mbyAyIDAgUgovSUQggWzxGNENDN0FFQjU0QjM2RkIyODNNDNUMzMjQ3OUFFMjgzRj48
       RjRDQzdBRUI1NEIzNkZCMjgzQzVDMzI0NzlBRDI4M0Y+XQo+PgpzdGFydHhyZWYKMzAx
       MgolJUVPRgo=
       </text>
     </nonXMLBody>
   </component>
</ClinicalDocument>
```

5.2.4 Complete Example (Wrapped PDF)

```
8920   <ClinicalDocument xmlns="urn:hl7-org:v3"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" classCode="DOCCLIN"
       moodCode="EVN" xsi:schemaLocation="urn:hl7-org:v3 CDA.xsd">
         <typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>
         <templateId root="1.3.6.1.4.1.19376.1.2.20"/>
8925     <id root="1.3.6.4.1.4.1.2835.2.7777"/>
         <code code="34133-9"  codeSystem="2.16.840.1.113883.6.1"
             codeSystemName="LOINC" displayName="SUMMARIZATION OF EPISODE NOTE"/>
         <title>Good Health Clinic Care Record Summary</title>
         <effectiveTime value="20050329224411+0500"/>
8930     <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>
         <languageCode code="en-US"/>
         <recordTarget>
           <patientRole>
             <id extension="12345" root="2.16.840.1.113883.3.933"/>
8935         <addr>
               <streetAddressLine>17 Daws Rd.</streetAddressLine>
               <city>Blue Bell</city>
               <state>MA</state>
               <postalCode>02368</postalCode>
8940           <country>USA</country>
             </addr>
             <patient>
               <name>
                 <prefix>Mrs.</prefix>
8945             <given>Ellen</given>
                 <family>Ross</family>
               </name>
               <administrativeGenderCode code="F"
                   codeSystem="2.16.840.1.113883.5.1"/>
8950           <birthTime value="19600127"/>
             </patient>
           </patientRole>
         </recordTarget>
         <author>
8955       <templateId root="1.3.6.1.4.1.19376.1.2.20.1"/>
           <time value="19990522"/>
           <assignedAuthor>
             <id extension="11111111" root="1.3.5.35.1.4436.7"/>
             <assignedPerson>
8960           <name>
                 <prefix>Dr.</prefix>
                 <given>Bernard</given>
                 <family>Wiseman</family>
                 <suffix>Sr.</suffix>
8965           </name>
             </assignedPerson>
             <representedOrganization>
               <id extension="aaaaabbbbb" root="1.3.5.35.1.4436.7"/>
               <name>Dr. Wiseman's Clinic</name>
8970         </representedOrganization>
           </assignedAuthor>
         </author>
         <author>
           <templateId root="1.3.6.1.4.1.19376.1.2.20.2"/>
8975       <time value="20050329224411+0500"/>
           <assignedAuthor>
             <id root="1.3.6.4.1.4.1.2835.2.1234"/>
```

```
                  <assignedAuthoringDevice>
                  <code code="CAPTURE" displayName="Image Capture" codeSystem="
8980              1.2.840.10008.2.16.4" />
                      <manufacturerModelName>SOME SCANNER NAME AND MODEL
                      </manufacturerModelName>
                      <softwareName>SCAN SOFTWARE NAME v0.0</softwareName>
                  </assignedAuthoringDevice>
8985              <representedOrganization>
                      <id root="1.3.6.4.1.4.1.2835.2"/>
                      <name>SOME Scanning Facility</name>
                      <addr>
                        <streetAddressLine>21 North Ave</streetAddressLine>
8990                  <city>Burlington</city>
                        <state>MA</state>
                        <postalCode>01803</postalCode>
                        <country>USA</country>
                      </addr>
8995              </representedOrganization>
            </assignedAuthor>
          </author>
          <dataEnterer>
            <templateId root="1.3.6.1.4.1.19376.1.2.20.3"/>
9000        <time value="20050329224411+0500"/>
            <assignedEntity>
              <id extension="22222222" root="1.3.6.4.1.4.1.2835.2"/>
              <assignedPerson>
                <name>
9005              <prefix>Mrs.</prefix>
                  <given>Bernice</given>
                  <family>Smith</family>
                </name>
              </assignedPerson>
9010        </assignedEntity>
          </dataEnterer>
          <custodian>
            <assignedCustodian>
              <representedCustodianOrganization>
9015            <id root="1.3.6.4.1.4.1.2835.2"/>
                <name>SOME Scanning Facility</name>
                <addr>
                  <streetAddressLine>21 North Ave</streetAddressLine>
                  <city>Burlington</city>
9020              <state>MA</state>
                  <postalCode>01803</postalCode>
                  <country>USA</country>
                </addr>
              </representedCustodianOrganization>
9025        </assignedCustodian>
          </custodian>
          <legalAuthenticator>
            <time value="19990522"/>
            <signatureCode code="S"/>
9030        <assignedEntity>
              <id extension="11111111" root="1.3.5.35.1.4436.7"/>
              <assignedPerson>
                <name>
                  <prefix>Dr.</prefix>
9035              <given>Bernard</given>
                  <family>Wiseman</family>
                  <suffix>Sr.</suffix>
                </name>
              </assignedPerson>
9040        </assignedEntity>
          </legalAuthenticator>
```

```
        <documentationOf>
          <serviceEvent >
            <effectiveTime>
9045          <low value="19800127"/>
              <high value="19990522"/>
            </effectiveTime>
          </serviceEvent>
        </documentationOf>
9050    <component>
          <nonXMLBody>
            <text mediaType="application/pdf" representation="B64">
            JVBERi0xLjMKJcfsj6IKNSAwIG9iago8PC9MZW5ndGggNiAwIFIvRmlsdGVyIC9GbGF0
            ZURlY29kZT4+CnN0cmVhbQp4nGWPMWsDMQyFd/8KjfJwqmVbkr0GQqFbg7fQoSRNWuhB
9055        Q/4/1L67TEEYme+9J1s3CMQQRm39NLuXg8H17gK89nN1N8eLAbZ2mmHXuql2QDVUhnZx
            a5iBcyQtoMIUM7TZHbH5KZEVDgm//SSUswbFHx/JzBLeu5yYxOIzE8bPcRWqdaGDmcZO
            BWc/9bfUNOPfOte44O9jxtcIKskqp0JZouJ5deYqeBn58ZmKtIU+2ptjqWQRJpGyrHDu
            K7CXIe2be+/1DzXQP+RlbmRzdHJlYW0KZW5kb2JqCjYgMCBvYmoKMjAxCmVuZG9iago0
            ...
9060        SW5mbyAyIDAgUgovSUQgWzxGNENDDN0FFQjU0QjM2RkIyODNDDNUMzMjQ3OUFFMjgzRj48
            RjRDDQzdBRUI1NEIzNkZCMjgzQzVDDMzI0NzlBRDI4M0Y+XQo+PgpzdGFydHhyZWYKMzAx
            MgolJUVPRgo=
            </text>
          </nonXMLBody>
9065    </component>
</ClinicalDocument>
```

Appendix A: Web Service Definition for Retrieve Specific Information for Display and Retrieve Document for Display Transaction

The following is an example WSDL definition of web services used in Transactions ITI-11 and ITI-12.
9070 This code is provided as an example and is not intended to replace the formal specification of
Transactions ITI-11 and ITI-12 in Volume 2. Also, the definitions of summaryRequestType,
listRequestType and contentType shall correspond to the capabilities of the Information Source Actor.

```xml
9075  <?xml version="1.0" encoding="utf8"?>

      <definitions xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
          xmlns:s="http://www.w3.org/2001/XMLSchema"
          xmlns:s0="http://rsna.org/ihe/IHERetrieveForDisplay"
          xmlns:tm="http://microsoft.com/wsdl/mime/textMatching/"
9080      xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
          targetNamespace="http://rsna.org/ihe/IHERetrieveForDisplay"
          xmlns="http://schemas.xmlsoap.org/wsdl/">

        <!-- Defines the types available for the parameters -->
9085    <!-- May also include the return type definitiions -->
        <types>
          <s:schema elementFormDefault="qualified"
      targetNamespace="http://rsna.org/ihe/IHERetrieveForDisplay">
            <!-- Add any items that control the returned values list or type here -->
9090        <!-- Add or remove items in the actual supplied WSDL to show the available types. -->
            <s:simpleType name="summaryRequestType">
              <s:restriction base="s:string">
                <s:enumeration value="SUMMARY" />
                <s:enumeration value="SUMMARY-RADIOLOGY" />
9095            <s:enumeration value="SUMMARY-CARDIOLOGY" />
                <s:enumeration value="SUMMARY-LABORATORY" />
                <s:enumeration value="SUMMARY-SURGERY" />
                <s:enumeration value="SUMMARY-EMERGENCY" />
                <s:enumeration value="SUMMARY-DISCHARGE" />
9100            <s:enumeration value="SUMMARY-ICU" />
              </s:restriction>
            </s:simpleType>

            <s:simpleType name="listRequestType">
9105          <s:restriction base="s:string">
                <s:enumeration value="LIST-ALLERGIES" />
                <s:enumeration value="LIST-MEDS" />
              </s:restriction>
            </s:simpleType>
9110
            <!-- Please list all content types available, and remove those not available. -->
            <s:simpleType name="contentType">
              <s:restriction base="s:string">
                <s:enumeration value="text/html" />
9115          </s:restriction>
            </s:simpleType>

            <!-- Indicates that this item is a returned rows restriction -->
            <s:simpleType name="ReturnedResultCount" type="s:positiveInteger" />
9120
            <!-- Please use the string "Search" as a prefix for all search criteria, and list below -->
            <!-- Indicates that this item is a search string -->
            <s:simpleType name="SearchString" type="s:string" />

9125

          </s:schema>
        </types>

9130  <message name="RetrieveSummaryInfoHttpGetIn">
        <!-- Add other parameters here if they are available, using types defined above. -->
        <part name="requestType" type="summaryRequestType" />
```

```
        <part name="patientID" type="SearchString" />
        <part name="lowerDateTime" type="s:dateTime" />
9135    <part name="upperDateTime" type="s:dateTime" />
        <part name="mostRecentResults" type="ReturnedResultCount" />
      </message>

      <message name="RetrieveSummaryInfoHttpGetOut">
9140    <!-- If a complex type is defined for the return value, then it is suggested that -->
        <!-- it be used here instead of s0:string.  If a complex type is allowed as one -->
        <!-- of the options, but an arbitrarily formatted string is also allowed, then create -->
        <!-- a union type here that allows either option. -->
        <part name="Body" element="s0:string" />
9145  </message>

      <message name="RetrieveListInfoHttpGetIn">
        <!-- Add other parameters here if they are available, using types defined above. -->
        <part name="requestType" type="listRequestType" />
9150    <part name="patientID" type="SearchString" />
      </message>

      <message name="RetrieveListInfoHttpGetOut">
        <!-- If a complex type is defined for the return value, then it is suggested that -->
9155    <!-- it be used here instead of s0:string.  If a complex type is allowed as one -->
        <!-- of the options, but an arbitrarily formatted string is also allowed, then create -->
        <!-- a union type here that allows either option. -->
        <part name="Body" element="s0:string" />
      </message>
9160  <message name="RetrieveDocumentHttpGetIn">
        <!-- Add other parameters here if they are available, using types defined above. -->

        <!-- It is recommended that one of the sub-types of SearchUID is chosen here -->
        <!-- Especially if SearchStudyUID is allowed, then the display client can know that -->
9165    <!-- it is permissable to use a dicom uid here -->
        <part name="documentUID" type="SearchString" />
        <part name="contentType" type="contentType" />
      </message>

9170  <message name="RetrieveDocumentHttpGetOut">
        <!-- If a complex type is defined for the return value, then it is suggested that -->
        <!-- it be used here instead of s:string.  If a complex type is allowed as one -->
        <!-- of the options, but an arbitrarily formatted string is also allowed, then create -->
        <!-- a union type here that allows either option. -->
9175    <part name="Body" element="s:string" />
      </message>

      <portType name="IHERetrieveForDisplayHttpGet">
        <operation name="RetrieveSummaryInfo">
9180      <input message="s0:RetrieveSummaryInfoHttpGetIn" />
          <output message="s0:RetrieveSummaryInfoHttpGetOut" />
        </operation>
          <operation name="RetrieveListInfo">
          <input message="s0:RetrieveListInfoHttpGetIn" />
9185      <output message="s0:RetrieveListInfoHttpGetOut" />
        </operation>
        <operation name="RetrieveDocument">
          <input message="s0:RetrieveDocumentHttpGetIn" />
          <output message="s0:RetrieveDocumentHttpGetOut" />
9190    </operation>
      </portType>

      <binding name="IHERetrieveForDisplayHttpGet" type="s0:IHERetrieveForDisplayHttpGet">
        <http:binding verb="GET" />
9195    <operation name="RetrieveSummaryInfo">
          <http:operation location="/IHERetrieveSummaryInfo" />
          <input>
            <http:urlEncoded />
          </input>
9200
          <output>
            <mime:content type="text/html" />
          </output>
```

```
9205          </operation>

          <operation name="RetrieveListInfo">
            <http:operation location="/IHERetrieveListInfo" />
            <input>
              <http:urlEncoded />
9210          </input>

            <output>
              <mime:content type="text/html" />
            </output>
9215        </operation>

          <operation name="RetrieveDocument">
            <http:operation location="/IHERetrieveDocument" />
            <input>
9220          <http:urlEncoded />
            </input>

            <!-- The type of the output should be restricted on a per-server basis to the types -->
            <!-- actually provided. -->
9225        <output>
              <mime:content type="text/html" />
              <mime:content type="application/x-hl7-cda-level-one+xml" />
              <mime:content type="application/pdf" />
              <mime:content type="image/jpeg" />
9230        </output>
          </operation>
        </binding>

        <!-- Bind the actual service here -->
9235    <service name="IHERetrieveForDisplay">
          <port name="IHERetrieveForDisplayHttpGet" binding="s0:IHERetrieveForDisplayHttpGet">
            <http:address location="http://localhost/" />
          </port>
        </service>
9240    <?xml version="1.0" encoding="utf8"?>

        <definitions xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
            xmlns:s="http://www.w3.org/2001/XMLSchema"
            xmlns:s0="http://rsna.org/ihe/IHERetrieveForDisplay"
9245        xmlns:tm="http://microsoft.com/wsdl/mime/textMatching/"
            xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
            targetNamespace="http://rsna.org/ihe/IHERetrieveForDisplay"
            xmlns="http://schemas.xmlsoap.org/wsdl/">

9250      <!-- Defines the types available for the parameters -->
          <!-- May also include the return type defintiions -->
          <types>
            <s:schema elementFormDefault="qualified"
        targetNamespace="http://rsna.org/ihe/IHERetrieveForDisplay">
9255          <!-- Add any items that control the returned values list or type here -->
              <!-- Add or remove items in the actual supplied WSDL to show the available types. -->
              <s:simpleType name="summaryRequestType">
                <s:restriction base="s:string">
                  <s:enumeration value="SUMMARY" />
9260              <s:enumeration value="SUMMARY-RADIOLOGY" />
                  <s:enumeration value="SUMMARY-CARDIOLOGY" />
                  <s:enumeration value="SUMMARY-LABORATORY" />
                  <s:enumeration value="SUMMARY-SURGERY" />
                  <s:enumeration value="SUMMARY-EMERGENCY" />
9265              <s:enumeration value="SUMMARY-DISCHARGE" />
                  <s:enumeration value="SUMMARY-ICU" />
                  <s:enumeration value="SUMMARY-RX" />
                </s:restriction>
              </s:simpleType>
9270
              <s:simpleType name="listRequestType">
                <s:restriction base="s:string">
                  <s:enumeration value="LIST-ALLERGIES" />
                  <s:enumeration value="LIST-MEDS" />
```

```
9275          </s:restriction>
            </s:simpleType>

            <!-- Please list all content types available, and remove those not available. -->
            <s:simpleType name="contentType">
9280          <s:restriction base="s:string">
                <s:enumeration value="text/html" />
              </s:restriction>
            </s:simpleType>

9285        <!-- Indicates that this item is a returned rows restriction -->
            <s:simpleType name="ReturnedResultCount" type="s:positiveInteger" />

            <!-- Please use the string "Search" as a prefix for all search criteria, and list below -->
            <!-- Indicates that this item is a search string -->
9290        <s:simpleType name="SearchString" type="s:string" />


          </s:schema>
9295    </types>

        <message name="RetrieveSummaryInfoHttpGetIn">
          <!-- Add other parameters here if they are available, using types defined above. -->
          <part name="requestType" type="summaryRequestType" />
9300      <part name="patientID" type="SearchString" />
          <part name="lowerDateTime" type="s:dateTime" />
          <part name="upperDateTime" type="s:dateTime" />
          <part name="mostRecentResults" type="ReturnedResultCount" />
        </message>
9305
        <message name="RetrieveSummaryInfoHttpGetOut">
          <!-- If a complex type is defined for the return value, then it is suggested that -->
          <!-- it be used here instead of s0:string. If a complex type is allowed as one -->
          <!-- of the options, but an arbitrarily formatted string is also allowed, then create -->
9310      <!-- a union type here that allows either option. -->
          <part name="Body" element="s0:string" />
        </message>

        <message name="RetrieveListInfoHttpGetIn">
9315      <!-- Add other parameters here if they are available, using types defined above. -->
          <part name="requestType" type="listRequestType" />
          <part name="patientID" type="SearchString" />
        </message>

9320    <message name="RetrieveListInfoHttpGetOut">
          <!-- If a complex type is defined for the return value, then it is suggested that -->
          <!-- it be used here instead of s0:string. If a complex type is allowed as one -->
          <!-- of the options, but an arbitrarily formatted string is also allowed, then create -->
          <!-- a union type here that allows either option. -->
9325      <part name="Body" element="s0:string" />
        </message>
        <message name="RetrieveDocumentHttpGetIn">
          <!-- Add other parameters here if they are available, using types defined above. -->

9330      <!-- It is recommended that one of the sub-types of SearchUID is chosen here -->
          <!-- Especially if SearchStudyUID is allowed, then the display client can know that -->
          <!-- it is permissable to use a dicom uid here -->
          <part name="documentUID" type="SearchString" />
          <part name="contentType" type="contentType" />
9335    </message>

        <message name="RetrieveDocumentHttpGetOut">
          <!-- If a complex type is defined for the return value, then it is suggested that -->
          <!-- it be used here instead of s:string. If a complex type is allowed as one -->
9340      <!-- of the options, but an arbitrarily formatted string is also allowed, then create -->
          <!-- a union type here that allows either option. -->
          <part name="Body" element="s:string" />
        </message>

9345    <portType name="IHERetrieveForDisplayHttpGet">
```

```
          <operation name="RetrieveSummaryInfo">
            <input message="s0:RetrieveSummaryInfoHttpGetIn" />
            <output message="s0:RetrieveSummaryInfoHttpGetOut" />
          </operation>
9350       <operation name="RetrieveListInfo">
            <input message="s0:RetrieveListInfoHttpGetIn" />
            <output message="s0:RetrieveListInfoHttpGetOut" />
          </operation>
          <operation name="RetrieveDocument">
9355        <input message="s0:RetrieveDocumentHttpGetIn" />
            <output message="s0:RetrieveDocumentHttpGetOut" />
          </operation>
        </portType>

9360    <binding name="IHERetrieveForDisplayHttpGet" type="s0:IHERetrieveForDisplayHttpGet">
          <http:binding verb="GET" />
          <operation name="RetrieveSummaryInfo">
            <http:operation location="/IHERetrieveSummaryInfo" />
            <input>
9365          <http:urlEncoded />
            </input>

            <output>
              <mime:content type="text/html" />
9370        </output>
          </operation>

          <operation name="RetrieveListInfo">
            <http:operation location="/IHERetrieveListInfo" />
9375        <input>
              <http:urlEncoded />
            </input>

            <output>
9380          <mime:content type="text/html" />
            </output>
          </operation>

          <operation name="RetrieveDocument">
9385        <http:operation location="/IHERetrieveDocument" />
            <input>
              <http:urlEncoded />
            </input>

