

**ACC, HIMSS and RSNA  
Integrating the Healthcare Enterprise**

5

**IHE IT Infrastructure Technical Framework  
Supplement 2004-2005**

10

**Cross-Enterprise  
Clinical Documents Sharing (XDS)**

15

**Public Comment Version**

**Comments due July 15, 2004**

20

20    **Contents**

	Introduction.....	4
	Scope of Supplement .....	5
	Open Issues and Questions .....	5
25	Work Breakdown .....	5
	Volume I – Integration Profiles .....	6
	10 Cross-Enterprise Clinical Document Sharing (XDS) .....	6
	10.1 Actors/Transactions .....	9
	10.2 Integration Profile Options.....	11
30	10.3 Integration Profile Process Flow .....	12
	10.4 General Principles .....	18
	Appendix XDS-A. XDS Security Environment .....	46
	Volume 2 – Transactions .....	47
	3.14 Register Document Set.....	47
35	3.15 Provide&Register Document Set .....	61
	3.16 Query Registry .....	69
	3.17 Retrieve Document .....	75
	3.18 Patient Identity Feed .....	78
	Appendix XDS-B – Required Registry Initialization .....	80
40	Appendix XDS-C – Affinity Domain Initialization.....	80
	Appendix XDS-D – Example of Provide and Register XML Schema.....	80
	Appendix XDS-E – Example of Query Response XML Schema.....	80
	Appendix XDS-F – XDS Security Environment.....	81
	A.1 Security Environment.....	81
45	A.2 Security Objectives.....	84
	A.3 Functional Environment .....	87

## Foreword

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 not to define new integration standards, but rather to support the use of existing standards, HL7, DICOM, IETF, and others, as appropriate in their respective domains in an integrated manner, defining configuration choices when necessary. When clarifications or extensions to existing standards are necessary, IHE refers recommendations to the relevant standards bodies.

This initiative has numerous sponsors and supporting organizations in different medical specialty domains and geographical regions. In North America the primary sponsors are the American College of Cardiology (ACC), the Healthcare Information and Management Systems Society (HIMSS) and the Radiological Society of North America (RSNA). IHE Canada has also been formed. IHE Europe (IHE-EUR) is supported by a large coalition of organizations including the European Association of Radiology (EAR) and European Congress of Radiologists (ECR), the Coordination Committee of the Radiological and Electromedical Industries (COCIR), Deutsche Röntgengesellschaft (DRG), the EuroPACS Association, Groupement pour la Modernisation du Système d'Information Hospitalier (GMSIH), Société Française 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.

The IHE Technical Frameworks for the various domains (IT Infrastructure, Cardiology, Laboratory, Radiology, etc.) 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 for these Technical Frameworks may be found at [www.rsna.org/IHE](http://www.rsna.org/IHE) or <http://www.himss.org/IHE>.

The IHE 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

90 depth. The volume I 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 clinical needs. The subsequent volumes provide detailed technical descriptions of each  
IHE transaction.

95 **This supplement to the IHE IT Infrastructure Technical Framework V1.0 is submitted for  
Public Comment between June 15, 2004 and July 15, 2004, per the scheduled announced in  
February 2004.**

**Comments are to be submitted before July 15, 2004 to:**

**<http://forums.rsna.org> under the “IHE” forum**

**Select the “*IT Infrastructure Supplements for Public Review*” sub-forum.**

100

**The IHE IT Infrastructure Technical Committee will address these comments and publish  
the Trial Implementation version in August 2004.**

## Introduction

105 This Supplement introduces a new IHE Integration Profile that facilitates the sharing across health enterprises of electronic clinical documents with textual and structured content.

This Integration Profile, referred to as XDS (for Cross-enterprise Document Sharing), is focused on providing a standards-based specification for managing the sharing of documents that healthcare enterprises (anywhere from a private physician to a clinic to an acute care in-patient facility) have decided to explicitly share. This contributes to the foundation of a shared  
110 Electronic Health Record.

## Background

One of the key integration problems in the realization of the EHR for the patients' continuity of care is the inability to share patient records across enterprises. Within these enterprises, multiple care delivery systems exist, each of which may be responsible for storage and retrieval  
115 of different cross sections of the clinical artifacts produced during patient care. Without commonly accepted mechanisms for accessing these repositories, it becomes difficult, if not impossible, to share documents from separate care delivery systems across a collection of cooperating enterprises.