9390        <!-- The type of the output should be restricted on a per-server basis to the types -->
            <!-- actually provided. -->
            <output>
              <mime:content type="text/html" />
              <mime:content type="application/x-hl7-cda-level-one+xml" />
9395          <mime:content type="application/pdf" />
              <mime:content type="image/jpeg" />
            </output>
          </operation>
        </binding>
9400
        <!-- Bind the actual service here -->
        <service name="IHERetrieveForDisplay">
          <port name="IHERetrieveForDisplayHttpGet" binding="s0:IHERetrieveForDisplayHttpGet">
            <http:address location="http://localhost/" />
9405      </port>
        </service>
```

Appendix B: Definition of Document Unique Ids

9410 The Retrieve Information for Display Integration Profile in its Retrieve Persistent Document transaction relies on a globally unique identification of persistent objects. It is the Information Source Actor's responsibility, when a specific document instance is available for retrieval, to assign to this document instance a globally unique identifier, thus allowing Display Actors to retrieve the same document instance at different points in time and to obtain the same semantics for its presented content.

9415 This appendix describes how unique identifiers for documents shall be created. A unique identifier may be created by the Information Source Actor or by any other system to which the information source is connected. The requirements specified in this appendix are derived from the common practices and definitions of OIDs in ISO 8824, HL7 V3 and CDA and UIDs in DICOM. They guarantee uniqueness across multiple countries, sites, vendors and equipment.

B.1:   Requirements for Document UIDs

9420 The UID identification scheme is based on the OSI Object Identification (numeric form) as defined by the ISO 8824 standard.

All Unique Identifiers, used within the context of this transaction shall be registered values as defined by ISO 9834-3 to ensure global uniqueness. These requirements result in the following structure for unique Ids.

9425 B.2:   Structure of a Document UID

Each Document UID is composed of two parts, an <org root> and a <suffix> separated by a "period". Therefore: UID = <org root>.<suffix>

The <org root> portion of the UID uniquely identifies an organization, (e.g., manufacturer, research organization, hospital, etc.), and is composed of a number of numeric components as defined by ISO 9430 8824. The <suffix> portion of the UID is also composed of a number of numeric components, and shall be unique within the scope of the <org root>. This implies that the organization identified in the <org root> is responsible for guaranteeing <suffix> uniqueness by providing registration policies. These policies shall guarantee <suffix> uniqueness for all UID's created by that organization. Unlike the <org root>, which may be common for UID's in an organization, the <suffix> shall take different unique 9435 values between different UID's that identify different objects. The <org root> is used only for uniqueness and not for any other purpose.

Although a specific implementation may choose some particular structure for its generated UIDs, it should never assume that a UID carries any semantics. A UID shall not be "parsed" to find a particular value or component. Component definition (for the suffix) is implementation-specific and may change 9440 as long as uniqueness is maintained. Parsing UID's (including extracting the root) may jeopardize the ability to inter-operate as implementations evolve.

B.3:   Document UID encoding rules

The UID encoding rules are defined as follows:

- Each component of a UID is a number and shall consist of one or more digits. The first digit of 9445 each component shall not be zero unless the component is a single digit.

> Note: Registration authorities may distribute components with non-significant leading zeroes. The leading zeroes should be ignored when being encoded (ie. "00029" would be encoded "29").

- Each component numeric value shall be encoded using the characters 0-9 of the Basic G0 Set of the International Reference Version of ISO 646:1990. This particular encoding is the same as the UTF-8 encoding for these characters in UNICODE.
- Components shall be separated by the character "." (2EH).
- UIDs shall not exceed 64 total characters, including the digits of each component, and separators between components.

B.4: How to obtain a UID registration root?

Organizations that define UIDs are responsible for properly registering their UIDs (at least obtain a registered <Org Root>) as defined for OSI Object Identifiers (ISO 9834-3). The organization defining the UID shall accept the responsibility of ensuring its uniqueness. IHE will not register UIDs or issue registered organization roots. There are a large number of means to obtain free or for a reasonable fee an organization root.

A useful resource that is often used by the DICOM community lists the many ways to obtain a registered UID Root for a small fee or even for free, anywhere in the world.

http://www.dclunie.com/medical-image-faq/html/part8.html#UIDRegistration

The manner in which the suffix of a Document UID is defined is not constrained by any IHE Integration Profile. Only the guarantee of its uniqueness by the defining organization is required by IHE.

B.5: Example of a Document UID

This example presents a particular choice made by a specific organization in defining its suffix to guarantee uniqueness. A variant is discussed.

"1.2.840.xxxxx.4076078054086.11059664469.235212"

(root)   (suffix)

In this example, the root is:

1	Identifies ISO
2	Identifies ANSI Member Body
840	Country code of a specific Member Body (U.S. for ANSI)
xxxxx	Identifies a specific Organization.(provided by ANSI)

In this example the remaining components of the suffix relate to the identification of a specific document instance:

4076078054086	802.3 MAC Address (004 076 078 054 086)
11059664469	Time system was booted (July 31, 2033 10:14:29)
235212	Monotonically increasing sequence number

In this example, the organization has chosen these components to guarantee uniqueness. Other organizations may choose an entirely different series of components to uniquely identify its documents.

Because of the flexibility allowed in creating Document UIDs, implementations should not depend on any assumed structure of UIDs and should not attempt to parse UIDs to extract the semantics of some of its components.

9485

B.6:   Representing UUIDs as OIDs

The standards ITU X.667 and ISO 9834-8 defined a particular OID root for the UUIDs, and define the translation between these two formats. The top node 2.25 is assigned for all UUIDs. This means that the UUID that can be written as urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6 (using hexadecimal

9490   notation) is also 2.25.329800735698586629295641978511506172918 (using dotted decimal notation). It can also be encoded using the ASN.1 rules in a binary form internally within X.509 Certificates and some LDAP messages. All of these are the same OID. The reverse is not true. Not all OIDs can be represented as UUIDs. UUIDs are a subset of the OIDs.

This relationship is one way to obtain OIDs in situations where an OID is needed. It is not necessary to

9495   use the 2.25 root. An OID assigning authority might take advantage of the UUID generation mechanisms to assign new OIDs within its own root domain. These OIDs would not be UUIDs, but they would be valid OIDs.

IHE_ITI_TF_5.0_Vol2_FT_2008-12-12.doc   407

Appendix C: HL7 Profiling Conventions

9500   The HL7 tables included in this document have been modified from the HL7 2.5 standard document. Such a modification is called a profile. Refer to the HL7 2.5 standard for the meanings of specific columns in the table.

The profiling tables in this document leverage the ongoing HL7 profile definition. To maintain this specification at a generic level, the following differences have been introduced:

9505   • Message specifications do not indicate the cardinality of segments within a message.

• For fields composed of multiple components, there is no indication of the size of each component.

• Where a table containing enumerated values is referenced from within a segment profile table, the enumerated values table is not always present.

9510   • The number of times a repeating field can repeat is not indicated.

• The conditions that would require inclusion of conditional fields are not defined when they depend on functional characteristics of the system implementing the transaction and they do not affect data consistency.

The following terms refer to the OPT column, which has been profiled:

9515   R   Required

R2   This is an IHE extension. If the sending application has data for the field, it is required to populate the field. If the value is not known, the field may not be sent.

R+   This is an IHE extension. This is a field that IHE requires that was listed as optional within the HL7 standard.

9520   **Table A-**   Optional

C   Conditional

IHE requires that Z-segments be present in HL7 transactions only when defined by the IHE IT Infrastructure Technical Framework. According to the HL7 standard, if the value of a field is not present, the receiver shall not change corresponding data in its database. However, if sender includes
9525   explicit NULL value (i.e., two double-quotes ""), it shall cause removal of any values for that field in the receiver's database.

Table C-1 provides a sample profile for an imaginary HL7 segment. Tables for real segments are copied from the HL7 2.5 standard with modifications made only to the OPT column.

9530   **Table C-1 Sample HL7 Profile**

SEQ	LEN	DT	OPT	TBL#	ITEM #	ELEMENT NAME
1	1	ST	R		xx001	Element 1
2	4	ST	O		xx002	Element 2
3	180	HD	R2		xx003	Element 3
4	180	HD	C		xx004	Element 4
5	180	HD	O		xx005	Element 5
6	180	HD	R+		xx006	Element 6

C.1: HL7 Message Profiling Convention

The messages used by each transaction are described in this document using static definitions as described for HL7 constrainable message profiles; refer to HL7 Version 2.5, Chapter 2, Section 2.12.6. The static definition of each message is represented within tables. The message level table represents the IHE-constrained message structure with its list of usable segments. The segment level table represents the IHE-constrained content of one segment with its usable fields.

C.1.1: Static definition - Message level

The message table representing the static definition contains 5 columns:

- Segment: gives the segment name, and places the segment within the hierarchy of the message structure designed by HL7, but hiding the traditional square brackets and braces that designate optionality and repeatability in HL7 standard message tables. The beginning and end lines of a segment group (see HL7 Version 2.5, Chapter 2, Section 2.5.2 for definition) are designated in this column by --- (3 dashes).

- Meaning: Meaning of the segment as defined by HL7. The beginning of a segment group is designated by one line in this column giving the segment group name in all caps, prefixed by --- (3 dashes), and followed by the keyword "begin". The end of a segment group is designated by one line in this column giving the segment group name in all caps, prefixed by --- (3 dashes), and followed by the keyword "end".

- Usage: Coded usage of the segment, in the context of this IHE Integration Profile. The coded values used in this column are:

  R: Required: A compliant sending application shall populate all "R" elements with a non-empty value. A compliant receiving application may ignore the information conveyed by required elements. A compliant receiving application shall not raise an error due to the presence of a required element, but may raise an error due to the absence of a required element.

  RE: Required but may be empty. The element may be missing from the message, but shall be sent by the sending application if there is relevant data. A conformant sending application shall be capable of providing all "RE" elements. If the conformant sending application knows a value for the element, then it shall send that value. If the conformant sending application does not know a value, then that element may be omitted. Receiving applications may ignore data contained in the element, but shall be able to successfully process the message if the element is omitted (no error message should be generated if the element is missing).

  O: Optional. The usage for this field within the message is not defined . The sending application may choose to populate the field; the receiving application may choose to ignore the field.

  C: Conditional. This usage has an associated condition predicate. (See HL7 Version 2.5, Chapter 2, Section 2.12.6.6, "Condition Predicate".)
  If the predicate is satisfied: A compliant sending application shall populate the element. A compliant receiving application may ignore data in the element. It may raise an error if the element is not present.
  If the predicate is NOT satisfied: A compliant sending application shall NOT populate the element. A compliant receiving application shall NOT raise an error if the condition

predicate is false and the element is not present, though it may raise an error if the element IS present.

CE: Conditional but may be empty. This usage has an associated condition predicate. (See HL7
9575 Version 2.5, Chapter 2, Section 2.12.6.6, "Condition Predicate".)
If the predicate is satisfied: If the conforming sending application knows the required values for the element, then the application must populate the element. If the conforming sending application does not know the values required for this element, then the element shall be omitted. The conforming sending application must be capable of populating the element
9580 (when the predicate is true) for all 'CE' elements. If the element is present, the conformant receiving application may ignore the values of that element. If the element is not present, the conformant receiving application shall not raise an error due to the presence or absence of the element.
If the predicate is NOT satisfied: The conformant sending application shall not populate the
9585 element. The conformant receiving application may raise an application error if the element is present.

X: Not supported. For conformant sending applications, the element will not be sent. Conformant receiving applications may ignore the element if it is sent, or may raise an application error.

9590 • Cardinality: Within square brackets, minimum and maximum number of occurrences authorized for this segment in the context of this Integration Profile.

• HL7 chapter: Reference of the HL7 v2.5 chapter that describes this segment.

C.1.2: Static definition – Segment level and Data Type level

9595 The Segment table and the Data Type table each contain 8 columns:

• **SEQ**: Position (sequence) of the field within the segment.

• **LEN**: Maximum length of the field

• **DT**: Field Data Type

• **Usage**: Usage of the field within this IHE Integration Profile. Same coded values as in the
9600 message level: R, RE, C, CE, O, X.

• **Cardinality**: Minimum and maximum number of occurrences for the field in the context of this Integration Profile.

• **TBL#**: Table reference (for fields using a set of defined values)

• **ITEM#**: HL7 unique reference for this field

9605 • **Element Name**: Name of the field in a Segment table. / Component Name: Name of a subfield in a Data Type table.

Table C1.2-1: Example: The MSH segment description

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	Element name

1	1	ST	R	[1..1]		00001	Field Separator
2	4	ST	R	[1..1]		00002	Encoding characters
3	227	HD	R	[1..1]	0361	00003	Sending Application
…							

9610 C.2:   HL7 Implementation Notes

C.2.1: Network Guidelines

The HL7 2.5 standard does not define a network communications protocol. Beginning with HL7 2.2 , the definitions of lower layer protocols were moved to the Implementation Guide, but are not HL7 requirements. The IHE Framework makes these recommendations:

9615
1. Applications shall use the Minimal Lower Layer Protocol defined in Appendix C of the HL7 Implementation Guide.

2. An initiating application that wants to send a message (initiate a transaction) will initiate a network connection to start the transaction. The receiver application will respond with an acknowledgement or response to query over the open connection. The initiating application
9620   can initiate a new transaction on the same connection. However, the initiating application must be able to handle cases where the connection has been closed due to possible timeout by the accepting application. For example if the initiating application does not submit a request over the connection in a timely manner, the accepting application has the right to close the connection. When this condition is detected, the initiating application needs to open a new
9625   connection for subsequent requests.

C.2.2: Message Control

According to the HL7 standard, each message shall begin with the MSH (message header) segment. Table C.2.2-1 identifies all required fields in this message. This table shall be interpreted according to the HL7 Standard unless otherwise noted in Appendix C.

9630   **Table C.2.2-1 IHE Profile - MSH segment**

SEQ	LEN	DT	OPT	TBL#	ITEM #	ELEMENT NAME
1	1	ST	R		00001	Field Separator
2	4	ST	R		00002	Encoding Characters
3	180	HD	R+		00003	Sending Application
4	180	HD	R+		00004	Sending Facility
5	180	HD	R+		00005	Receiving Application
6	180	HD	R+		00006	Receiving Facility
7	26	TS	R		00007	Date/Time Of Message
8	40	ST	O		00008	Security
9	13	CM	R	0076/ 0003	00009	Message Type
10	20	ST	R		00010	Message Control ID
11	3	PT	R		00011	Processing ID

12	60	VID	R	0104	00012	Version ID
13	15	NM	O		00013	Sequence Number
14	180	ST	O		00014	Continuation Pointer
15	2	ID	O	0155	00015	Accept Acknowledgment Type
16	2	ID	O	0155	00016	Application Acknowledgment Type
17	3	ID	O	0399	00017	Country Code
18	16	ID	C	0211	00692	Character Set
19	250	CE	O		00693	Principal Language Of Message
20	20	ID	O	0356	01317	Alternate Character Set Handling Scheme
21	10	ID	O	0449	01598	Conformance Statement ID #

Adapted from the HL7 Standard, version 2.5 and version 2.3.1

Note: This element is only applicable in HL7 version 2.5 and thus is only applicable for those transactions based on HL7 v2.5

The IHE IT Infrastructure Technical Framework requires that applications support HL7-recommended values for the fields *MSH-1-Field Separator* and *MSH-2-Encoding Characters*.

9635   Field *MSH-18-Character Set* shall only be valued if the message utilizes character sets other than ISO IR-6, also known as ASCII.

Implementations supporting sequence number protocol (and using the field *MSH-13-Sequence Number)* shall be configurable to allow them to perform transactions without such protocol.

C.2.3: Acknowledgment Modes

9640   The information in this section reflects the usage of acknowledgement and error segments in HL7 v2.5.

Common ACK static definition:

Segment	Meaning	Usage	Card.	HL7 chapter
MSH	Message Header	R	[1..1]	2
MSA	Message Acknowledgement	R	[1..1]	2
ERR	Error	C	[0..*]	2

The ACK message is in all cases an application level acknowledgement, which conveys application errors (if any) detailed by the receiving application.

9645   The receiving application shall application-reject an incoming message, if it does not recognize either the message type (MSH-9.1) or the trigger event (MSH-9.2).

Field MSA-1 of the acknowledgement shall contain the value **AR**.

The components of Field ERR-2 of the acknowledgement shall be populated as follows.

ERR-2.1:   **MSH**

ERR-2.2:   **1**

9650   ERR-2.3:   **9**

ERR-2.4:   **1**

ERR-2.5:   **1**   if an unrecognized message type

2   if an unrecognized trigger event

The components of Field ERR-3 of the acknowledgement shall be populated as follows.

9655   ERR-3.1:   **200**   if an unrecognized message type

                        201   if an unrecognized trigger event

          ERR-3.2:   **Unsupported message type** or

                        Unsupported trigger event as appropriate

          ERR-3.3:   **HL70357**

9660   Details of field encoding of these segments are discussed in the following sections.

C.2.3.1:   MSA - Message Acknowledgement segment

Standard Reference: HL7 Version 2.5, Chapter 2 (Section 2.15, "Message control")

This segment contains information sent while acknowledging another message.

Table C.2.3.1-1: MSA - Message Acknowledgement

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	Element name
1	2	ID	R	[1..1]	0008	00018	Acknowledgement code
2	20	ST	R	[1..1]		00010	Message Control Id
3	80	ST	X	[0..0]		00020	Text Message
4	15	NM	O	[0..1]		00021	Expected Sequence Number
5			X	[0..0]		00022	Delayed Acknowledgment Type
6	250	CE	X	[0..0]	0357	00023	Error Condition

9665   **MSA-1 Acknowledgment Code (ID)**, required.

As is the case throughout IHE, original mode acknowledgement is in use. IHE ITI authorizes only one of the three values below, taken from *HL7 Table 0008 - Acknowledgement code*:

Table C.2.3.1-2: HL7 table 0008 - Acknowledgement code

Value	Description	Comment
AA	Original mode: Application Accept	The message has been accepted and integrated by the receiving application
AE	Original mode: Application Error	The message contains errors. It SHALL not be sent again without correcting the error.
AR	Original mode: Application Reject	The message has been rejected by the receiving application. If the rejection is not related to an invalid value in the MSH segment, the sender may try again to send the message later.

MSA-2 Message Control ID (ST), required.

9670   Definition: This field contains the message control ID from Field *MSH-10-Message Control ID* of the incoming message for which the acknowledgement is sent.

MSA-3 Text Message (ST), not supported. See the ERR segment.

MSA-6 Error Condition (CE), not supported. See the ERR segment.

C.2.3.2:   ERR - Error segment

9675   Standard Reference: HL7 Version 2.5, Chapter 2 (Section 2.15, "Message control")

This segment is used to add error comments to acknowledgment messages.

Table C.2.3.2-1: ERR – Error segment

SEQ	LEN	DT	Usage	Card.	TBL#	ITEM#	Element name
1	493	ELD	X	[0..0]		00024	Error Code and Location
2	18	ERL	RE	[0..*]		01812	Error Location
3	705	CWE	R	[1..1]	0357	01813	HL7 Error Code
4	2	ID	R	[1..1]	0516	01814	Severity
5	705	CWE	O	[0..1]	0533	01815	Application Error Code
6	80	ST	O	[0..10]		01816	Application Error Parameter
7	2048	TX	O	[0..1]		01817	Diagnostic Information
8	250	TX	O	[0..1]		01818	User Message
9	20	IS	O	[0..*]	0517	01819	Inform Person Indicator
10	705	CWE	O	[0..1]	0518	01820	Override Type
11	705	CWE	O	[0..*]	0519	01821	Override Reason Code
12	652	XTN	O	[0..*]		01822	Help Desk Contact Point

ERR-1 is deprecated in HL7 Version 2.5 (*i.e.*, retained for backward compatibility only) and therefore not supported by IHE.

9680   **ERR-2** is populated except when the error is not within an HL7 field, component or subcomponent. For example, if the receiver returns an acknowledgement containing *MSA-2-acknowledgement code* value **AR** to indicate that the receiving application was unavailable, ERR-2 is not populated.

ERR-3 HL7 Error Code (CWE) is required. It identifies the HL7 (communication) error code. Valid values are given by HL7 Table 0357:

9685   HL7 Table 0357 - Message error condition codes

Value	Description	Comment
0	Message accepted	Success. Optional, as the AA conveys success. Used for systems that must always return a status code.
100	Segment sequence error	Error: The message segments were not in the proper order, or required segments are missing.
101	Required field missing	Error: A required field is missing from a segment
102	Data type error	Error: The field contained data of the wrong data type, e.g. an NM field contained "FOO".
103	Table value not found	Error: A field of data type ID or IS was compared against the corresponding table, and no match was found.
200	Unsupported message type	Rejection: The Message Type is not supported.
201	Unsupported event code	Rejection: The Event Code is not supported.
202	Unsupported processing id	Rejection: The Processing ID is not supported.
203	Unsupported version id	Rejection: The Version ID is not supported.
204	Unknown key identifier	Rejection: The ID of the patient, order, etc., was not found. Used for transactions *other than* additions, e.g. transfer of a non-existent patient.
205	Duplicate key identifier	Rejection: The ID of the patient, order, etc., already exists. Used in response to addition transactions (Admit, New Order, etc.).
206	Application record locked	Rejection: The transaction could not be performed at the application storage

Value	Description	Comment
		level, e.g., database locked.
207	Application internal error	Rejection: A catchall for internal errors not explicitly covered by other codes.

ERR-4 Severity (ID) is required. It identifies the severity of an application error. Valid values are given by HL7 Table 0516:

HL7 Table 0516 – Error severity

Value	Description	Comment
W	Warning	Transaction successful, but there may be issues
I	Information	Transaction was successful but includes information, *e.g.*, inform patient
E	Error	Transaction was unsuccessful

C.2.4: Common Segment Definitions

9690   The following table specifies the contents of the EVN segment that is common to several HL7-based transaction messages defined in this volume.

Table C.2.4-1 IHE Profile - EVN segment

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	3	ID	O	0003	00099	Event Type Code
2	26	TS	R		00100	Recorded Date/Time
3	26	TS	O		00101	Date/Time Planned Event
4	3	IS	O	0062	00102	Event Reason Code
5	60	XCN	O	0188	00103	Operator ID
6	26	TS	R2		01278	Event Occurred
7	180	HD	O		01534	Event Facility #

Adapted from the HL7 Standard, version 2.5 and version 2.3.1

Note: This element is only applicable in HL7 version 2.5 and thus is only applicable for those transactions based on HL7 v2.5

9695   Field *EVN-1-Event Type Code* is optional; however, if present, its value shall be equal to the second component of the field *MSH-9-Message Type*.

C.2.5: Message granularity

The sending application shall send as many messages as there are events recorded. For instance, if at the same time there is a change both to the patient's location (from emergency room to GI surgery ward)
9700   and to the patient's attending doctor (from Dr. Eric Emergency to Dr. John Appendectomy), the sending application will transmit two movements using HL7 messages ADT^A02 (transfer) and ADT^A54 (change attending doctor). Both events will have the same effective date/time (EVN-6 – Event Occurred). If the Historic Movement option is in use, each of these movements will have a unique identifier.

9705   The exceptions to this fine granularity are:

- The Admit Inpatient (A01) and Register Outpatient (A04) events can also assign a location and an attending doctor to the patient, known when the event is recorded.

- A change of patient class (A06 or A07) also assigns at the same time a new location to the patient.

9710
- The Cancel Discharge/End Visit event also includes at the same time the patient location after the cancellation has been processed.

C.2.6: HL7 empty field convention

According to the HL7 standard, if the value of a field is not present, the receiver shall not change corresponding data in its database. However, if the sender defines the field value to be the explicit
9715 NULL value (i.e., two double quotes ""), it shall cause removal of any values for that field in the receiver's database. This convention is fully applied by IHE profiles based on HL7 v2.x messages.

Appendix D: Cross-Profile Interactions of PIX and PSA

When the Context Manager Actor in a Patient Synchronized Application Integration Profile is grouped
with a Patient Identifier Cross-reference Consumer in a Patient Identifier Cross-referencing Integration
Profile, patient identifiers must be accessible to both actors in a consistent manner. This Appendix
provides the necessary mapping rules.

The Patient Identifier Cross-Referencing (PIX) Integration Profile defines a general-purpose mapping of
a Patient ID within a Patient Identification Domain to aliases in other Patient Identification Domains.
This mapping is intended to be used across all IHE systems that require patient identification in
transactions crossing Patient Identification Domains. The PIX Integration Profile relies on HL7 V2
Transactions.

The Patient Synchronized Application Integration Profile relies on HL7 CCOW which, confronted with
a similar need, has defined a Patient Mapping API within its architecture. The HTTP Technology
mapping for the CCOW Patient Mapping Agent API supports its operation over a network interface,
thus creating an alternative to HL7 V2 messages.

As IHE strives to avoid the inclusion in its integration profiles of incompatible but functionally
equivalent variants, it has decided to use HL7 V2 ADT messages for the Patient Identifier Cross-
referencing Integration Profiles. In consequence, the combined use of the Patient Synchronized (CCOW
based) Integration Profile and of the Patient Identifier Cross-referencing Integration profiles requires
that the IHE Context Manager Actor uses the services of the PIX Integration Profile. To do so, the
Patient Identifier Cross-reference Consumer Actor in communication with the Patient Identifier Cross-
reference Manager Actor operates as a substitute for the CCOW Patient Mapping Agent. This is shown
in diagram D-1 below as a dashed oval surrounding the Patient Cross-reference Manager and the Patient
Identifier Cross-reference Consumer actors. As a result it is likely that a context management solution
would bundle a PMA proxy application that would implement the PIX Query in support of the Patient
Identifier Cross-reference Consumer Actor.
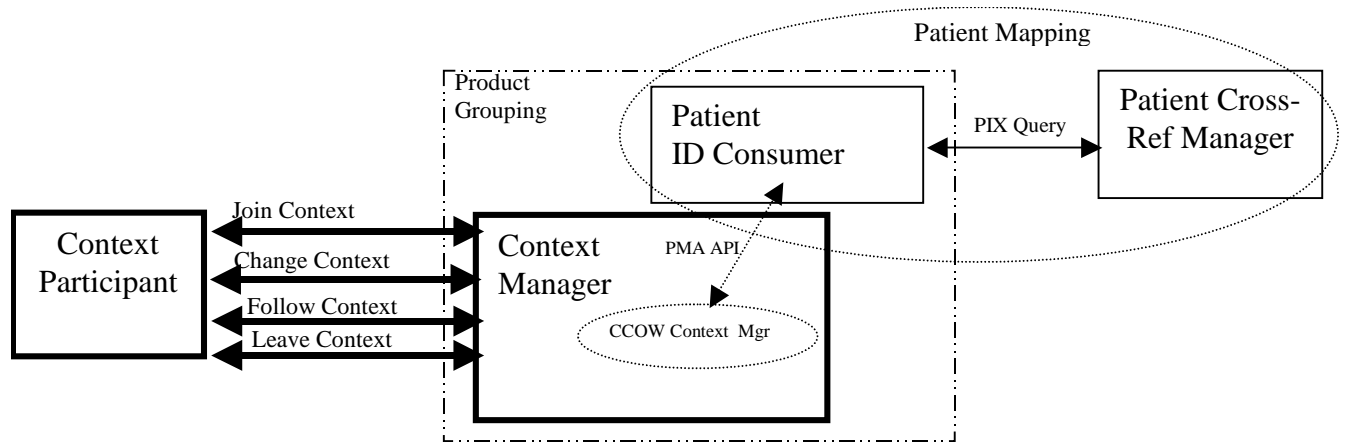
Figure D-1: Actor Grouping Diagram

This Appendix provides the definition of the mapping of the CCOW Patient Mapping Agent API
methods onto the PIX Query Transaction (HL7 V2 QBP^Q23/RSP^K23) as defined by the PIX
Integration Profile.

Table D-1 shows the definition of the Patient Mapping Methods parameters as implemented in Web
technology. Most of these Arguments relate to the normal operations of the Patient Mapping Agent
methods that pose no mapping challenge except for the ItemNames and ItemValues which pose some
constraints. The first constraint comes from the translation of Patient Identity Domains for both query
and response from and to a CCOW defined name / value pair. The second one comes from the fact that
CCOW participant applications can set more than one identifier in context the ability to detect when
these identifiers represent the identities of more than one patient. IHE has taken steps to mitigate these
issues by further restricting how the IHE Context Participant implements the methods. Each of these
constraints is addressed in sections below.

Table D-1 ContextChangesPending

Argument Name	Data Type	Comment
HTTP Request Message		
Interface	string	"ContextAgent"
Method	string	"ContextChangesPending"
agentCoupon	long	"-1"
contextManager	string	URL for the Context Manager that is requesting the patient id cross-reference
itemNames	string[]	One or more item names (e.g. Patient.Id.IdList)
itemValues	string[]	The patient identifiers corresponding to the domains identified in item names
contextCoupon	long	Context Coupon value for pending context change transaction
managerSignature	string	Not required
HTTP Reply Message		
agentCoupon	long	"-1"
itemNames	string[]	See below for valid item names for patient subject
itemValues	string[]	See below for any constraints on item values
contextCoupon	long	Return the value provided in request
agentSignature	string	Not required
Decision	string	"valid" or "invalid"
Reason	string	Reason text if mapping is invalid

Adapted from the HL7 Context Management "CCOW" Standard, version 1.4

D.1: Namespace Translation from PIX Query to CCOW

The CCOW standard defines multiple identifier items that may be set into the context by an instigating
participant application. The current list of valid identifier names are listed in Table D-2.

Table D-2 Patient Subject Identifiers

Patient Subject Identifier Item Name	HL7 Meaning	HL7 Data Type	HL7 Semantic Constraints on Values	Case Sensitive
Patient.Id.MRN.*Suffix*	Patient medical record number, per PID-2	ST	HL7 Table 0203 Identifier Type = MR	No
Patient.Id.MPI	Patient identifier in the "Master Patient	ST	HL7 Table 0203 Identifier Type = PT or PI (as agreed upon by context sharing systems) and	No

Patient Subject Identifier Item Name	HL7 Meaning	HL7 Data Type	HL7 Semantic Constraints on Values	Case Sensitive
	Index", per PID-2		Assigning Authority represents the MPI system	
Patient.Id.NationalIdNumber	Patient national identifier number, per PID-2	ST	HL7 Table 0203 Identifier Type = PT and Assigning Authority represents agreed upon National Authority	No
Patient.Id.IdList	A list of patient identifiers for a patient, per PID-3	CX	May be a repeating set of CX item values (per Section 1.7 of the HL7 Context Management "CCOW" Standard: Subject Data Definitions document), each of which contains an identifier that denotes the same patient	No

Adapted from the HL7 Context Management "CCOW" Standard, version 1.4

9765 IHE has specified in the Context Change Transaction as documented in ITI TF-2 that the Context Participant Actor shall use the Patient.Id.IdList item. The intent is to eliminate translation as the Patient.Id.IdList value maps directly to PIX Query Transaction QPD-3.

Applications using in their identifier items Patient.Id.MRN.Suffix will need to migrate to the Patient.Id.IdList item as expected by the HL7 CCOW standard.

9770 D.2: Processing Multiple Identifiers

CCOW participant applications are permitted to populate as many patient identifiers as they have available to them. This means that when a user selects a patient in one of these applications the context is populated with multiple identifiers for the selected patient. When the CCOW Patient Mapping Agent (PMA) accepts multiple patient identifiers as input, the PMA has the responsibility of invalidating
9775 patient mapping and causing the context change transaction to be cancelled if it determines that the multiple identifiers supplied as part of the transaction identify more than one patient.

The QPD segment as defined in the IHE PIX Query Transaction specifies a single identifier uniquely identifying one patient within a given Patient Identification Domain. In the case where multiple identifiers are populated, the context manager may have to process the response to the initial PIX Query
9780 Transaction to evaluate if the other identifiers in context are included. If so, no further processing is required. Otherwise, an additional PIX Query will need to be issued and the results processed. Should a non-null result be returned, indicating the identifier uniquely identifies a different patient for the given domain, the context manager shall assume "invalid" in the decision field and "multiple patients identified" in the reason field.

9785 In order to mitigate this condition, IHE specifies that all context participants supporting the Patient Synchronized Applications profile shall only set one identifier for the patient when a Patient Identifier Cross-referencing Integration Profile is used by the context manager. This means that the context participant for those applications that manage multiple patient identifiers will need to be configurable as to which identifier item is passed in the Change Context Transaction.

9790   # Appendix E: Usage of the CX Data Type in PID-3-Patient Identifier List

The Health Level Seven Standard (HL7) uses data type CX to express various identifiers, including the Patient ID in the third field of the PID segment. We discuss here how IHE IT Infrastructure expects the CX data type to be populated in the *PID-3-Patient Identifier List* fields of messages that it defines.

Requirements for populating the elements of *PID-3-Patient Identifier List* vary slightly, depending on
9795   what actor is originating the transaction in which the PID segment is sent. If the Patient Identifier Cross-reference Manager is the source of the PID segment, the requirements (specifically, with respect to populating the Assigning Authority subcomponents) are more rigorous than otherwise.

PID-3-Patient Identifier List permits multiple occurrences of the CX data type. Data type CX contains 8 components as shown below. This structure allows expression of the value and context for each
9800   identifier that the system knows.

Table E-1: Components of HL7 Data Type CX

Cmp	Len	DT	Opt	Tbl	Name
1	15	ST	R		ID
2		ST	O		Check digit
3		ID	O	0061	Code identifying the check digit scheme employed
4	227	HD	R		Assigning authority
5		ID	O	0203	Identifier type code
6		HD	O		Assigning facility
7		DT	O		Effective date
8		DT	O		Expiration date

Adapted from the HL7 Standard, Version 2.5

Each occurrence of *PID-3-Patient Identifier List* contains, at a minimum, an identifier value in Component 1 and an assigning authority in Component 4. The assigning authority unambiguously
9805   provides the context for the identifier. It is also common practice to provide an identifier type code in Component 5, but this is not required by IHE. Other components are optional and will not be discussed here; implementers may refer to HL7 Version 2.5 for more information.

Component 1 of Data Type CX, **ID**, is of data type ST. This data type allows a free text value of up to 15 characters.[8]

9810   Component 4 of Data Type CX, **Assigning Authority**, is of data type HD. This data type contains 3 components that, when implemented at the component level, become subcomponents of Component 4. The requirements for the subcomponents of Component 4 vary by actor.

E.1:   Patient Identifier Cross-reference Manager actor requirements

The Patient Identifier Cross-reference Manager Actor is expected to have access to complete internal
9815   and external identifier information for the Assigning Authority of the patient identifier. To facilitate interoperability, it is required that the Patient Identifier Cross-reference Manager Actor populate <u>all</u>

---

8   As implemented in HL7 Version 2.5. Prior to Version 2.5, HL7 did not specify the length of individual components. Although the profiles in IHE-ITI are based Versions 2.3.1 and 2.4 of HL7, they use the component length constraints provided by Version 2.5 to support forward compatibility.

subcomponents of the Assigning Authority component. The usage of these subcomponents will be explained in the examples below.

This requirement applies to the response portion of Transaction ITI-9 (PIX Query) and to Transaction ITI-10 (PIX Update Notification).

Table E-2: Usage of HL7 Data Type CX by the PIX Manager Actor

Cmp	Sbc	Len	DT	Opt	Tbl	Name	Conditionality predicate
1		15	ST	R		ID	
2			ST	O		Check digit	
3			ID	O	0061	Code identifying the check digit scheme employed	
4		227	HD	R		Assigning authority	Subcomponent 1 must refer to the same entity as Subcomponents 2 and 3.
4	1	20	IS	R	0363	Namespace ID	
4	2	199	ST	R		Universal ID	
4	3	6	ID	R	0301	Universal ID type	
5			ID	O	0203	Identifier type code	
6			HD	O		Assigning facility	If all three subcomponents are populated, they must refer to the same entity.
6	1		IS	O	0300	Namespace ID	
6	2		ST	C		Universal ID	Populated if, and only if, Subcomponent 3 is populated.
6	3		ID	C	0301	Universal ID type	Populated if, and only if, Subcomponent 2 is populated
7			DT	O		Effective date	
8			DT	O		Expiration date	

IHE specifies that the Patient Identifier Cross-reference Manager actor must populate all 3 subcomponents of Component 4. The following rules apply:

Subcomponent 1 of Component 4, **Namespace ID**, is of data type IS. HL7 specifies that when valued in the Patient ID field, the value in this subcomponent be a code taken from user-defined Table 0363, *Assigning Authority*. Version 2.5 of HL7 provides suggested values for assigning authorities in various local jurisdictions, such as **USSSA** for U.S. Social Security Administration. Sites may add values to this table, but for interoperability must ensure that added values (and meanings) are agreed upon by all communicating systems.

Subcomponent 2 of Component 4, **Universal ID**, is of data type ST. This subcomponent contains a value from either a known external domain or a specified internal domain. The domain is given in Subcomponent 3.

Subcomponent 3, **Universal ID Type**, is of data type ID. This subcomponent contains a code taken from HL7 Table 0301, *Universal ID Type*. Table 0301 contains values for various known external identifier domains such as **DNS** (Internet dotted name) and **ISO** (International Standards Organization Object Identifier, or OID), as well as the values **L, M,** and **N** to permit the use of internal identifier domains.

Subcomponent 1 must refer to the same entity as Subcomponents 2 and 3.

E.2:   Other actor requirements

9840   The PID segment may also appear in messages generated by other IHE Actors, including the Patient ID Cross-reference Consumer and the Information Source.   These actors must also populate the Assigning Authority.

However, IHE specifies that they need not populate all three subcomponents of Assigning Authority. They must populate either Namespace ID (an entry from a user-defined table), or Universal ID and
9845   Universal ID Type (allowing the use of an externally defined identifier scheme).

This requirement applies to Transaction 8 (Patient Identity Feed), to the query portion of Transaction ITI-9 (PIX Query), and to any other transaction (except for the response portion of ITI-9 and for ITI-10) that populates *PID-3-Patient Identifier List*.

Table E-3: Usage of HL7 Data Type CX by other IHE Actors

Cmp	Sbc	Len	DT	Opt	Tbl	Name	Conditionality predicate
1		15	ST	R		ID	
2			ST	O		Check digit	
3			ID	O	0061	Code identifying the check digit scheme employed	
4		227	HD	R		Assigning authority	If all three subcomponents are populated, they must refer to the same entity.
4	1	20	IS	C	0363	Namespace ID	Must be populated if Subcomponents 2 and 3 are not populated.
4	2	199	ST	C		Universal ID	Must be populated if Subcomponent 1 is not populated. Populated if, and only if, Subcomponent 3 is populated.
4	3	6	ID	C	0301	Universal ID type	Must be populated if Subcomponent 1 is not populated. Populated if, and only if, Subcomponent 2 is populated.
5			ID	O	0203	Identifier type code	
6			HD	O		Assigning facility	If all three subcomponents are populated, they must refer to the same entity.
6	1		IS	O	0300	Namespace ID	
6	2		ST	C		Universal ID	Populated if, and only if, Subcomponent 3 is populated.
6	3		ID	C	0301	Universal ID type	Populated if, and only if, Subcomponent 2 is populated.
7			DT	O		Effective date	
8			DT	O		Expiration date	

9850   The definitions of the subcomponents of Component 4 are as given above for the Patient Identifier Cross-reference Manager actor. If all three subcomponents are defined, Subcomponent 1 must refer to the same entity as Subcomponents 2 and 3.

E.3: Examples of use

Metropolitan Medical Center treats a patient, Jane Smith, for whom 3 identifiers are known. (For this example, assume that the HL7 V2 default delimiters are in use: | for field separator, ^ for component separator, ~ for repetition separator and & for subcomponent separator.)

E.4: Data sent by source systems

The source systems provide data to the Patient Identifier Cross-reference Manager. These data are sent either in a Patient Identity Feed transaction [ITI-8] or in response to a PIX Query.

Patient Smith's Social Security number is **999-99-4452**. This number is assigned by the U.S. Social Security Administration.

> The ADT system sends the Social Security number at registration, in an occurrence of *PID-3-Patient Identifier List* that looks like this:
>
> ### 999-99-4452^^^USSSA
>
> Note that only Subcomponent 1 of Assigning Authority is assigned here, while Subcomponents 2 and 3 are left empty.

Patient Smith's medical record number is **9990-99497**. This number is assigned by Metropolitan Medical Center, for which no external identifier is known. Metropolitan Medical Center incorporates the Namespace ID **99MMC** for the medical record numbers it assigns.

> The ADT system sends the medical record number at registration, in an occurrence of *PID-3-Patient Identifier List* that looks like this:
>
> ### 999099497^^^99MMC
>
> Note again that only Subcomponent 1 of Assigning Authority is assigned here.

Patient Smith's medical insurance number is **99998410**. This number is assigned by MLH Life & Casualty Company, whose Internet domain name is **www.mlhlifecasualty.com**.9

> The billing system sends the medical insurance number in an occurrence of *PID-3-Patient Identifier List* that looks like this:
>
> ### 99998410^^^&www.mlhlife.com&DNS
>
> Note that only Subcomponents 2 and 3 of Assigning Authority are assigned here. Also note the value **DNS** in the third subcomponent of Component 4 to indicate an Internet domain name.

E.5: Data sent by the Patient Identifier Cross-reference Manager

The Patient Identifier Cross-reference Manager implements HL7 Table 0363, *Assigning Authority*, by incorporating the values in HL7 Version 2.5 as well as the values **99MMC** for Metropolitan Medical

---

9   Implementers should take into account the possibility that, as with any domain identifier, Internet domain identifiers – either fully qualified domain names (FQDNs) or IPv4 or IPv6 addresses – are liable to change.

9885   Center and **99MLHLIFE** for MLH Life & Casualty.10 It also includes a known ISO Object Identifier for the Social Security Administration, **1.2.mm.nnnnn.555.6666**.11

To send the identifiers in *PID-3-Patient Identifier List*, the Patient Identifier Cross-reference Manager builds and concatenates them as follows.

9890   In the first occurrence, the Social Security number is sent in the first component, as well as the known internal and external values for SSN assigning authority in the fourth component. Note the value **ISO** in the third subcomponent of Component 4 to indicate an ISO Object Identifier.

`999-99-4452^^^USSSA&1.2.mm.nnnnn.555.6666&ISO`

9895   In the second occurrence, the medical insurance number is sent in the first component, as well as the known internal and external values for insurance number assigning authority in the fourth component.

`99998410^^^99MLHLIFE&www.mlhlife.com&DNS`

9900   In the third occurrence, the medical record number is sent in the first component, as well as the known internal and external values for MRN assigning authority in the fourth component. Note that no external value is known for MRN assigning authority, so the HIS repeats the internal value as an external value and uses the value **L** in the third subcomponent of Component 4 to indicate a locally assigned value.

9905   `999099497^^^99MMC&99MMC&L`

In sending all values in a PIX Update Notification transaction [ITI-10], the Patient Identifier Cross-reference Manager concatenates the three *PID-3-Patient Identifier List* values using the repetition separator:

`|999994452^^^USSSA&1.2.mm.nnnnn.555.6666&ISO~99998410^^^99ABCLIF`
9910   `E&www.abclife.com&DNS~999099497^^^99MMC&99MMC&|`

---

10   The use of **99** to preface these codes is not mandated by HL7, but reflects the practice directed by Chapter 7 of HL7 Version 2.5 for specifying local coding system values.

11   This OID is fictitious. The real OID for the SSA should be substituted here.

Appendix F: Intentionally Left Blank

Appendix G: Transition from Radiology Basic Security to ATNA

Retired.

9915