This Integration Profile enables a number of healthcare delivery organizations belonging to a clinical affinity domain (e.g. a community of care) to cooperate in the care of a patient by sharing clinical records in the form of documents as they proceed with their patients' care delivery activities. In the context of this IHE Integration Profile, a document is a very broad concept that represents a unit of health information being shared. An XDS Document may include any type of information in any standard format. In this manner, a document-centric  
120 longitudinal record is accumulated over time for patients. Care providers are offered the means to query and retrieve specific clinical documents of interest from this longitudinal cross-enterprise record.

## Proposed Solution

130 XDS will use the concepts of document repositories and document registries. These are distinct entities with separate responsibilities:

- The repository is responsible for storing documents in a transparent and persistent manner and responding to document retrieval requests.
- The registry is responsible for storing information about the documents so that documents of interest for the care of a patient may be easily found, selected and retrieved  
135 irrespective of the repository where they are actually stored.

**XDS is document-content neutral. It will support any type of document without regard to content and format.**

This makes the XDS IHE Integration Profile equally able to handle documents containing simple text, formatted text (e.g. HL7 CDA Level 1), images or structured and vocabulary coded clinical

- 140 information. In order to ensure the necessary interoperability between the document sources and the document consumers, these documents shall comply with widely accepted standards (e.g. HL7 CDA, CEN EHRCOM, ASTM CCR, DICOM, etc.).

## Scope of Supplement

- 145 This supplement extends the existing IHE IT Infrastructure Technical framework and assumes that the reader is familiar with the IHE process and methodology in defining Integration Profiles, as well as familiar with the five IHE IT Infrastructure Integration profiles defined by the IHE ITI Technical Framework Version 1.0. The IHE ITI Technical Framework Version 1.0 documentation is available at [www.himss.org/ihe](http://www.himss.org/ihe) or [www.rsna.org/ihe](http://www.rsna.org/ihe).

- 150 The XDS Integration Profile is not intended to addresses all Cross-enterprise EHR communication needs. Some of them may require the use of other IHE Integration profiles, such as Patient Identifier Cross-Referencing, Audit Trail & Node Authentication, Retrieve Information for Display, etc. Others may be only partially supported. Others may require future IHE Integration profiles, which will be defined by IHE as soon as the necessary base standards are available.

- 155 This supplement is issued for a one-month public comment until July 15<sup>th</sup> and is targeted to be issued for trial implementation in August 2004. IHE Connectathons will be held early 2005 in various regions of the world to test a number of vendor implementations of this profile. A final text version is scheduled to be issued by early spring 2005, following demonstrations at various venues, including HIMSS 2005.

- 160 The development of this IHE Integration Profile relies on considerable work and standards development activities that have been performed in this domain in many countries around the world (e.g. OASIS-ebXML, HL7 CDA, CEN EHRcom, etc.).

## Open Issues and Questions

- 165 1. Child/mother multi ID  
2. Revision of meta-Data  
3. Explain that meta-data is not part of the legal medical record.

## Work Breakdown

- 170 Volume 1: XDS Integration Profile, Actors, Transactions, Options and Process Flow.  
Charles Parisot, Peggy Rands, Keith W. Boone, Didi Davis and Karima Bourquard  
Volume 2: Transactions  
Bill Majurski, Emmanuel Cordonnier, Fred Behlen  
Volume 1 & 2: Security  
Rob Horn and Glen Marshall

175

## Volume I – Integration Profiles

<i>Add the following section to Vol 1 of the IHE ITI Technical framework</i>
--

### 10 Cross-Enterprise Clinical Document Sharing (XDS)

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

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

Examples of affinity domains include:

- Community of Care supported by a Local Health Information Infrastructure (LHII) in order to serve all patients in a given region.
- Nationwide EHR
- 190 • Specialized or Disease-oriented Care
  - Cardiology Specialists and an Acute Cardiology Center
  - Oncology network
  - Diabetes network
- Federation of enterprises
- 195 ○ A regional federation made up of several local hospitals and healthcare providers
- Government sponsored facilities (i.e., VA or Military)
- Insurance Provider Supported Communities