The previous appendix G was an XSLT that demonstrated the format translation from the Basic Radiology Schema to the RFC-3881 Schema. It did not generate the correct controlled vocabulary terms. This caused confusion. A variety of techniques can be used to perform this conversion. The IHE ITI Technical Framework does not specify any particular technique that should be used or will be maintained.

_____

Appendix H: Required Registry Initialization and Schema

9920 ### H.1: Initialization

A standard ebXML Registry must be initialized with key Classification Schemes and object types to support XDS. An ebXML Registry SubmitObjectsRequest is available to perform this initialization. It includes:

- Classification Schemes that anchor the definition of ExternalIdentifiers

9925
- Additions to the ObjectType ClassificationScheme that introduces a general XDS ClassificationNode that anchors these additions. The usable new ClassificationNodes are: XDSDocumentEntry, XDSDocumentEntryStub, XDSFolder, and XDSSubmissionSet. XDSDocumentEntry and XDSDocumentEntryStub are used as new objectTypes for use in an ExtrinsicObjectto create XDS specific object types. XDSFolder and XDSSubmissionSet are
9930 used to classify RegistryPackage objects to label them as XDS Folders or XDS SubmissionSets.

- External Classification Schemes to support attribute coding.

This initialization includes the assignment of UUIDs to these definitions. These pre-assigned UUIDs shall be used when implementing XDS.

H.2: Schema

9935 An XML Schema has been defined for XDS.

H.3: Location

These resources be found on the IHE website:

http://www.ihe.net

Select *Resources* tab (one of the tabs listed across the top of the page)

9940 Select *Integration Profiles – Supplemental Information*

Navigate to the XDS section

_____

_____

Appendix I: Required Initialization of the XDS Affinity Domain

This initialization supports the operation of the Registry Adaptor. The following information must be
9945   provided by the XDS Affinity Domain administrator and loaded into the Registry Adaptor. This
supports the functionality specified for the Registry Adaptor in section 3.14.4.1.2.11. How this
information is loaded into the Registry Adaptor or how the Registry Adaptor is implemented is not
defined by this profile.

1. List of acceptable mimeTypes for documents indexed by the registry.

9950   2. PIX domain name (Assigning Authority) for XDS Affinity Domain. PatientIds attached to
metadata submitted to this registry must come from this PIX Assigning Authority.

3. Acceptable values for all coded attributes represented in the registry by ebXML External
Classifications. These include classCode, eventCode, confidentialityCode,
healthCareFacilityTypeCode, formatCode for XDS Document and XDSSubmissionSet.code and
9955   XDSFolder.codeList.

_____

Appendix J: Example Submissions and Query Results

Links to reference information like: sample submissions, queries, query results and frequently asked questions may be found on the IHE website at:

9960   http://www.ihe.net/IT_infra/committees/index.cfm

Appendix K: XDS Security Environment

This Appendix expands on the summary provided in the XDS Volume 1 specification (ITI TF-1: Appendix H).

9965 The XDS operations assume that a suitable security and privacy environment has been established. Almost all of the relevant threats will be managed by agreements, policies, and technologies that are external to the XDS transactions. The few that affect the XDS transactions will be managed by generic security mechanisms that are not unique to XDS. The threats and security objectives that must be addressed are described in sections 1 and 2 below. Only a few of these have issues that are unique to the XDS application.

9970 Section 3 discusses these few threats and objectives in terms of the agreements and policies that need to be established to create a suitable environment for XDS. Establishing these agreements often involves business agreement discussions that are part of establishing the XDS Affinity Domain. These agreements are necessary because the exchange of documents implies agreeing to the delegation of responsibility for maintaining the security of these documents and for providing the necessary audit and record keeping facilities.

K.1: Security Environment

K.1.1: Threats

Specific threats to the overall XDS system are listed below. These threats are identified using the Common Criteria nomenclature defined by ISO 17799. Most of these are mitigated by policies, procedures, and technologies that are not unique to XDS and do not require any special XDS considerations. Many of these mitigations do require that the parties within the XDS Affinity Domain have agreement on details of how they will work together.

T.ADMIN_ERROR Improper administration may result in defeat of specific security features.

9985 **T.ADMIN_ROGUE** Authorized administrator's intentions may become malicious resulting in TSF data to be compromised.

T.AUDIT_CORRUPT A malicious process or user may cause audit records to be lost or modified, or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.

9990 **T.CONFIG_CORRUPT** A malicious process or user may cause configuration data or other trusted data to be lost or modified.

T.DISASTER System or network may failure due to disaster (e.g. fire, earthquake).

T.DOS A malicious process or user may block others from system resources via a resource exhaustion denial of service attack.

9995 **T.EAVESDROP** A malicious process or user may intercept transmitted data inside or outside of the enclave. Some of the XDS environments are not concerned with eavesdrop exposure. They may employ external protective mechanisms such as physical network security or VPNs to protect against eavesdropping.

T.HARDWARE Hardware may malfunction.

10000   **T.IMPROPER_INSTALLATION** XDS components may be delivered, installed, or configured in a manner that undermines security.

T.INSECURE_START   Reboot may result in insecure state of the operating system.

T.INTRUSION   Malicious software (e.g. virus) may be introduced into the system.

T.MASQUERADE   A malicious process or user on one machine on the network may masquerade as
10005   an entity on another machine on the same network.

T.OBJECTS_NOT_CLEAN   Systems may not adequately remove the data from objects between usage by different users, thereby releasing information to a user unauthorized for the data. This also includes swapping hard disk with PHI during service and repair.

T.POOR_DESIGN   Unintentional or intentional errors in requirement specification, design or
10010   development of the TOE components may occur.

T.POOR_IMPLEMENTATION   Unintentional or intentional errors in implementing the design of the XDS environment may occur.

T.POOR_TEST   Incorrect system behavior may result from inability to demonstrate that all functions and interactions within the XDS operation are correct.

10015   **T.REPLAY**   A malicious process or user may gain access by replaying authentication (or other) information.

T.SPOOFING   A hostile entity may masquerade itself as part of the XDS Affinity Domain and communicate with authorized users who incorrectly believe they are communicating with authorized members.

10020   **T.SYSACC**   A malicious process or user may gain unauthorized access to the administrator account, or that of other trusted personnel.

T.UNATTENDED_SESSION   A malicious process or user may gain unauthorized access to an unattended session.

T.UNAUTH_ACCESS   Unauthorized access to data by a user may occur. This includes access via
10025   direct user interaction with the device, access via network transactions, and access via removable electronic and printed media.

T.UNAUTH_MODIFICATION   Unauthorized modification or use of XDS attributes and resources may occur.

T.UNDETECTED_ACTIONS   Failure of the XDS components to detect and record unauthorized
10030   actions may occur.

T.UNIDENTIFIED_ACTIONS   Failure of the administrator to identify and act upon unauthorized actions may occur.

T.UNKNOWN_STATE   Upon failure of XDS components, the security of the XDS environment may be unknown.

10035   **T.USER_CORRUPT**   User data may be lost or tampered with by other users.

K.1.2: Security and Privacy Policy

There are a wide variety of security and privacy regulations established by law and regulation. These are interpreted and extended to create individual enterprise policies. This equipment will be installed into a variety of enterprises that are subject to a variety of laws and regulations. The XDS environment will provide support for the common aspects of these enterprise policies. The policy statements whose enforcement must be provided by the XDS security mechanisms are:

P.ACCOUNT The users of the system shall be held accountable for their actions within the system.

P.AUTHORIZATION The system must limit the extent of each user's abilities in accordance with the TSPP. (See P.PATIENT_CARE)

P.AUTHORIZED_USERS Only those users who have been authorized to access the information within the system may access the system. (See P.PATIENT_CARE)

P.CRYPTOGRAPHY The system shall use standard approved cryptography (methods and implementations) for key management (i.e., generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e., encryption, decryption, signature, hashing, key exchange, and random number generation services).

P.DECLARATIVE_SECURITY The system shall allow the administrator to define security related rules. Examples include defining access control policies and password expiration restriction.

P.I_AND_A All users must be identified and authenticated prior to accessing any controlled resources with the exception of public objects.

P.OBJECTAUTHORIZATION The XDS components must enforce the policy regarding how authorization is established for protected objects. The policy determines how access control and other policies are enforced. (This is often considered part of P.Authorization, but in the XDS context it may make sense to consider this as a separate policy.)

P.PATIENT_CARE The security and privacy measures should not prevent patient care. In particular, there should be emergency bypass mechanisms to override security when necessary to provide patient care.

P.SYSTEM_INTEGRITY The system must have the ability to periodically validate its correct operation and, with the help of Administrators, Backup and Restore Operators, and Service Personnel, it must be able to recover from any errors that are detected.

P.TRACE The primary method for enforcing the security and privacy policy is the use of auditing. The XDS components must have the ability to review the actions of individuals. The XDS environment must provide sufficient audit information to external audit and monitoring systems to permit the review of actions of individuals by that other system.

P.TRUSTED_RECOVERY Procedures and/or mechanisms shall be provided to assure that, after a system failure or other discontinuity, recovery without a protection compromise is obtained

P.VULNERABILITY_SEARCH The XDS environment must undergo an analysis for vulnerabilities beyond those that are obvious.

K.1.3: Security Usage Assumptions

Assumptions of the use of the XDS environment:

A.PHYSICAL It is assumed that appropriate physical security is provided within the domain for the value of the IT assets and the value of the stored, processed, and transmitted information.

A. AUDIT_REVIEW It is assumed that there will be audit repository and review services provided that can accept audit information from the XDS components in real time.

10080 **A.OPERATION** It is assumed that networks, firewalls, etc. are deployed and maintained to meet appropriate network security levels.

A.PERSONNEL It is assumed that the organization can assure IT user & other workforce personal integrity/trustworthiness.

A.PKI It is assumed that there will be a facility to provide signed certificates as needed for node and
10085 user authentication. The key management maybe done manually or automatically depending on the availability of appropriate technology.

K.2: Security Objectives

This section defines the security objectives for the XDS environment. These objectives are suitable to
10090 counter all identified threats and cover all identified organizational security policies and assumptions. Common Criteria nomenclature is used. The XDS component security objectives are identified with "O." appended to at the beginning of the name and the environment objectives are identified with "OE." appended to the beginning of the name.

K.2.1: XDS Component Security Objectives

10095 **O.ACCESS** The XDS components will ensure that users gain only authorized access to it and to the resources that it controls. (See O.EMERGENCY_BYPASS)

O.ACCESS_HISTORY The XDS components will display information (to authorized users) related to previous attempts to establish a session.

O.ADMIN_ROLE The XDS components will provide separate administrator roles to isolate
10100 administrative actions. These include a General Administrator role, a Backup and Restore Operator role, a Cryptographic Administrator role, and a Service Personnel role. Additional roles can be defined. These roles are collectively called Administrators.

O.ADMIN_TRAINED The XDS components will provide authorized Administrators with the necessary information for secure management and operation.

10105 **O.AUDIT_GENERATION** The XDS components will provide the capability to detect and create records of security and privacy relevant events associated with users. The XDS components will reliably transmit this information to the central audit repository, and provide reliable local storage of events until the central audit repository has confirmed receipt. (See OE.AUDIT_REVIEW)

O.AUDIT_PROTECTION Each XDS component will provide the capability to protect audit
10110 information within its scope of control.

O.AUDIT_REVIEW If an external central audit repository is not part of the environment, the components will be configured to provide limited capability to analyze and selectively view audit information. (See OE.AUDIT_REVIEW)

O.CONFIG_MGMT All changes to the components and its development evidence will be

10115   tracked and controlled.

O.DECLARATIVE_SECURITY The components will allow security functions and access control to be defined by the authorized administrator.

O.DISASTER_RECOVERY The components should allow the authorized Administrators to perform backup and restore of electronic data, and rapid configuration and reconfiguration of device

10120   operation. In addition, the TOE should support administrative procedures to restore operation after disasters that may have substantially destroyed portions of the hospital operation and where substitute temporary systems are in place.

O.DISCRETIONARY_ACCESS The components will control accesses to resources based upon the identity of users and the role of users. (See O.EMERGENCY_BYPASS)

10125   **O.DISCRETIONARY_USER_CONTROL** The components will allow authorized users to specify which resources may be accessed by which users and groups of users. (See O.EMERGENCY_BYPASS)

O.EMERGENCY_BYPASS The XDS components should allow access to any secured data during a declared medical emergency.

10130   **O.ENCRYPTED_CHANNEL** Based on the environmental policies, encryption may be used to provide confidentiality of protected data in transit over public network.

O.INSTALL The XDS components will be delivered with the appropriate installation guidance in the form of installation manuals and training to establish and maintain component security.

O.INTRUSION_DETECTION The XDS components will ensure intrusion of malicious software

10135   (e.g. virus) is detected.

O.MANAGE The XDS components will provide all the functions and facilities necessary to support the authorized Administrators in their management of the security of the TOE.

O.PROTECT The XDS components will provide means to protect user data and resources.

O.RECOVERY Procedures and/or mechanisms will be provided to assure that recovery is

10140   obtained without a protection compromise, such as from system failure or discontinuity.

O.REMOTE_SERVICE The XDS components will provide the means for remote service without sacrificing security or privacy policy.

O.RESIDUAL_INFORMATION The XDS components will ensure that any information contained in a protected resource is not released when the resource is reallocated. Information on permanent

10145   media such as hard disk shall be secured during service and repair.

O.RESOURCE_SHARING No user will block others from accessing resources.

O.SELF_PROTECTION Each XDS component will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.

O.TRAINED_USERS The XDS environment will provide authorized users with the necessary

10150   guidance for secure operation.

_____

O.TRUSTED_PATH   **The TOE** will provide a means to ensure users are not communicating with some other entity pretending to be the TOE. This covers entity authentication. (See O.USER_AUTHENTICATION.)

O.TRUSTED_SYSTEM_OPERATION   The XDS components will function in a manner that maintains security.

O.USER_AUTHENTICATION   The XDS components will verify the claimed identity of the interactive user. (See O.ENTITY_AUTHENTICATION.)

O.USER_IDENTIFICATION   The XDS components will uniquely identify the interactive users.

K.2.2: Environment Security Objectives

OE.PHYSICAL   Physical security will be provided within the domain for the value of the IT assets protected by the XDS environment and the value of the stored, processed, and transmitted information.

OE.AUDIT_REVIEW   There may be an audit repository and review service provided that can accept audit information from the XDS environment in real time. This facility will provide review and analysis functions. (See O.AUDIT_GENERATION, O.AUDIT_REVIEW)

OE.OPERATION   Networks, firewalls, etc. are deployed and maintained to meet appropriate network security levels.

OE.PERSONNEL   Assure IT user & other workforce personal integrity/trustworthiness.

OE.PKI   There will be a facility to provide signed certificates as needed for node and user authentication.

K.3: Functional Environment

The XDS can be modelled as having four different organizations that have a delegated responsibility relationship where each organization has a different functional responsibility. In some configurations a single organization is responsible for two or more of these functions, which makes delegation much easier. This section discusses the major areas that must be solved.

The four functions are:

Creator – This functional organization has created the PHI and is legally responsible to the patient and others for providing healthcare and for protecting this data.

Repository – This functional organization is responsible for providing access to persistent documents to readers. The creator has delegated responsibility to the repository to provide adequate protection for a subset of the PHI. This subset is called the document.

Registry - This functional organization is responsible for providing query services to readers. The creator has delegated responsibility to the to the registry to provide adequate protection for a subset of the PHI. This subset is called the metadata.

Reader – This functional organization is providing healthcare services that make use of data that is contained in the metadata and the documents.

There are three levels of difficulty in delegation.

_____

_____

"**Trivial**" delegation is that where it is not necessary to delegate the responsibility for implementing the threat mitigation. In those cases it does not matter whether the organizations have the same policy or mitigations. For example, if the registry provides adequate mitigation against the threat of disaster, it need not be concerned with the disaster related policies of the reader.

10190

"**Easy**" delegation is that where the two organizations have the equivalent policies. In those cases there is an initial difficult phase of discovering that the policies are the same and evaluating that the mitigation strategies are acceptable. This results in a simple binary decision to approve or disapprove a business relationship permitting the exchange of data. With the exception of the three policy classes described as "hard" below, the details of policies are likely to differ, but the goals are sufficiently uniform that a simple business decision can be made.

10195

For the "easy" delegation, the IHE transactions must provide adequate mitigations for the threats so that the business decision to exchange data can be made based simply on review of the partners policies and mitigations. This means that some IHE transactions will have additional security requirements attached. For example, encryption to avoid the threat of eavesdropping may be required. These requirements are not unique to XDS and will be able to use standardized security features like TLS and VPN tools. These requirements may be significantly different from the usual practice within an enterprise, because of the differences in the environment.

10200

"**Hard**" delegation is that where the two organizations have different policies or inconsistent/incompatible mitigation strategies. These are likely to occur for the following policies, where organizations often disagree on the details of the policy goals, and where policies often change:

10205

P.Authorization – The authorized access policies and authorized modification policies often differ, and are often subject to change. The changes that occur are often at a detailed level, e.g. access rights to a particular patient information may change. This means that either there is an agreed mechanism to propogate changes, or an acceptance that policy changes may not be enforced, or there will be restrictions on the data exchange to avoid delegating responsibility for data that is subject to change.

10210

P.Account and P.trace – The policies for accountability and traceability often differ. These are much less subject to change, but it is often difficult to reconcile delegation when these policies differ. This will be an especially difficult issue for repository and registry functions that support multiple different creator organizations.

10215

P.ObjectAuthorization – The policies regarding creation and modification of access rights often differ. In addition, any of the policy and threat mitigations may be determined to be unacceptable by creator, registry, or repository. In the simple situation where there are only four real world participants this simply means that there is no business relationship. In the more complex world where the registry or repository are in many relationships with many creators and readers it introduces a serious problem. Either the registry and repository must limit its relationship to that small set of creators and readers that mutually accept all the policies and mitigations of all the other organizations, or there must be a mitigation strategy so that creators can restrict delegations by the registry and repository to only those readers that have policies and mitigations that are acceptable to the creator.

10220

10225

Mitigations for differences include the following:

Limit the data exchange to that data where the differences are not significant. For example, highly sensitive data like psychiatric notes might not be shared, while relatively insignificant data like allergy information is shared.

_____

10230   Provide a revocation mechanism to deal with policy changes, so that future delegations can be prohibited. It is often impractical to revoke past delegations because the PHI has already been disclosed. But the revocation mechanism can stop further delegation from taking place. This revocation mechanism must be part of the P.Authorization and P.ObjectAuthorization policies and must be mutually acceptable for this mitigation to be effective.

10235   Trusted third party inspections and audits can sometimes deal with reconciliation of differences in P.Account and P.Trace.

An "approved delegation" list identifying acceptable and unacceptable creator/reader pairs can mitigate the repository and registry issues when the reader has incompatible policies with the creator. This does require the creator to accept the approved delegation policy and implementation of the repository and
10240   registry, but it reduces the combinatorial explosion of policy combinations between creators, repositories, registries, and readers into a linear growth in complexity.

The "approved delegation" may go further into identification of persons, but this is only a viable path when all parties have policies the easily support delegation of personal responsibility. Persons are usually required to comply with organizational policies, and organizations generally use roles rather than
10245   persons to establish policies. The often viable exception is the special case of the "deny access to person X". This can be a viable means of dealing with situations involving a conflict of interest. This kind of access denial may be applicable to just a particular subset of the PHI exchanged, (e.g. denying access to an ex-spouse).

These mitigations do not directly change the technical requirements for the XDS transactions. They are
10250   policy decisions that may affect how particular actors are configured. The implementation of XDS actors will need to be aware that this kind of site-specific configuration management and policy control will be routinely required.

Appendix L: Relationship of Document Entry Attributes and Document Headers

10255   XDS Document Entry attributes, placed in the XDS Document Registry by Document Sources, may be
derived from header data present in the document content. Although the XDS Integration Profile does
not mandate a strict relationship, this appendix illustrates sample mappings of XDS Document Entry
attributes to header fields of some standard document formats.   This relationship does not imply that
values are mapped or copied directly as transformations may be needed between conventions in the

10260   EHR-CR and EHR-LR (e.g. vocabulary mappings).

Table L-1 Relationship of XDS Document Attributes to Document header fields

Attribute	CDA R1-2000	CDA R2 Draft Aug 2004	EHRCOM
patientId	levelone >clinical_document_header >>patient >>>id mapped into XDS Affinity Domain patient id domain	ClinicalDocument >recordTarget >>patientRole >>>id mapped into XDS Affinity Domain patient id domain	Class: EHR_EXTRACT attribute: subject_of_care[1]: II mapped into XDS Affinity Domain patient id domain
serviceStartTime	levelone >clinical_document_header>>patient_encounter >>>encounter_tmr	ClinicalDocument >documentationOf >>event >>>effectiveTime low=	Class: CLINICAL_SESSION attribute: session_time[1]: IVL<TS>
serviceStopTime	levelone >clinical_document_header >>patient_encounter >>>encounter_tmr	ClinicalDocument >documentationOf >>event >>>effectiveTime high=	
classCode	Inferred from levelone >clinical_document_header >>document_type_cd RT= EX=	Inferred from ClinicalDocument >code codeSystem= code=	Class COMPOSITION Attribute: to be added.

Attribute	CDA R1-2000	CDA R2 Draft Aug 2004	EHRCOM

classCodeDisplayName	Inferred from
	levelone
	>clinical_document_header
	>>document_type_cd
	   DN=
		Inferred from
		ClinicalDocument
		>code
		  codeSystem=
		  code=	

practiceSettingCode	levelone
	>clinical_document_header
	>>patient_encounter
	>>>practice_setting_cd
	   V=
	   S=
		Inferred from
		ClinicalDocument
		>code
		  codeSystem=
		  code=
			(need input from CEN TC 251)

practiceSettingCodeDisplayName	levelone
	>clinical_document_header
	>>patient_encounter
	>>>practice_setting_cd
	   DN=
		Inferred from
		ClinicalDocument
		>code
		  codeSystem=
		  code=	

healthcareFacilityTypeCode	Inferred from
	levelone
	>clinical_document_header
	>>patient_encounter
	>>>practice_setting_cd
	   V=
	   S=
		Inferred from
		ClinicalDocument
		>code
		  codeSystem=
		  code=
			Class CLINICAL_SESSION
			attribute:
			healthcare_facility[0..1]: II

healthcareFacilityTypeCodeDisplayName	Inferred from
	levelone
	>clinical_document_header
	>>patient_encounter
	>>>practice_setting_cd
	   DN=
		Inferred from
		ClinicalDocument
		>code
		  codeSystem=
		  code=	

availabilityStatus	N/A	N/A	N/A

Attribute	CDA R1-2000	CDA R2 Draft Aug 2004	EHRCOM
	(Generated and maintained by the Registry)	(Generated and maintained by the Registry)	(Generated and maintained by the Registry)
uniqueId	levelone >clinical_document_header >>id	ClinicalDocument >id	Class RECORD_COMPONENT attribute: rc_id[1]: II

typeCode	levelone
	>clinical_document_header
	>>document_type_cd
	  RT=
	  EX=
		ClinicalDocument
		>code
		  codeSystem=
		  code=
			Class RECORD_COMPONENT
			attribute: meaning[0..1]: CV

typeCodeDisplay Name	levelone
	>clinical_document_header
	>>document_type_cd
	  DN=
		ClinicalDocument
		>code
		  displayName=	

formatCode		ClinicalDocument >typeId	Class EHR_EXTRACT attribute: rm_id[1]: String

eventCode	Inferred from
	levelone
	>clinical_document_header
	>>document_type_cd
	  RT=
	  EX=
		Inferred from
		ClinicalDocument
		>code
		  codeSystem=
		  code=
			(need input from CEN TC 251)

eventCodeDisplay Name	Inferred from
	levelone
	>clinical_document_header
	>>document_type_cd
	  RT=
	  EX=
		Inferred from
		ClinicalDocument
		>code
		  codeSystem=
		  code=
			(need input from CEN TC 251)

title	Inferred from levelone >clinical_document_header >>document_type_cd DN=	ClinicalDocument >title	Class: RECORD_COMPONENT attribute: name[1]: TEXT
authorInstitution	levelone >clinical_document_header >>originating_organization >>>organization	ClinicalDocument >author >>assignedAuthor >>>representedOrganization >>>>name	Class CLINICAL_SESSION attribute: healthcare_facility[0..1]: II

Attribute	CDA R1-2000	CDA R2 Draft Aug 2004	EHRCOM
authorPerson	levelone >clinical_document_header >>originator >>>person	ClinicalDocument >author >>assignedAuthor >>>assignedAuthorChoice >>>>person	Class: COMPOSITION attribute: composer[0..1]: II
legalAuthenticator	levelone >clinical_document_header >>legal_authenticator >>>person	ClinicalDocument >legalAuthenticator >>assignedEntity >>>person	Class FUNCTIONAL_ROLE (association from class ATTESTATION) attribute: performer[1]: II
URI	N/A	N/A	N/A
parentDocument Relationship	levelone >clinical_document_header >>document_relationship >>>document_relationship.type_cd	ClinicalDocument >relatedDocument typeCode=	IN THE CASE OF REPLACEMENT Class: AUDIT_INFO attribute: revision_status CS_REV_STAT IN THE CASE OF ADDENDUM or TRANSFORM Class LINK attribute nature: CV
parentDocumentId	levelone >clinical_document_header >>document_relationship >>>related_document >>>>id	ClinicalDocument >relatedDocument >>parentDocument >>>id	IN THE CASE OF REPLACEMENT attribute: previous_version[0..1]: II This attribute uniquely identifies the RECORD_COMPONENT of which the current RECORD_COMPONENT is a revision (null for the first ever version). IN THE CASE OF ADDENDUM or TRANSFORM Class LINK Attribute: target[1]: II

confidentialityCode	levelone
	>clinical_document_header
	>>confidentiality_cd
	  RT=
	  EX=
		ClinicalDocument
		>confidentialityCode
			Class RECORD_COMPONENT
			attribute: sensitivity[1]: CS_SENSITIVITY

languageCode	xml:lang attribute	ClinicalDocument >relatedDocument typeCode=	This attribute is a property of all text data types in CEN, and so we have not defined a separate overall language to govern the whole document. It might be reasonable to assume that the natural language used for the name attribute is considered to be a reasonable guide to the

Attribute	CDA R1-2000	CDA R2 Draft Aug 2004	EHRCOM
			value of this attribute.
patientId AssignBySource	levelone >clinical_document_header >>patient >>>person >>>>id	ClinicalDocument >recordTarget >>patientRole >>>id	Class: EHR_EXTRACT attribute: subject_of_care[1]: II
patientInfo AssignBySource	levelone >clinical_document_header >>patient >>>person >>>>person_name	ClinicalDocument >recordTarget >>patientRole >>>patientPatient >>>>name	
size	N/A Total length of submitted document.	N/A Total length of submitted document.	N/A Total length of submitted document.
hash	N/A Hash of submitted document.	N/A Hash of submitted document.	N/A Hash of submitted document.
entryUUID	N/A Generated by registry	N/A Generated by registry.	N/A Generated by registry.

Appendix M: Using Patient Demographics Query in a Multi-Domain Environment

10265 ## M.1: HL7 QBP^Q22 Conformance Model

The HL7 Find Candidates Query (QBP^Q22) defines a patient demographics query between a client application and an MPI system (HL7 V2.5, Page 3-64). This implies that the server maintains a master record of the patient demographics, but may know a number of patient identifiers from other domains.

In the QBP^Q22 Conformance Statement, QPD-8 (What Domains Returned) is defined as "the set of
10270 domains for which identifiers are returned in PID-3" (HL7 V2.5, Page 3-66, second table). Note that this field does not cite "demographics information in some domains", but about "identifiers issued in some domains", and explicitly specifies that these identifiers are returned in PID-3 (Patient ID List).

In the example following the Conformance Statement in HL7 2.5, three patient records are included in the query response; each returned patient record includes two identifiers in PID-3 (domains METRO
10275 HOSPITAL and SOUTH LAB) as requested in the query. However, one set of demographic information is returned in the remainder of the PID segment. The example does not illustrate or assume a mechanism for returning multiple sets of demographic information.

Thus it appears that QBP^Q22 is not intended to provide a way to issue a single query for patient demographics maintained in multiple different patient registration systems (domains).

10280 ## M.2: IHE PDQ Architecture

In the PDQ Integration Profile, the supplier is characterized as a Patient Demographics Supplier. The supplier is not assumed nor required to be an MPI system. It may be holding information from only a single patient identification domain, or may instead hold information from multiple identification domains.

10285 The latter case would apply if, for example, the Patient Demographics Supplier is grouped with an actor accepting ADT feeds from multiple patient registration systems in different domains. Equivalently, the Patient Demographics Supplier Actor (or some other Actor with which it is grouped) may manage a set of patient demographics sources, but is not expected to cross-reference them (as a PIX Actor or an MPI system). A conceptual model embracing both multi-domain concepts is shown in the following picture.

10290
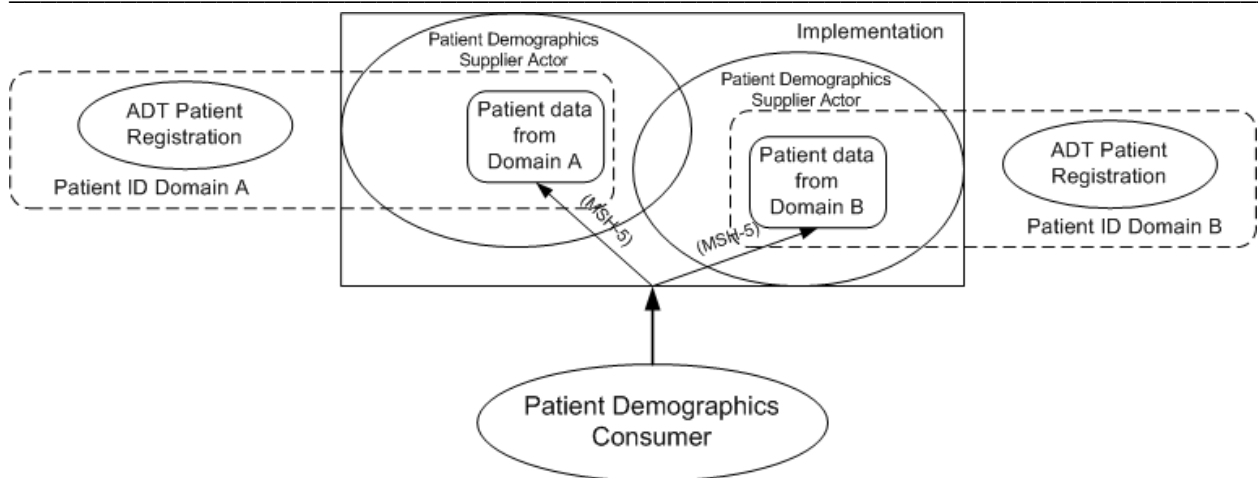
10295

Because of the definition of QBP^Q22, it must be determined which patient demographics source a QBP^Q22 query is asking for, before any processing of the query request can proceed. The identification of a need for such determination is the key difference between the IHE PDQ transactions and the original HL7 QBP^Q22 definitions.

10300   Three obvious alternatives exist for determining the patient demographics source.

3.   The supplier advertises different application entities for each of the patient demographics sources it manages. By addressing its query to a particular application entity in *MSH-5-Receiving Application*, the consumer explicitly selects a source it is asking for.

4.   The consumer is required to populate PID-3.4 in QPD-3 (Query Parameter) with the domain
10305   name administered by the corresponding source (patient identifier domain) it is asking for.

5.   The consumer includes in QPD-8 (What Domains Returned) the domain name of the corresponding patient information source it is asking for.

In selecting among these alternatives for the PDQ Profile, IHE-ITI took into account the need to constrain the current HL7 QBP^Q22 definition while maintaining the integrity of the HL7 standard
10310   query and at the same time to model the IHE PDQ Profile properly to satisfy its real-world purpose. Based on these considerations, alternative 1 is the best selection, although alternative 2 is acceptable. Alternative 3 is not acceptable because it violates the definition of QPD-8 that is stated in the HL7 Standard.

M.3:   Implementing PDQ in a multi-domain architecture

10315   There are three possible approaches in using PDQ in a multi-domain environment:

1.   Group the PDQ Patient Demographics Supplier Actor with a PIX Patient Identifier Cross-reference Manager Actor. This allows the use of QPD-8 to request *patient identifiers* from other domains to be returned in the demographics query response to the PDQ Patient Demographics Consumer.

10320   2.   Group the PDQ Patient Demographics Supplier Actor with a PIX Patient Identifier Cross-reference Consumer Actor. This allows the use of QPD-8 to request *patient identifiers* from

other domains to be returned in the demographics query response to the PDQ Patient Demographics Consumer.

3. Group the PDQ Patient Demographics Consumer Actor with a PIX Patient Identifier Cross-reference Consumer Actor. This obliges the Patient Demographics Consumer to use separate query requests to obtain patient demographics information (PDQ query) and patient identifiers from the domains in which it is interested (PIX query).

Approach 3 is not recommended if Approach 1 or 2 is feasible. To require the Patient Demographics Consumer to issue a separate PIX query increases complexity and might not be permissible in the actual implementation architecture.

When Approach 1 or 2 is implemented, QPD-8 may be used by the Patient Demographics Consumer to ask for patient identifiers from the single domain used to identify patients in the Affinity Domain.. The patient demographics information returned comes from the patient demographics source that is associated with *MSH-5-Receiving Application*; the patient demographics source may or may not be associated with the patient identifier domain.

In Approach 2, note that the PDQ Patient Demographics Supplier is grouped with the PIX Patient Identifier Cross-reference Consumer. This combined actor will use a PIX Query to satisfy the request of the client from additional patient identifiers and return them in PID-3.

_____

10340   **Appendix N: Common Data Types**

This section describes IHE constraints of commonly used HL7 data types.

N.1:   CX Data Type

CX: Extended Composite ID with check digit

SEQ	LEN	DT	Usage	CARD	TBL#	COMPONENT NAME
1	15	ST	R	[1..1]		ID Number
2	1	ST	O	[0..1]		Check Digit
3	3	ID	O	[0..1]	0061	Check Digit Scheme
4	227	HD	R	[1..1]	0363	Assigning Authority
5	5	ID	RE	[0..1]	0203	Identifier Type Code
6	227	HD	O	[0..1]		Assigning Facility
7	8	DT	O	[0..1]		Effective Date
8	8	DT	O	[0..1]		Expiration Date
9	705	CWE	O	[0..1]		Assigning Jurisdiction
10	705	CWE	O	[0..1]		Assigning Agency or Department

The constraints above particularly apply to the Patient Identifiers carried in the PID segment.

10345   The data type has been constrained because the IHE Framework regards the Assigning Authority and the Identifier Type Code as essential components.

A common value of the Identifier Type Code for a Patient Identifier assigned by the healthcare organization (PID-3) is "PI". Other values are defined in Table 0203 of HL7 2.5 section 2.A.3.5.

Example: `12345^^^Saint-John Hospital^PI`

10350   The Identifier Type Code for Patient Account Number (PID-18) is "AN".

N.2:   EI Data Type

EI: Entity Identifier

SEQ	LEN	DT	Usage	CARD	TBL#	COMPONENT NAME
1	16	ST	R	[1..1]		Entity Identifier
2	20	IS	C	[0..1]	0363	Namespace ID
3	199	ST	C	[0..1]		Universal ID
4	6	ID	C	[0..1]	0301	Universal ID Type

_____

Component 1 is required. Either component 2 or both components 3 and 4 are required. Components 2, 3 and 4 may be all present.

10355   The EI is appropriate for machine or software generated identifiers. The generated identifier goes in the first component. The remaining components, 2 through 4, are known as the assigning authority; they can also identify the machine/system responsible for generating the identifier in component 1.

Example 1: `AB12345^RiversideHospital`

Example 2: `AB12345^^1.2.840.45.67^ISO`

10360   Example 3: `AB12345^RiversideHospital^1.2.840.45.67^ISO`

IHE constrains the length of the first component to 16 characters. National extensions can extend this length up to a maximum of 199.

IHE recommends that Component 2, "Namespace ID," always be populated. Particularly when there are
10365   several concurrent assigning authorities within the healthcare enterprise, this Namespace ID will indicate which assigning authority provided the identifier in Component 1.

N.3:   HD Data Type

HD: Hierarchic designator

SEQ	LEN	DT	Usage	CARD	TBL#	COMPONENT NAME
1	20	IS	R	[1..1]	0300	Namespace ID
2	199	ST	C			Universal ID
3	6	ID	C		0301	Universal ID Type

This Integration Profile requires that a field of Data Type HD be populated with:

10370   • Either the first component "Namespace ID" alone, which in this case contains a local identifier of the object.

• Or with all three components, "Namespace ID" containing the name of the object, "Universal ID" containing its universal OID, and "Universal ID Type" containing the value **ISO**.

This data type is particularly used in this profile to identify facilities, applications and assigning
10375   authorities: sending and receiving applications, sending and receiving facilities, last update facility, assigning authority of an identifier, etc.

N.4:   PL data Type

PL: Person Location

SEQ	LEN	DT	Usage	CARD.	TBL#	COMPONENT NAME
1	20	IS	O	[0..1]	0302	Point of Care
2	20	IS	O	[0..1]	0303	Room
3	20	IS	O	[0..1]	0304	Bed

SEQ	LEN	DT	Usage	CARD.	TBL#	COMPONENT NAME
4	227	HD	O	[0..1]		Facility
5	20	IS	O	[0..1]	0306	Location Status
6	20	IS	C	[0..1]	0305	Person Location Type
7	20	IS	O	[0..1]	0307	Building
8	20	IS	O	[0..1]	0308	Floor
9	199	ST	O	[0..1]		Location Description
10	427	EI	O	[0..1]		Comprehensive Location Identifier
11	227	HD	O	[0..1]		Assigning Authority for Location

10380   Comments on some components:

Component 1: Point of Care (IS):

> HL7 definition: This component specifies the code for the point where patient care is administered. It is conditional on PL.6 Person Location Type (e.g., nursing unit or department or clinic). After floor, it is the most general patient location designation.

10385   HL7 user-defined table 0302 does not suggest any value. The codification of point of cares will be defined at the site level in acute care settings.

Component 4: Facility (HD):

> HL7 definition: This component is subject to site interpretation but generally describes the highest level physical designation of an institution, medical center or enterprise. It is the most general
10390   person location designation.

> The codification of facilities will be defined at the highest level, according to the context of use of the PAM profile (community affinity domain, acute care setting, ambulatory domain, etc.).

Component 6: Person Location Type (IS):

> HL7 definition: Person location type is the categorization of the person's location defined by
10395   facility, building, floor, point of care, room or bed. Although not a required field, when used, it may be the only populated field. It usually includes values such as nursing unit, department, clinic, SNF, physician's office. Refer to *User-defined Table 0305 - Person location type* for suggested values.

User-defined Table 0305 – Person location type

Value	Description	Comment
C	Clinic	
D	Department	
H	Home	
N	Nursing Unit	
O	Provider's Office	

Value	Description	Comment
P	Phone	
S	SNF	

10400   National extensions of this profile may further constrain on extend this table.

N.5: TS Data Type

TS: Time Stamp

SEQ	LEN	DT	Usage	CARD	TBL#	COMPONENT NAME
1	24	DTM	R	[1..1]		Time
2	1	ID	X	[0..0]	0529	Degree of Precision

The first subfield is required. It specifies a point in time.

Maximum length: 24.

10405   HL7 Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]][+/-ZZZZ]

Constrained format in this PAM profile: YYYY[MM[DD[HH[MM[SS]]]]][+/-ZZZZ]

The least precise date possible is YYYY (only the year).

The most precise date possible is YYYYMMDDHHMMSS (up to the second).

The time zone (+/-ZZZZ) is represented as +/-HHMM offset from Coordinated Universal Time (UTC),
10410   (formerly Greenwich Mean Time (GMT)), where +0000 or -0000 both represent UTC (without offset).

Note that if the time zone is not included, the time zone defaults to the local time zone of the sender.

The second subfield is deprecated in HL7 v2.5, therefore not supported by this PAM profile.

N.6: XPN Data Type

10415 XPN: Extended Person Name

SEQ	LEN	DT	USAGE	CARD	TBL#	COMPONENT NAME
1	194	FN	RE	[0..1]		Family Name
2	30	ST	O	[0..1]		Given Name
3	30	ST	O	[0..1]		Second and Further Given Names or Initials Thereof
4	20	ST	O	[0..1]		Suffix (e.g., JR or III)
5	20	ST	O	[0..1]		Prefix (e.g., DR)
6	6	IS	X	[0..0]	0360	Degree (e.g., MD)
7	1	ID	R	[1..1]	0200	Name Type Code
8	1	ID	O	[0..1]	0465	Name Representation Code
9	483	CE	O	[0..1]	0448	Name Context
10	53	DR	X	[0..0]		Name Validity Range
11	1	ID	O	[0..1]	0444	Name Assembly Order
12	26	TS	O	[0..1]		Effective Date
13	26	TS	O	[0..1]		Expiration Date
14	199	ST	O	[0..1]		Professional Suffix

This data type is usually in a repeatable field, to allow a list of names. Examples: Legal name, display name.

Subfield 1 "Family Name" is required if known to the sender.

Subfield 7 "Name Type Code" is required. The PAM profile allows these values from *HL7 Table 0200 –*
10420 *Name type:*

HL7 Table 0200 - Name type

Value	Description	Comment
A	Alias Name	
B	Name at Birth	
C	Adopted Name	
D	Display Name	
I	Licensing Name	

Value	Description	Comment
L	Legal Name	
M	Maiden Name	
N	Nickname /"Call me" Name/Street Name	
R	Registered Name (animals only)	
S	Coded Pseudo-Name to ensure anonymity	
T	Indigenous/Tribal/Community Name	
U	Unspecified	

This table may be further defined and restrained in national extensions of this profile.

Subfields 6 (Degree) and 10 (Name Validity Range) are deprecated in HL7 v2.5, therefore not supported by the PAM profile

10425

Appendix O: Intentionally Left Blank

Appendix P: Examples of messages

P.1: Example of transaction ITI-31: Admit for Surgical Procedure

10430   This example illustrates the use of ITI-31 with the following options:

- Inpatient/Outpatient Encounter Management
- Advanced Encounter Management
- Temporary Patient Transfer Track
- Historic Movement Management

10435   **P.1.1: Storyboard**

Robert LAW arrives from home to Saint-Louis Hospital. Operator Janine WHITE registers Robert in the administrative systems and creates a new account for billing. The reason of admission is a surgery of the heart, and Robert is under the responsibility of Cardiology. Before the surgery, a chest X-Ray and an electrocardiogram have to be performed. After the surgery, Robert is transferred to the Intensive Care

10440   Unit for 2 days. The transfer to the ICU is entered with two errors (wrong bed, wrong time). This transfer is corrected with the appropriate values. Then Robert is transferred back to Cardiology. Two weeks after admission, Robert is sent back home. Later on, his last movement in cardiology is corrected.

Objects	Attributes
Patient	Legal name: Robert LAW
	ID: 12345
	Sex: male
	Date of birth: October 2nd 1946
	Billing Account Number: 987654
Administrative Operator	Legal name: Janine WHITE, ID: 1001
	Legal name: Eva STRAW, ID: 1002
	Legal name: Betty GARDNER, ID: 1003
	Legal name: Jana BLACKMORE, ID: 1004
Assigning Facility	Saint-Louis Hospital
Attending Doctors	Legal name: Charles BROWN, ID: 2001
	Legal name: Ray JOHNSON, ID: 2002
Family Doctor	Legal name: Bob FAMILY, ID 7777
Medical Departments	Name: Cardiology, Code: 6043, Bed: 1, Room: 200
	Name: Cardiology, Code: 6043, Bed: 3, Room: 202
	Name: Radiology, Code: 5001
	Name: ICU, Code: 5050, Bed: 1, Room: 430

10445   **P.1.2: Interaction Diagram**

The following diagram illustrates the interactions used in this Example. The acknowledgement messages are not shown.