200 Within a clinical affinity domain, certain common policies and business rules must be defined. They include how patients are identified, consent is obtained, access is controlled, or how to structure, organize or represent clinical information. This Integration Profile does not define such policies and business rules; however it has been designed to accommodate a wide range of needs. The management of clinical documents through document repositories and document registries creates a longitudinal record of information about a patient within a given clinical affinity domain. These are distinct entities with separate responsibilities:

- 205 • The document repository is responsible for storing documents in a transparent, reliable and persistent manner and responding to document retrieval requests.
- The document registry is responsible for storing information about those documents so that the documents of interest for the care of a patient may be easily found, selected and retrieved irrespective of the repository where they are actually stored.

210 The concept of document in XDS is not limited to textual information. As XDS is document content neutral, any type of clinical information without regard to content and representation is

supported. This makes the XDS IHE Integration Profile equally able to handle documents containing simple text, formatted text (*e.g.*, HL7 CDA Level 1), images (*e.g.*, DICOM) or structured and vocabulary coded clinical information (*e.g.*, CDA version 2, CCR, DICOM SR).  
215 In order to ensure the necessary interoperability between the document sources and the document consumers, these documents shall comply with widely accepted standards (*e.g.*, HL7 CDA, CEN EHRCOM, ASTM CCR, DICOM).

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

The XDS Integration Profile is not intended to addresses all cross-enterprise EHR communication needs. Some of them may require the use of other IHE Integration profiles, such  
225 as Patient Identifier Cross-Referencing, Audit Trail and Node Authentication, Enterprise User Authentication, and Retrieve Information for Display. Others may be only partially supported. Others may require future IHE Integration profiles, which will be defined by IHE as soon as the necessary base standards are available. Specifically:

- 230 1. The management of dynamic information (non-document-oriented) such as allergy lists, medication lists, problem lists, etc is not addressed by XDS. However, the Retrieve Information for Display Integration Profiles may be used to provide an elementary support of such capabilities through the use of an application (Information Source Actor) extracting such information from previously submitted clinical documents (in a coded form) and offering it for human display access. A complementary approach to managing  
235 updates and structured application access to such dynamic clinical information may be expected as a separate Integration Profile in the future.
- 240 2. The placing and tracking of orders (*e.g.* drug prescriptions, radiology orders, etc.) is not supported by XDS. This does not preclude the use of XDS to store and register orders and corresponding results when such artifacts need to be recorded in the patient’s health record. A complementary approach to cross-enterprise order workflow (*ePrescription*, *eReferral*) may be expected as separate Integration Profiles in the future.
- 245 3. The management of independent patient identification registration will be supported with the use of the IHE Patient Identifier Cross-referencing Integration Profile.
- 250 4. The operation of any Clinical Affinity Domain will require that a proper security model be put in place. It is expected that a range of security models should be possible. Although the XDS Integration Profile is not intended to include nor require any specific security model, it is expected that XDS implementers will want to group XDS Actors with actors from the IHE Audit Trail and Node Authentication and/or IHE Enterprise User Authentication Profiles. More details on grouping XDS Actors with these profiles can be found in Appendix A.2 Integration with ATNA and EUA. Appendix B Security addresses XDS Security requirements and issues in greater detail.



5. XDS does not define the mechanisms by which patient information is transferred from one clinical affinity domain to another. A complementary Integration Profile may be expected in the future.
- 255 6. XDS does not address transactions for the management or configuration of a clinical affinity domain, for example, the configuration of network addresses or the definition of what type of clinical information is to be shared in a specific clinical affinity domain

## **Glossary**

### **EHR-CR**

- 260 The care delivery systems used within an enterprise for managing episodes of patient care are called in this document the Electronic Health Record – Care Delivery Record, abbreviated as EHR-CR.

### **EHR-LR**

- 265 The collection of cooperating actors within a Clinical Affinity Domain which support storage, retrieval and query of patient records produce an aggregate system called in this document the Electronic Health Record – Longitudinal Record, abbreviated as EHR-LR.