```
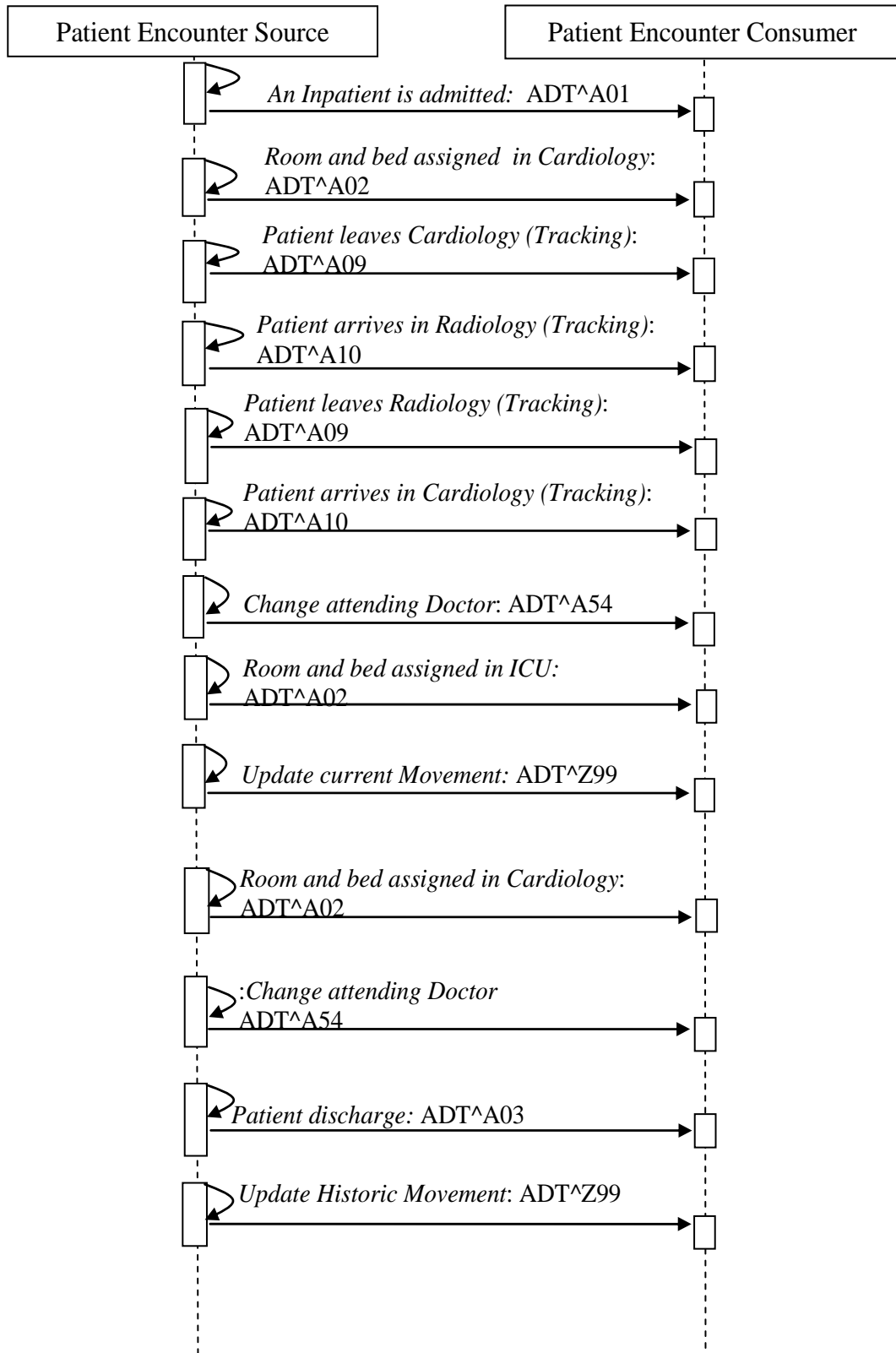        ┌────────────────────────────┐         ┌────────────────────────────┐
        │  Patient Encounter Source  │         │ Patient Encounter Consumer │
        └────────────────────────────┘         └────────────────────────────┘
                    │                                         │
        An Inpatient is admitted:  ADT^A01 ────────────────▶
                    │                                         │
        Room and bed assigned  in Cardiology:
        ADT^A02  ──────────────────────────────────────────▶
                    │                                         │
        Patient leaves Cardiology (Tracking):
        ADT^A09  ──────────────────────────────────────────▶
                    │                                         │
        Patient arrives in Radiology (Tracking):
        ADT^A10  ──────────────────────────────────────────▶
                    │                                         │
        Patient leaves Radiology (Tracking):
        ADT^A09  ──────────────────────────────────────────▶
                    │                                         │
        Patient arrives in Cardiology (Tracking):
        ADT^A10  ──────────────────────────────────────────▶
                    │                                         │
        Change attending Doctor: ADT^A54 ──────────────────▶
                    │                                         │
        Room and bed assigned in ICU:
        ADT^A02  ──────────────────────────────────────────▶
                    │                                         │
        Update current Movement: ADT^Z99 ──────────────────▶
                    │                                         │
        Room and bed assigned in Cardiology:
        ADT^A02  ──────────────────────────────────────────▶
                    │                                         │
        :Change attending Doctor
        ADT^A54  ──────────────────────────────────────────▶
                    │                                         │
        Patient discharge: ADT^A03 ────────────────────────▶
                    │                                         │
        Update Historic Movement: ADT^Z99 ─────────────────▶
                    │                                         │
```

_____

P.1.3: Messages

10450 Operator Janine White admits Robert Law as an Inpatient in the administrative system of Saint-Louis Hospital. She creates a new billing account number (987654). The attending doctor of Robert Law is Doctor Charles Brown, during Robert's stay in the Cardiology department.