### **Document**

- 270 An XDS Document is the smallest unit of information that may be provided to a Document Repository and registered in Document Registry. An XDS Document may contain simple text, formatted text (e.g. HL7 CDA Level 1), images (e.g. DICOM) or structured and vocabulary coded clinical information (e.g. CDA version 2, CCR).

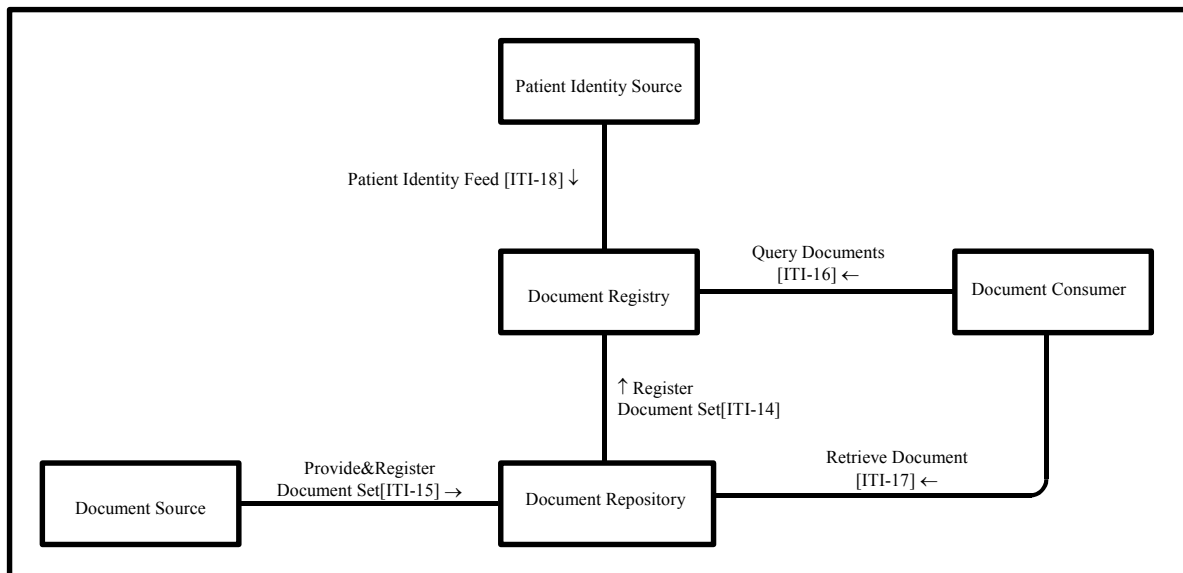
### **Submission Set**

- 275 An XDS Submission Set creates a permanent record of a set of new XDS Documents and previously registered XDS Documents related to care event(s) provided to a patient by a care deliver organization, EHR-CR.

### **Folder**

- 280 An XDS Folder allows Document Sources in EHR-CRs to group the records they submit with other related documents. What constitutes a Folder and the vocabulary associated with the specific Folders used by EHR-CRs is decided by an agreement between the care delivery organization members of a Clinical Affinity Domain.

## 10.1 Actors/Transactions



**Figure 10.1-1 Cross-Enterprise Document Sharing Diagram**

285

**Table 10.1-1 XDS - Actors and Transactions**

Actors	Transactions	Optionality	Section in Vol. 2
Document Consumer	Query Documents	R	
	Retrieve Document	R	
Document Source	Provide and Register Document Set	R	
Document Repository	Provide and Register Document Set	R	
	Register Document Set	R (Note)	
	Retrieve Document	R	
Document Registry	Register Document Set	R (Note)	
	Query Documents	R	
	Patient Identity Feed	R	
Patient Identity Source	Patient Identity Feed	R	

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

### 10.1.1 Actors

290

#### 10.1.1.1 Document Source

The Document Source actor is the producer and publisher of documents. It is responsible for putting documents into a Document Repository actor. It also supplies meta-data to the

Document Repository Actor for subsequent registration of the documents with the Document Registry actor.

295    **10.1.1.2 Document Consumer**

The Document Consumer Actor queries a Document Registry Actor for documents meeting certain criteria, and retrieves selected documents from one or more Document Repository actors.

**10.1.1.3 Document Registry**

300    The Document Registry actor maintains meta-data about each registered document in a document entry. This includes a link to the Document Repository where the actual document is stored. The Document Registry responds to queries from Document Consumer actors about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration.