```
10455   MSH|^~\&|?|Saint-Louis|?|Saint-
        Louis|20050530082015||ADT^A01^ADT_A01|000001|T|2.5|||||FRA|8859/15|EN
        EVN||20050530082000||||1001^WHITE^Janine|20050530082000
        PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
        987654^^^Saint-Louis^AN
        ROL||AD|FHCP|7777^FAMILY^Bob
10460   PV1|1|I||||||2001^BROWN^Charles
        ZBE|mvt1|20050530082000||INSERT|N
```

Robert LAW arrives in Cardiology and a secretary (Eva STRAW) validates the arrival by assigning a room and a bed to the Patient. Had the bed been assigned at admission time, the patient location would 10465 have been part of the ADT^A01 message.

```
        MSH|^~\&|?|Saint-Louis|?|Saint-
        Louis|20050530082015||ADT^A02^ADT_A02|000001|T|2.5|||||FRA|8859/15|EN
        EVN||20050530082500||||1002^STRAW^Eva|20050530082500
10470   PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
        987654^^^Saint-Louis^AN
        PV1|1|I||6043^200^1^Saint-Louis
        ZBE|mvt2|20050530082500||INSERT|N
```

10475 The electrocardiogram is performed in the Cardiology department. However, Robert needs to be transferred to Radiology for the chest X-Ray. This move to a temporary location is tracked by two messages: A09 when departing the cardiology, A10 when arrived in Radiology. These tracking events are not Movements, and don't use the ZBE segment.

```
10480   MSH|^~\&|?|Saint-Louis|?|Saint-
        Louis|20050530082015||ADT^A09^ADT_A09|000001|T|2.5|||||FRA|8859/15|EN
        EVN||20050530123000|||1002^STRAW^Eva|20050530122500
        PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
        987654^^^Saint-Louis^AN
10485   PV1|1|I|||||6043^200^1^Saint-Louis|||||5001^^^Saint-Louis
```

```
        MSH|^~\&| ?|Saint-Louis| ?|Saint-
        Louis|20050530082015||ADT^A10^ADT_A09|000001|T|2.5|||||FRA|8859/15|EN
        EVN||20050530123000|||1003^GARDNER^Betty|20050530123000
10490   PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
        987654^^^Saint-Louis^AN
        PV1|1|I|||||6043^200^1^Saint-Louis|||||5001^^^Saint-Louis
```

When the X-Ray is performed, Robert leaves the Radiology department and comes back to Cardiology. 10495 Two other movement-tracking messages are generated.

10500
```
MSH|^~\&|?|Saint-Louis|?|Saint-
Louis|20050530082015||ADT^A09^ADT_A09|000001|T|2.5|||||FRA|8859/15|EN
EVN||20050530123000|||1002^STRAW^Eva|20050530125000
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
PV1|1|I|6043^200^1^Saint-Louis|||||||||||||||||||||||||||||||||||||||||||||||||
|5001^^^Saint-Louis
```

10505
```
MSH|^~\&|?|Saint-Louis|?|Saint-
Louis|20050530082015||ADT^A10^ADT_A09|000001|T|2.5|||||FRA|8859/15|EN
EVN||20050530123000|||1002^STRAW^Eva|20050530125500
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
PV1|1|I|6043^200^1^Saint-Louis|||||||||||||||||||||||||||||||||||||||||||||||
```
10510
```
|5001^^^Saint-Louis
```

The surgery is planned for the next day. When the surgery is completed, Robert LAW is transferred to
the Intensive Care Unit for 2 days. Ray JOHNSON is the new attending physician during these 2 days.

10515
```
MSH|^~\&|?|Saint-Louis|?|Saint-
Louis|20050530082015||ADT^A54^ADT_A54|000001|T|2.5|||||FRA|8859/15|EN
EVN||20050531114000|||1002^STRAW^Eva|20050531114000
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
PV1|1|I|||||2002^JOHNSON^Ray
ZBE|mvt3|20050531114000||INSERT|N
```

10520 When Robert LAW arrives in ICU, a secretary (Jana BLACKMORE) validates the arrival by assigning a
room and a bed. She makes two typing mistakes (wrong bed, wrong time)

10525
```
MSH|^~\&|?|Saint-Louis|?|Saint-
Louis|20050530082015||ADT^A02^ADT_A02|000001|T|2.5|||||FRA|8859/15|EN
EVN||20050531114400|||1004^BLACKMORE^Jana|20050531114400
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
PV1|1|I|5050^430^11^Saint-Louis|||6043^200^1^Saint-Louis
ZBE|mvt4|20050531114400||INSERT|N
```

After Robert LAW is moved to his new bed, Jana B BLACKMORE corrects the two mistyping in the
10530 movement.

10535
```
MSH|^~\&|?|Saint-Louis|?|Saint-
Louis|20050530082015||ADT^Z99^ADT_A01|000001|T|2.5|||||FRA|8859/15|EN
EVN||20050531114400|||1004^BLACKMORE^Jana|20050531115800
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
PV1|1|I|5050^430^1^Saint-Louis|||6043^200^1^Saint-Louis
ZBE|mvt4|20050531104400||UPDATE|N|A02
```

10540   After 2 days, Robert LAW leaves the ICU and comes back to Cardiology. A new room and bed are
assigned to the Patient.

```
MSH|^~\&|?|Saint-Louis|?|Saint-
Louis|20050530082015||ADT^A02^ADT_A02|000001|T|2.5|||||FRA|8859/15|EN
EVN||20050601161200|||1002^STRAW^Eva|20050601161200
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
PV1|1|I|6043^202^2^Saint-Louis|||5050^430^1^Saint-Louis
ZBE|mvt5|20050601161200||INSERT|N
```

10550

```
MSH|^~\&| ?|Saint-Louis| ?|Saint-
Louis|20050530082015||ADT^A54^ADT_A54|000001|T|2.5|||||FRA|8859/15|EN
EVN||20050601161000|||1004^BLACKMORE^Jana|20050601161200
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
PV1|1|I||||||2001^BROWN^Charles
ZBE|mvt6|20050601161200||INSERT|N
```

After 12 days, Robert LAW is discharged and sent back home.

10560
```
MSH|^~\&|?|Saint-Louis|?|Saint-
Louis|20050530082015||ADT^A03^ADT_A03|000001|T|2.5|||||FRA|8859/15|EN
EVN||20050613180000|||1001^WHITE^Janine|20050613180000
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
PV1|1|I|6043^200^1^Saint-Louis|||||||||||||||||||||||||||||||||||||1
ZBE|mvt7|20050613180000||INSERT|N
```
10565

One hour later the Cardiology corrects an error of both time and bed in the last patient assigned location
in cardiology, triggering an update of the Historic Movement identified as mvt5:

10570
```
MSH|^~\&|?|Saint-Louis|?|Saint-
Louis|20050530082015||ADT^Z99^ADT_A01|000001|T|2.5|||||FRA|8859/15|EN
EVN||20050601161200|||1002^STRAW^Eva|20050613190000
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
PV1|1|I|6043^202^3^Saint-Louis|||5050^430^1^Saint-Louis
ZBE|mvt5|20050601161233||UPDATE|Y|A02
```
10575

P.2:   Example of transaction ITI-31: Admit and cancel admit

This example uses transaction ITI-31 without any option, to illustrate a cancellation message:

P.2.1: Storyboard

10580   Operator Janine WHITE registers an admission for patient Robert LAW in the administrative system of
Saint-Louis Hospital. After a while it turns out that the patient has been directed to the wrong hospital.
The patient is redirected to another hospital and the admission is cancelled.

Objects	Attributes
Patient	Legal name: Robert LAW
	ID: 12345
	Sex: male
	Date of birth: October 2nd 1946
	Billing Account Number: 987654
Administrative Operator	Legal name: Janine WHITE, ID: 1001
Assigning Facility	Saint-Louis Hospital
Attending Doctors	Legal name: Charles BROWN, ID: 2001
	Legal name: Ray JOHNSON, ID: 2002
Family Doctor	Legal name: Bob FAMILY, ID 7777

10585 P.2.2: Interaction Diagram

The following diagram illustrates the interactions used in this Example. The acknowledgement messages are not shown.

P.2.3: Messages

10590 Operator Janine White admits Robert Law as an Inpatient in the administrative system of Saint-Louis Hospital. She creates a new billing account number (987654). The attending doctor of Robert Law is Doctor Charles Brown.