**10.1.1.4 Document Repository**

305    The Document Repository actor persistently stores documents. It assigns and maintains a unique identifier for each document, to allow Document Consumers to retrieve them.

**10.1.1.5 Patient Identity Source**

The Patient Identity Source actor assigns a unique identifier to each instance of a patient as well as maintains a collection of identity traits.

310

**10.1.2 Transactions**

**10.1.2.1 Provide and Register Document Set**

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

**10.1.2.2 Register Document Set**

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

---

### 10.1.2.3 Query Documents

330 The Query Documents transaction is issued by the Document Consumer actor on behalf of a care provider (EHR-CR) to a Document Registry. The Document Registry actor searches among the Document Entries to locate documents (assuming permission is granted) that meet the provider's specified query criteria. It will return a list of document entries that contain meta-data found to meet the specified criteria including the locations and identifier of each corresponding document in Document Repositories

### 10.1.2.4 Retrieve Document

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

### 10.1.2.5 Patient Identity Feed

340 This is Transaction 8, defined as part of the Patient Identifier Cross-referencing Integration Profile. It conveys the patient identifier and corroborating demographic data, captured when a patient's identity is established, modified or merged or in cases where the key corroborating demographic data has been modified. Its purpose in the XDS Integration Profile is to populate the registry and repository with patient identifiers that have been registered for the affinity domain.

## 10.2 Integration Profile Options

345 Options that may be selected for this Integration Profile are listed in the table X.2-1 along with the Actors to which they apply. Dependencies between options when applicable are specified in notes.

**Table X.2-1 XDS - Actors and Options**

Actor	Options	Vol & Section
Document Source	<i>No options defined</i>	--
Document Repository	<i>No options defined</i>	--
Document Registry	<i>No options defined</i>	--
Document Consumer	<i>No options defined</i>	--
Patient Identity Source	<i>No options defined</i>	--

350

### 10.3 Integration Profile Process Flow

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

Two examples of Affinity Domains are described below, a cardiac care network and community EHR

#### Example 1: Cardiac Patient Management Scenario

This scenario spans about 3 weeks of a patient's cardiac episode. The patient presents to her primary care provider (PCP) with complaints of shortness of breath, nausea, tiredness and chest pains. This doctor works closely with a local hospital that has recently established a cardiac care network that allows PCPs, cardiologists, laboratories and two local hospitals to share clinical documents to improve patient care.

1. Before the patient examination, the PCP queries the cardiac care network for clinical information on the patient over the last two years. He locates a prior ECG report that is retrieved. He performs a new ECG and determines that the patient should be referred to a cardiologist.

Using PCP EMR system, he creates a submission request for a "PCP office visit" that includes a submission set of 3 new documents (visit note, referral letter, new ECG report) and reference to the prior ECG report. In addition, he chooses to create a "cardiac assessment" Folder to contain all four document in order to facilitate collaboration with the cardiologist.