```
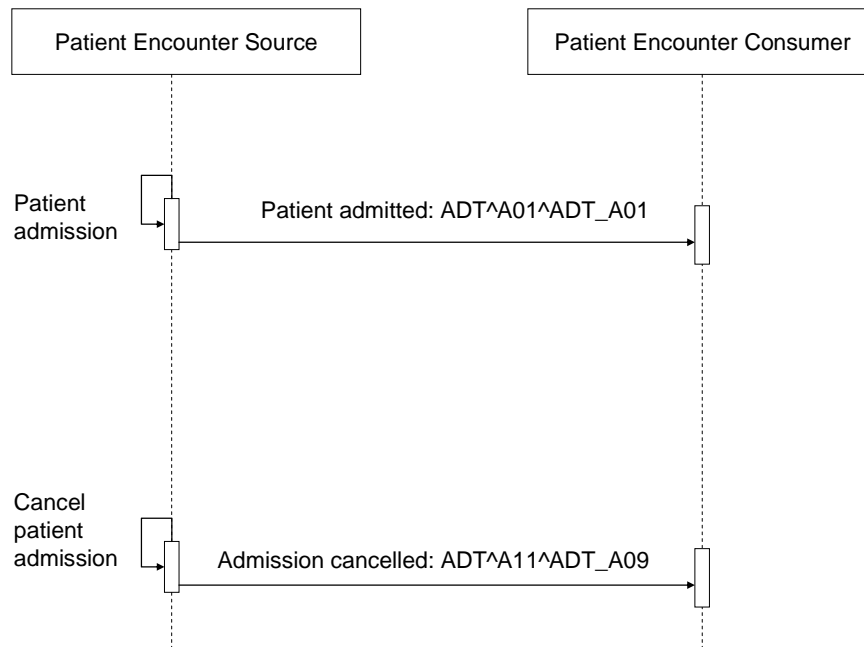MSH|^~\&|?|Saint-Louis|?|Saint-
Louis|20050530082015||ADT^A01^ADT_A01|000001|T|2.5|||||FRA|8859/15|EN
```

```
EVN||20050530082000|||1001^WHITE^Janine|20050530082000
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
ROL||AD|FHCP|7777^FAMILY^Bob
PV1|1|I||||||2001^BROWN^Charles
ZBE|mvt1|20050530082000||INSERT|N
OBX||NM|3142-7^BODY WEIGHT (STATED)^LN||62|kg|||||F
OBX||NM|8303-0^BODY HEIGHT^LN||1.70|m|||||F
```

10600

10605 The patient is redirected afterwards to another hospital. Janine White cancels the admission.

```
MSH|^~\&|?|Saint-Louis|?|Saint-
Louis|20050530084400||ADT^A11^ADT_A09|000001|T|2.5|||||FRA|8859/15|EN
EVN||20050530084350|||1001^WHITE^Janine|20050530082000
PID|1||12345^^^Saint-Louis^PI||LAW^Robert^^^^^L|||M|||||||||||
987654^^^Saint-Louis^AN
PV1|1|I||||||2001^BROWN^Charles
ZBE|mvt1|20050530082000||CANCEL|N
```

10610

10615 **Appendix Q: Intentionally Left Blank**

_____

Appendix R: Intentionally Left Blank

Appendix S: Intentionally Left Blank

10620

Appendix T: Use of eMail (Informative)

The off-line mode protocol uses the classical email exchange, based on SMTP server(s) as well as a POP3 server storing the recipient mailbox. The different steps of the exchange are described below, depending on the success or failure status of the exchange. The mechanism may be similar and use the evolution of these protocols (ESMTP, EMAP4). The Document Source and the Document Recipient shall at least support SMTP and POP3, but they may also support ESMTP and EMAP or similar. The example may also apply for a Document Repository when the off-line protocol binding is used.

10625

In case the message cannot reach the Document Recipient POP3 server, the diagram is the following:
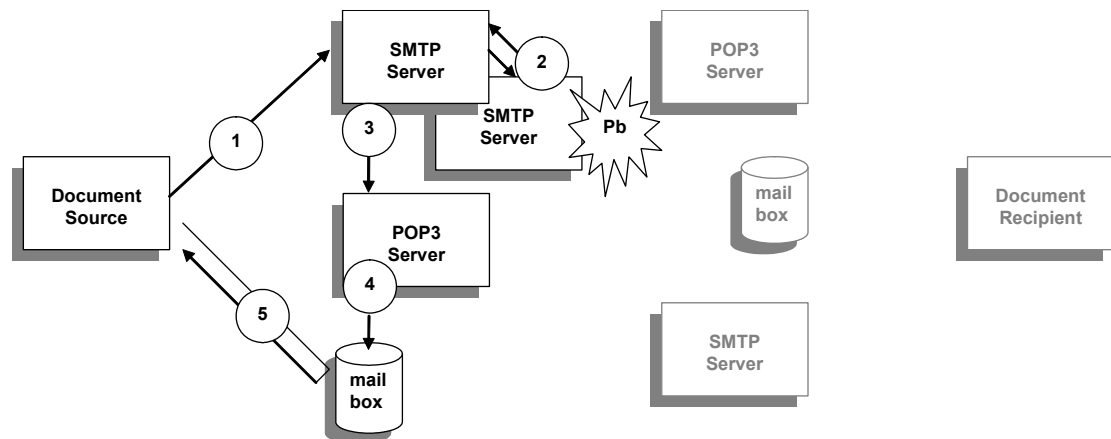
10630   **Figure T-1: Exchange diagram when the message is sent with error**

Where the steps are:

1. Initial message sent by the Document Source to its SMTP server

2. Transfer of this message to the Document Recipient POP3 server, potentially through a number of other SMTP servers acting as relays, but with a problem arising (which could be also at the POP3 Server level as "user email unknown" or "over quota exceeded in the destination mailbox"). An error message "Delivery Status Notification" (DSN) is generated by the server where the problem occurs, and sent back to the sender (using its "reply to" address if present, its "from" address otherwise)

10635

3. Reception of the negative DSN message by the Document Source POP3 server

10640

4. Store of the received message by the POP3 server in the mail box dedicated to the Document Source

5. Query and retrieve of the message by the Document Source from its mailbox (and normally deletion of this message).

In case the message reaches the Document Recipient POP3 server, the diagram is the following:
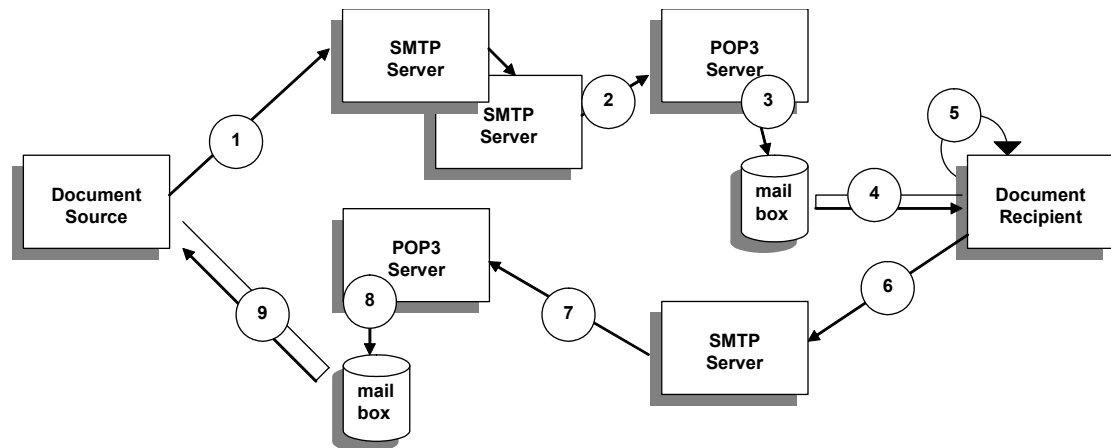
10645

Figure T-2 Exchange diagram when the message is successfully sent

Where the steps are:

1. Initial message sent by the Document Source to its SMTP server

2. Transfer of this message to the Document Recipient POP3 server, potentially through a number
10650   of other SMTP servers acting as relays

3. Store of the received message by the POP3 server in the mail box dedicated to the Document
   Recipient

4. Query and retrieve of the message by the Document Recipient from its mailbox (and normally
   deletion of this message).

10655   5. Local confirmation of the success (or failure) when it "processes" the message inside the
   Document Recipient (which could be that the user has read the message or at least that it has
   been correctly imported in the EHR)

6. Generation by the Document Recipient of a "Message Delivery Notification" message, that can
   be positive (respectively negative with the status)

10660   7. Reception of the positive MDN message by the Document Source POP3 server

8. Store of the received message by the POP3 server in the mailbox dedicated to the Document
   Source

9. Query and retrieve of the message by the Document Source from its mailbox (and normally
   deletion of this message).
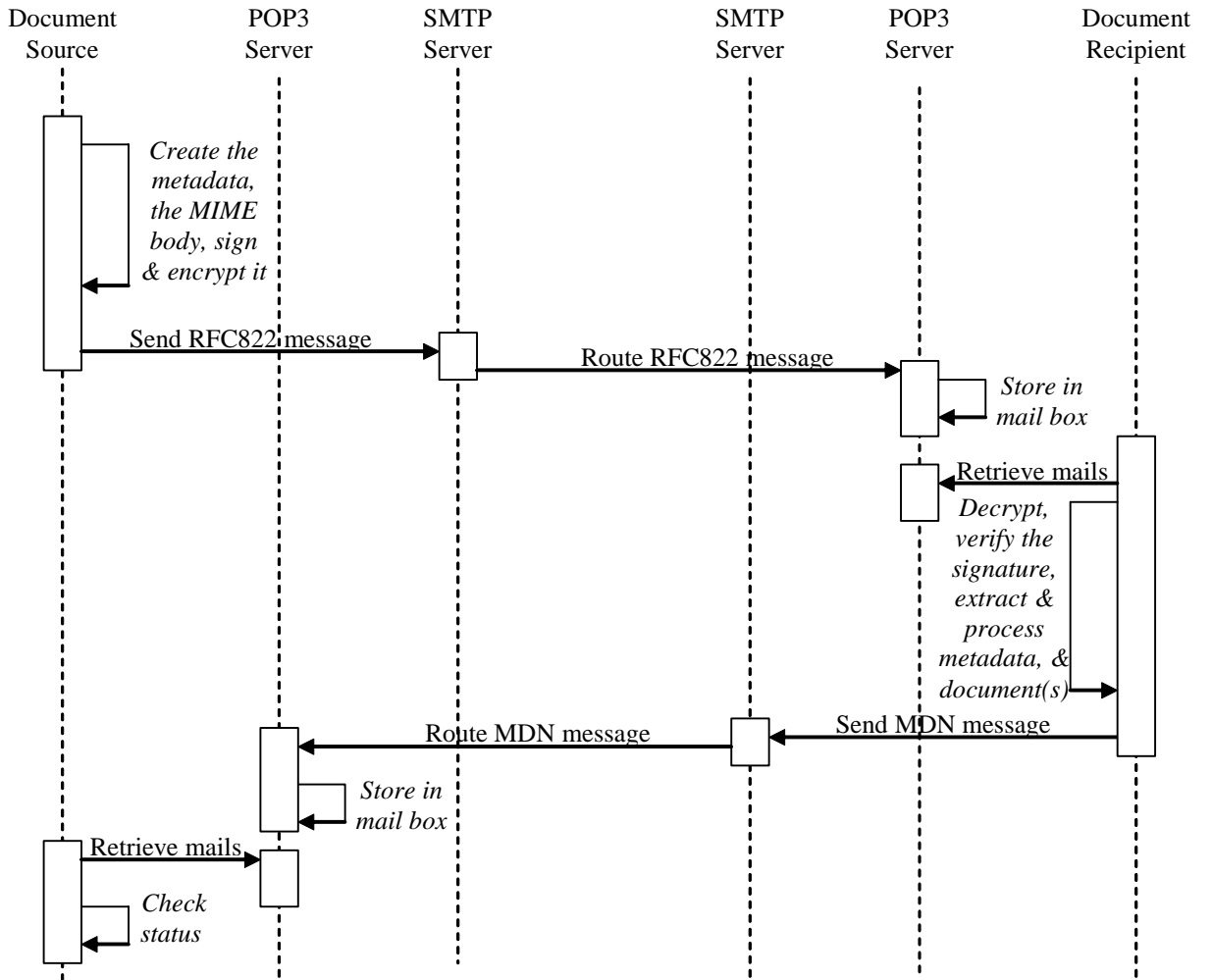
10665

Figure T-3 Sequence diagram of a secured message exchange

Appendix U: Intentionally Left Blank

10670

Appendix V: Web Services for IHE Transactions

V.1: Introduction

"Web Services" has become a catch-all phrase describing a wide range of HTTP transactions over a TCP/IP network. A more precise definition of Web Services implies richer infrastructure capabilities
10675 with all transactions built using SOAP messages. This appendix provides the guidelines for specifying the use of SOAP-based Web Services as the messaging infrastructure and transport mechanism for IHE transactions.

V.2: Relevant Standards

Virtually all web services specifications are developed under the auspices of the World Wide Web
10680 Consortium (W3C) or the Organization for the Advancement of Structured Information Standards (OASIS). The Web Services-Interoperability organization (WS-I) publishes profiles, which incorporate several existing standards, and constrain them for interoperability. For each profile, WS-I also publishes a test assertion document and corresponding interoperability testing tools for Java and C#.

V.2.1: WS-I Profiles

10685 Even though the Web Services for IHE transactions will be based on SOAP 1.2, they will take advantage of the guidelines expressed in the WS-I Basic Profile 1.1 (BP 1.1) and Simple SOAP Binding Profile 1.0 (SSBP 1.0) where applicable. Some IHE transaction may also take advantage of the WS-I Basic Security Profile 1.0 (BSP 1.0).

V.2.2: WS-* Specifications

10690 In addition to the requirements of the current WS-I profiles, the Web Services for IHE transactions will support the following Web Services standards:

- WS-Addressing
- MTOM
- XOP
10695 - WS-Security

WS-I have started workgroups on defining profiles combining several of the above WS-* standards, as well as including:

- WS-SecureConversation
- WS-Trust
10700 - WS-Policy
- WS-ReliableMessaging

In the future, the Web Services for IHE transactions will consider support for these new WS-I profiles, or particular WS-* standards as needed by specific use cases.

V.2.3: HL7 Web Services Profile

10705 The HL7 Web Services Profile provides a framework for using Web Services as the transport mechanism for HL7 V3 messages. The framework provides a layered approach to specifying Web Services requirements. IHE will use the same approach as a guideline when specifying Web Services transport for IHE transactions and will do its best to maintain this consistency over time.

V.2.4: XML Namespaces

10710 Table V.2.4-1 lists XML namespaces that are used in this appendix. The choice of any namespace prefix is arbitrary and not semantically significant.

Table V.2.4-1 XML Namespaces and Prefixes

Prefix	Namespace	Specification
wsdl (or default)	http://schemas.xmlsoap.org/wsdl/	WSDL 1.1 binding for SOAP 1.1 WSDL 1.1 binding for SOAP 1.2
wsoap12	http://schemas.xmlsoap.org/wsdl/soap12/	WSDL 1.1 binding for SOAP 1.2
wsoap11	http://schemas.xmlsoap.org/wsdl/soap/	WSDL 1.1 binding for SOAP 1.1
wsoap	Either wsoap11 or wsoap12, depending on context	
wsa	http://www.w3.org/2005/08/addressing	WSA 1.0 - Core
wsaw	http://www.w3.org/2006/05/addressing/wsdl	WSA 1.0 - WSDL binding*
soap12	http://www.w3.org/2003/05/soap-envelope	SOAP 1.2
soap11	http://schemas.xmlsoap.org/soap/envelope/	SOAP 1.1
soap	Either soap11 or soap12 depending on context	
Hl7	urn:hl7-org:v3	HL7 V3 XML ITS
xsd	http://www.w3.org/2001/XMLSchema	XML Schema
xsi	http://www.w3.org/2001/XMLSchema-instance	XML Schema

10715 *While this specification only advanced to W3C Candidate Recommendation status, the "Web services Addressing 1.0 – WSDL Binding" is already implemented in various software development platforms and therefore it is used in the trial implementation version. It is also the version published in the W3C Web Services Addressing 1.0 Test Suite. When the forthcoming replacement specification, Web Services Addressing 1.0 - Metadata, is available and implemented in common software development platforms it will be used in the final text of this Appendix.

V.3: Web Services Requirements

10720 The requirements in this section represent guidance for IHE Technical Framework authors who need to use web services in specific transactions. These requirements fall into two categories:

1. Providing consistency and clarity in the IHE specifications.

2. Affecting the wire format of the transactions.

Note: When the requirements for particular text are specified, the following notation is used:

10725
- curly braces (i.e. {}) are used to denote a part of a string which shall always be replaced with a string corresponding to the specific transaction, actor, or profile;
- square brackets (i.e. []) are used t o denote a part of a string which shall be either replaced with a string corresponding to the specific transaction, or shall be completely omitted.

V.3.1: Requirements for Transactions using HL7 V3 Messages

10730 When IHE transactions use HL7 V3 Messages, the Web Services protocol will conform to the HL7 Web Services Basic, Addressing, Security, and Reliable Messaging Profiles, with additional constraints as specified in the following sub-sections.

V.3.1.1: HL7 WS Basic Profile Constraints

The Sender and Receiver shall conform to the HL7 WS Basic Profile with four modifications. The first
10735 modification is the requirement of supporting SOAP 1.2, while the HL7 WS Basic Profile provides the choice of supporting either SOAP 1.1 or SOAP 1.2, or both.

The second modification is to HL7-WSP200, which recommends that a WSDL document describes a specific HL7 application role. For consistency with non-HL7 V3 transactions, IHE specifications shall provide an example WSDL document for all transactions of an actor per profile (see IHE-WSP200).

10740 The third modification is to HL7-WSP201, which recommends that the HL7 Application Role ID is to be used as the name of the WSDL definition. For consistency with non-HL7 V3 transactions the name of the example WSDL definition provided in the IHE specification shall be the actor name of the transaction's receiver (see the IHE-WSP201).

The fourth modification is to HL7-WSP202, which specifies the use of the HL7 namespace as the target
10745 namespace of the WSDL document. This would prevent creating a single WSDL for actors which use both HL7 V3 and non-HL7 V3 IHE transactions (e.g. an XDS registry implementing the XDS.b profile with the Patient Identity Feed HL7 V3 transaction). For consistency among all IHE transactions, when creating an IHE transaction specification, the WSDL target namespace shall be specified as "urn:ihe:<committee name>:<profile>:<year> (see IHE-WSP202).

10750 ### V.3.1.2: HL7 WS Addressing Profile Constraints

The Sender and Receiver should conform to the HL7 WS Addressing Profile. No additional constraints are made in this sub-section.

V.3.1.3: HL7 WS Security Profile Constraints

IHE does not specify whether the Sender and Receiver should implement the HL7 WS Security Profile.
10755 The decision to implement the HL7 WS Security Profile is left to implementers. Each IHE transaction specifies its ATNA requirements for security and authentication. Security profiles such as Cross-Enterprise User Assertion (XUA) contain further security requirements. With the publication of WS-Security 1.1 and when the WS-I Basic Security Profile 1.1 is released, it is expected that ATNA (or a different profile) may incorporate additional options for Web Services, and the HL7 WS Security Profile
10760 will be incorporated in this appendix.

V.3.1.4: HL7 WS Reliable Messaging Profile Constraints

IHE does not specify whether the Sender and Receiver should implement the HL7 WS Reliable
Messaging Profile. The decision to implement the HL7 WS Reliable Messaging Profile is left to
implementers. When the WS-I Reliable Secure Profile Working Group releases a profile it is expected
10765   that additional options for Web Services may be added, and the HL7 WS Reliable Messaging Profile
will be incorporated in this appendix.

V.3.2: Requirements for Transactions which don't use HL7 V3 Messages

The following IHE web services requirements are derived from the HL7 Web Services profile. This
provides consistency among the IHE transactions, compatibility to existing Web Services
10770   implementations through the WS-I profiles, and a well-defined mechanism for adding additional layers
of web services in the future. The HL7 Web Services profile also provides detailed background
regarding the requirements presented here.

The numbering scheme for the individual requirements uses the following convention:

   • IHE-WS[P|A|S|RM]nnn[.e]) text

10775   P, A, S, and RM represent the Basic, Addressing, Security, and Reliable Messaging requirements
sections in this specification, nnn represents a unique number for this specification, and text is the text of
the requirement. This directly corresponds to the convention used in the HL7 Web Services profile, and
for easier navigation, the same numbers correspond to the equivalent requirements in both
specifications. Note that not all implementation decisions from the HL7 Web Services profile are
10780   relevant for non-HL7 web services transactions. If there are cases where an IHE Web Services
requirement exists that does not correspond to an implementation decision from the HL7 Web Services
Profile, the optional extension to the number (shown as .e above) can be used to eliminate the possibility
of confusion.

Requirement Identifier	Requirement text	SOAP message format affected?
IHE-WSP200	Example WSDL documents shall implement a specific IHE Actor within a specific IHE Integration Profile.	No
IHE-WSP201	The attribute /wsdl:definitions/@name in the example WSDL document provided with an IHE specification shall be the name of the IHE Actor actor providing the service.	No
IHE-WSP202	The targetNamespace of the example WSDL shall be urn:ihe:{committee}:{profile}:{year}	No
IHE-WSP203	The example WSDL shall include XML Schema Definition references for the transactions payloads.	No
IHE-WSP205	Two WSDL messages shall be defined for a request-response transaction.	No
IHE-WSP206	In the example WSDL provided by an IHE specification a single WSDL part named Body shall be defined for each WSDL message and the part type shall refer to an element defined in the Schema Definition required in IHE-WSP203.	Determines the format of the SOAP Body
IHE_WSP207	For each input and output message defined in the WSDL portType operation an attribute wsaw:Action SHALL be included.	No
IHE_WSP208	WSDL operations SHALL use **wsdl:operation/wsdl:input/@wsaw:Action = "urn:ihe:{committee}:{Year}:{Transaction**	Determines the SOAP header content for wsa:Action

	name}[Operation]" and **wsdl:operation/wsdl:output/@wsaw:Action = "urn:ihe:{committee}:{Year}:{Transaction name}[Operation]Response"**	
IHE_WSP211	For each operation defined in the WSDL portType a wsoap:operation/@soapAction attribute shall be provided. The value of wsoap:operation/@soapAction shall be consistent with the name for the corresponding WSDL operation defined in the WSDL portType (see IHE-WSP207 and IHE-WSP208)	Determines the value of soapAction
IHE_WSP212	The example WSDL provided with an IHE specification shall use the SOAP Binding described in WSDL 1.1 Chapter 3 and the binding extension for SOAP 1.2.	No
IHE_WSP215	IHE transactions referencing the standards specified by Appendix V shall support SOAP 1.2, unless otherwise noted in the transaction. The example WSDL document provided with an IHE specification shall contain a SOAP 1.2 binding unless the transaction specifically notes that SOAP 1.2 is not supported.	Determines the namespace of the SOAP message
IHE_WSP216	For transactions which require SOAP 1.1 (contrary to the default SOAP 1.2) the WSDL shall contain a SOAP 1.1 binding. If the example WSDL document provided with an IHE specification contains a SOAP 1.1 binding, it shall use the SOAP Binding described in WSDL 1.1 Chapter 3.	Determines the namespace of the SOAP message
IHE_WSP300	SOAP messages and WSDL documents shall conform to the WS-I Basic Profile 1.1 (within the requirements for IHE-WSP215).	Yes
IHE_WSA100	The example WSDL provided with IHE transactions shall use the WS-Addressing framework when specifying the Web Services protocol.	Determines the WSA content for the SOAP header
IHE_WSA101	All `<wsa:Action>` elements shall have the mustUnderstand attribute set (`mustUnderstand="1"`)	Ensures that web services frameworks are configured to properly generate and process WS-Addressing headers
IHE_WSA102	The `<wsa:ReplyTo>` element of the initiating message shall be present and shall have the mustUnderstand attribute set (`mustUnderstand="1"`)	Ensures that responses are routed to the appropriate web services end point, or as an immediate response

10785

V.3.2.1: Basic Requirements

V.3.2.1.1. Naming conventions and namespaces

IHE-WSP200) Example WSDL documents shall implement a specific IHE Actor within a specific IHE Integration Profile.

10790   This editorial requirement means that if several IHE actors within a profile are combined, then separate WSDL documents for each actor need to be provided. This only applies to actors, which provide a particular service, i.e. the receivers in an IHE transaction.

___

IHE-WSP201) The attribute /wsdl:definitions/@name in the example WSDL document provided with
an IHE specification shall be the IHE Actor Name of the actor providing the service.

10795 The suggested nomenclature for WSDL artifacts is represented in the following table. NAME is the
value of the /wsdl:definitions/@name attribute which will be specified for each transaction.

WSDL Artifact	Proposed Naming
message	{Transaction Name}_Message
portType	{NAME}_PortType
Operation	{NAME}_{Transaction Name}[_OperationID]
SOAP 1.1 binding	{NAME}_Binding_Soap11
SOAP 1.1 port	{NAME}_Port_Soap11
SOAP 1.2 binding	{NAME}_Binding_Soap12
SOAP 1.2 port	{NAME}_Port_Soap12

Here is an example of how the nomenclature can be applied:

```
For wsdl:definitions/@name="XDSRegistry":

    message          -> "StoredQuery_Message"
    portType         -> "XDSRegistry_PortType"
    operation        -> "XDSRegistry_StoredQuery_Request"
    SOAP 1.2 binding -> "XDSRegistry_Binding_Soap12"
    SOAP 1.2 port    -> "XDSRegistry_Port_Soap12"
    SOAP 1.1 binding -> "XDSRegistry_Binding_Soap11"
    SOAP 1.1 port    -> "XDSRegistry_Port_Soap11"
```

10800

10805

IHE-WSP202) The targetNamespace of the example WSDL shall be
urn:ihe:{committee}:{profile}:{year}

This requirement excludes the optional {type} that can be added to the end of the namespace. Other IHE
specifications which use XML namespaces can add this optional part to the URN. As an example the
10810 namespace for the XDS.b Integration Profile is urn:ihe:iti:xds-b:2007.

IHE-WSP203) The example WSDL shall include XML Schema Definition references for the
transactions payloads.

The purpose of this requirement is to specify how authors of IHE profiles specify the transactions which
use web services. This requires both the existence of an XML schema definition for the transaction
10815 payloads, and the manner in which it is specified in the WSDL file – by reference.

V.3.2.1.2: Message and portType Definitions

IHE-WSP205) Two WSDL messages shall be defined for a request-response transaction.

IHE-WSP206) In the example WSDL provided by an IHE specification a single WSDL part named
Body shall be defined for each WSDL message and the part type shall refer to an element defined in the
10820 Schema Definition required in IHE-WSP203.

IHE-WSP207) For each input and output message defined in the WSDL portType operation an attribute
wsaw:Action SHALL be included.

For compatibility with the Addressing requirements and consistency with naming across IHE Web Services implementations, the wsaw:Action attribute for each WSDL input and output message must be defined.

The wsaw:Action attribute shall be ignored by Web Services implementations that do not support WS-Addressing. It is very important to have the attribute in mixed cases where just one of the endpoints might support the WS-Addressing specification to avoid communication or routing errors.

IHE-WSP208) WSDL operations SHALL use **wsdl:operation/wsdl:input/@wsaw:Action = "urn:ihe:{committee}:{Year}:{Transaction name}[Operation]" and wsdl:operation/wsdl:output/@wsaw:Action = "urn:ihe:{committee}:{Year}:{Transaction name}[Operation]Response"**

For example, the wsaw:Action value for the Stored Query transaction is specified as "urn:ihe:iti:2007:StoredQuery" and "urn:ihe:iti:2007:StoredQueryResponse".

The optional [Operation] component is used when the same message in the same transaction is used in different operations, and requires a different response. An example of that are the two operations that can be achieved using the HL7 V3 Query Continuation message: query continuation, and query cancel (which are handled via the HL7 WS Profile rules).

V.3.2.1.3: Binding

Multiple WSDL bindings can be defined in order to support different protocols and transports. The naming is consistent with the naming rules specified in the previous section.

IHE-WSP211) For each operation defined in the WSDL portType a wsoap:operation/@soapAction attribute shall be provided. The value of wsoap:operation/@soapAction shall be consistent with the name for the corresponding WSDL operation defined in the WSDL portType (see IHE-WSP207 and IHE-WSP208)

IHE-WSP212) The example WSDL provided with an IHE specification shall use the SOAP Binding described in WSDL 1.1 Chapter 3 and the binding extension for SOAP 1.2.

IHE-WSP215) IHE transactions referencing the standards specified by Appendix V shall support SOAP 1.2, unless otherwise noted in the transaction. The example WSDL document provided with an IHE specification shall contain a SOAP 1.2 binding unless the transaction specifically notes that SOAP 1.2 is not supported.

SOAP 1.2 is the base standard for several WS specification, and has many available and easily accessible implementations.

IHE-WSP216) For transactions which require SOAP 1.1 (contrary to the default SOAP 1.2) the WSDL shall contain a SOAP 1.1 binding. If the example WSDL document provided with an IHE specification contains a SOAP 1.1 binding, it shall use the SOAP Binding described in WSDL 1.1 Chapter 3.

A SOAP 1.1 binding can be useful for backwards compatibility.

IHE-WSP300) SOAP messages and WSDL documents shall conform to the WS-I Basic Profile 1.1 (within the requirements for IHE-WSP215).

Example 1: Example WSDL File with an Non-HL7 Transaction
```
<definitions xmlns:wsoap11="http://schemas.xmlsoap.org/wsdl/soap/"
```

```
        xmlns="http://schemas.xmlsoap.org/wsdl/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
10865     xmlns:ihe="urn:ihe:iti:xds-b:2007" xmlns:rs="urn:oasis:names:tc:ebxml-
    regrep:xsd:rs:3.0"
        targetNamespace="urn:ihe:iti:xds-b:2007"
    xmlns:wsoap12="http://schemas.xmlsoap.org/wsdl/soap12/"
        xmlns:wsaw="http://www.w3.org/2007/05/addressing/wsdl" name="XDSRepository">
10870     <documentation>IHE XDS Document Repository</documentation>
        <types>
            <xsd:schema elementFormDefault="qualified">
                <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
                    schemaLocation="../schema/ebXML_RS/rs.xsd"/>
10875           <xsd:import namespace="urn:ihe:iti:xds-b:2007"
    schemaLocation="../schema/IHE/IHEXDS.xsd"/>
            </xsd:schema>
        </types>
        <message name="RetrieveDocumentSet_Message">
10880       <documentation>Retrieve Document Set</documentation>
            <part name="body" element="ihe:RetrieveDocumentSetRequest"/>
        </message>
        <message name="RetrieveDocumentSetResponse_Message">
            <documentation>Retrieve Document Set Response</documentation>
10885       <part name="body" element="ihe:RetrieveDocumentSetResponse"/>
        </message>
        <message name="ProvideAndRegisterDocumentSet_Message">
            <documentation>Provide and Register Document Set</documentation>
            <part name="body" element="ihe:ProvideAndRegisterDocumentSetRequest"/>
10890     </message>
        <message name="ProvideAndRegisterDocumentSetResponse_Message">
            <documentation>Provide And Register Document Set Response</documentation>
            <part name="body" element="rs:RegistryResponse"/>
        </message>
10895   <portType name="XDSDocumentRepository_PortType">
            <operation name="ProvideAndRegisterDocumentSet">
                <input message="ihe:ProvideAndRegisterDocumentSet_Message"
                    wsaw:Action="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b"/>
                <output message="ihe:ProvideAndRegisterDocumentSetResponse_Message"
10900               wsaw:Action="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-
    bResponse"/>
            </operation>
            <operation name="RetrieveDocumentSet">
                <input message="ihe:RetrieveDocumentSet_Message"
10905               wsaw:Action="urn:ihe:iti:2007:RetrieveDocumentSet"/>
                <output message="ihe:RetrieveDocumentSetResponse_Message"
                    wsaw:Action="urn:ihe:iti:2007:RetrieveDocumentSetResponse"/>
            </operation>
        </portType>
10910   <binding name="XDSDocumentRepository_Binding_Soap11"
    type="ihe:XDSDocumentRepository_PortType">
            <wsoap11:binding style="document"
    transport="http://schemas.xmlsoap.org/soap/http"/>
            <operation name="ProvideAndRegisterDocumentSet">
10915           <wsoap11:operation
    soapAction="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b"/>
                <input>
                    <wsoap11:body use="literal"/>
                </input>
```

```
10920                <output>
                         <wsoap11:body use="literal"/>
                     </output>
                 </operation>
                 <operation name="RetrieveDocumentSet">
10925                <wsoap11:operation soapAction="urn:ihe:iti:2007:RetrieveDocumentSet"/>
                     <input>
                         <wsoap11:body use="literal"/>
                     </input>
                     <output>
10930                    <wsoap11:body use="literal"/>
                     </output>
                 </operation>
             </binding>
             <binding name="XDSDocumentRepository_Binding_Soap12"
10935    type="ihe:XDSDocumentRepository_PortType">
                 <wsoap12:binding style="document"
         transport="http://schemas.xmlsoap.org/soap/http"/>
                 <operation name="ProvideAndRegisterDocumentSet">
                     <wsoap12:operation
10940    soapAction="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b"/>
                     <input>
                         <wsoap12:body use="literal"/>
                     </input>
                     <output>
10945                    <wsoap12:body use="literal"/>
                     </output>
                 </operation>
                 <operation name="RetrieveDocumentSet">
                     <wsoap12:operation soapAction="urn:ihe:iti:2007:RetrieveDocumentSet"/>
10950                <input>
                         <wsoap12:body use="literal"/>
                     </input>
                     <output>
                         <wsoap12:body use="literal"/>
10955                </output>
                 </operation>
             </binding>
             <service name="XDSDocumentRepository_Service">
                 <port name="XDSDocumentRepository_Port_Soap11"
10960    binding="ihe:XDSDocumentRepository_Binding_Soap11">
                     <wsoap11:address
         location="http://servicelocation/XDSDocumentRepository_Service"/>
                 </port>
                 <port name="XDSDocumentRepository_Port_Soap12"
10965                binding="ihe:XDSDocumentRepository_Binding_Soap12">
                     <wsoap12:address
         location="http://servicelocation/XDSDocumentRepository_Service"/>
                 </port>
             </service>
10970    </definitions>
```

V.3.2.2: Addressing Requirements

The Web Services Addressing specification (WS-Addressing) defines a framework for a transport-neutral SOAP messaging. Although understanding the concepts outlined in WS-Addressing is important,

most of the underlying details will be shielded by the abstraction layers provided to developers. This specification assumes an abstract separation between the application layer, the Web services messaging infrastructure layer, and the message transport layer.

The IHE transaction is built at the application layer, it is passed to the Web services messaging infrastructure layer where the SOAP message is constructed according to the rules set in the WSDL. The action value specified in the WSDL is used to construct the <wsa:Action> SOAP header. The endpoint address specified in the WSDL (or the supplied end point reference) is used to construct the <wsa:To>. Depending on the message exchange pattern (e.g., one-way, request-response), other WS-Addressing headers may be added at this point (e.g., <wsa:From>, <wsa:ReplyTo>, etc.).

IHE-WSA100) The example WSDL provided with IHE transactions shall use the WS-Addressing framework when specifying the Web Services protocol.

IHE-WSA101) All `<wsa:Action>` elements shall have the mustUnderstand attribute set (`mustUnderstand="1"`)

IHE-WSA102) The `<wsa:ReplyTo>` element of the initiating message shall be present and shall have the mustUnderstand attribute set (`mustUnderstand="1"`)

Example 2: Request Message
```
<soap12:Envelope xmlns:soap12="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsa="http://www.w3.org/2005/08/addressing">
      <soap12:Header>
            <wsa:Action
soap12:mustUnderstand="1">urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-
b</wsa:Action>
            <wsa:MessageID>urn:uuid:1600bc1a-10fd-4c3a-b41b-
7a15f4f46fb9</wsa:MessageID>
            <wsa:ReplyTo soap12:mustUnderstand="1">

      <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
            </wsa:ReplyTo>
            <wsa:To>
http://localhost:2647/XdsService/IHEXDSRepository.svc
      </wsa:To>
      </soap12:Header>
      <soap12:Body>
            <ProvideAndRegisterDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007"/>
      </soap12:Body>
</soap12:Envelope>
```

Example 3: Response Message
```
<soap12:Envelope xmlns:soap12="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsa="http://www.w3.org/2005/08/addressing">
      <soap12:Header>
            <wsa:Action
soap12:mustUnderstand="1">urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-
bResponse</wsa:Action>
            <wsa:RelatesTo>urn:uuid:1600bc1a-10fd-4c3a-b41b-
7a15f4f46fb9</wsa:RelatesTo>
      </soap12:Header>
      <soap12:Body>
            <rs:RegistryResponse xmlns:rs="urn:oasis:names:tc:ebxml-
regrep:xsd:rs:3.0"/>
```

```
        </soap12:Body>
</soap12:Envelope>
```

V.3.2.3: Security Requirements

11025

The IHE ATNA Integration Profile contains requirements which address certain aspects of security and authentication, including HTTPS transport requirements. Individual transactions which use Web Services will incorporate these requirements depending on their needs. Security profiles such as Cross-Enterprise User Assertion (IHE XUA) contain further security requirements. With the publication of the WS-I Basic Security Profile it is expected that ATNA will incorporate additional options for Web Services, and this appendix will reflect any requirements specific for Web Services for IHE transactions.

11030

V.4: Web Services for specific IHE Transactions

The Web Services specification is provided in three parts. The first part will be in Volume 2, where a separate subsection shall be added for each affected IHE transaction at the end of the "Message Semantics" section. This subsection shall detail the types and message parts of the WSDL. The actor-specific constraints against the IHE Web Services Requirements specified above shall be added at the end of each "Expected Actions" section.

11035

The second, informative part of the specification shall be on the IHE Wiki website (http://wiki.ihe.net), which shall contain a complete WSDL (Web Services Description Language) description of the web service, which aggregates the snippets from Volume 2 described above. There will be one WSDL contract per actor per profile. Each transaction is represented by a port type, where the operations names and message names follow the requirements specified in V.3.2.1.1. The complete WSDL is for reference purposes for implementers, and will not contain resolvable links to the XML schema.

11040

In order to provide implementers with an easily accessible resource, the WSDL files will also be available on the ftp://ftp.ihe.net server. It is expected that the WSDL files on the public ftp server will contain resolvable links, pointing to publicly available versions of the payload schema.

11045

V.4.1: Profiles using Web Services with HL7 V3 Messages

There are three supplements first published for Trial Implementation in 2007, which contain HL7 V3 messages: the PIXV3/PDQV3 ITI profile, XDS.b profile, and QED PCC profile. They contain specific values for the web services used for these transactions.

11050

V.4.2: Profiles using Web Services with other Transactions

The XDS.b profile describes the specific values for the web services used for its various transactions.

V.5: Web Services Standards Evolution

As the industry acceptance of newer standards/newer versions of existing standards progresses, new options will be added to existing transactions. One such expected change is the support for WS-Security and WS-Reliable Messaging as new options to web services transactions.

11055

V.6: Web Services References

WS-I: http://ws-i.org/

WS-I Basic Profile 1.1: http://www.ws-i.org/Profiles/BasicProfile-1.1.html

11060 WS-I Simple SOAP Binding Profile: http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html

SOAP 1.1: http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

SOAP 1.2: http://www.w3.org/TR/soap12-part0/

WSDL 1.1 SOAP 1.1 binding (Chapter 3): http://www.w3.org/TR/wsdl.html#_soap-b

WSDL 1.1 SOAP 1.2 binding: http://www.w3.org/Submission/wsdl11soap12/

11065 HL7 V3 Web Services Profile: http://www.hl7.org/v3ballot/html/infrastructure/transport/transport-wsprofiles.htm

WS-Addressing: http://www.w3.org/TR/ws-addr-core

WS-I Basic Security Profile: http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html

MTOM: http://www.w3.org/TR/soap12-mtom/

11070 XOP: http://www.w3.org/TR/xop10/

WS-Security 1.0: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss#technical

WS-Security 1.1: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss#technical

WS-Secure Conversation: http://specs.xmlsoap.org/ws/2005/02/sc/WS-SecureConversation.pdf

WS-Trust: http://docs.oasis-open.org/ws-sx/ws-trust/v1.3/ws-trust.html

11075 WS-Policy: http://www.w3.org/Submission/WS-Policy/

WS-Reliable Messaging: http://docs.oasis-open.org/ws-rx/wsrm/200702

11080

Appendix W: Implementation Material

Implementation material for ITI profiles such as XDS, XCA, RFD can be found on the IHE FTP site under ftp://ftp.ihe.net/TF_Implementation_Material/ITI/.

Some of the types of implementation material available are schema, examples and informative WSDL.

11085

GLOSSARY

See IHE IT Infrastructure Technical Framework. Vol 1: Glossary.