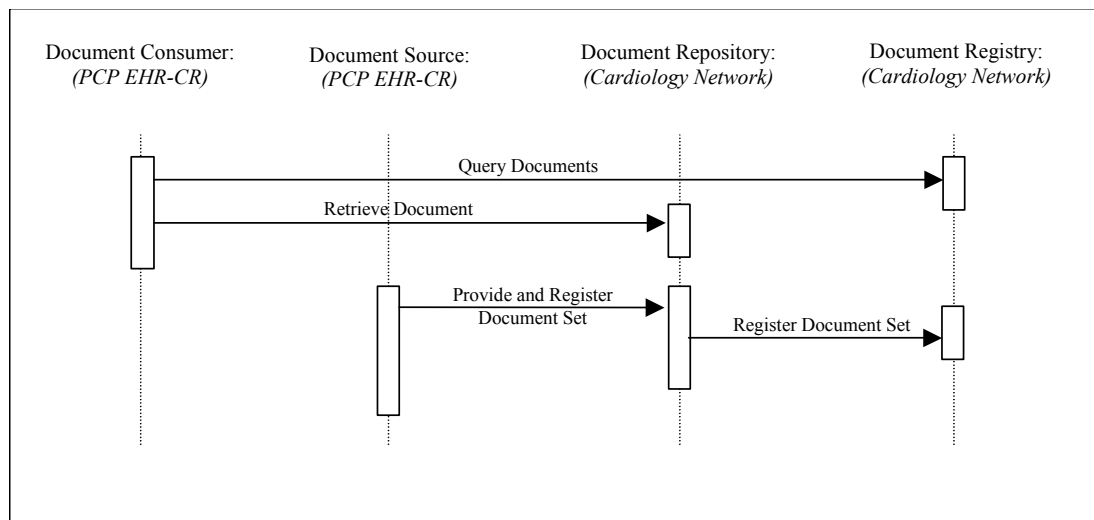


Figure 10.3-1 PCP Query Transactions Process Flow

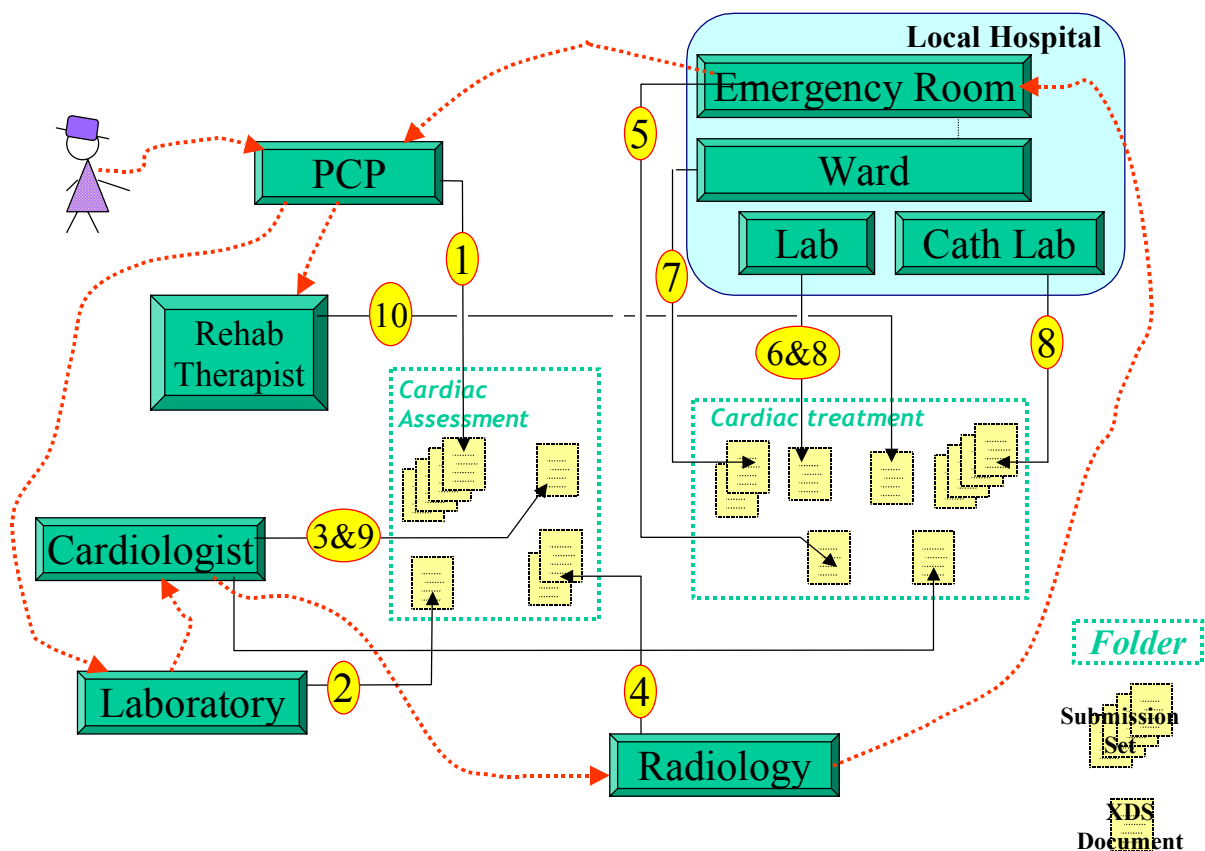
The PCP EMR system implements the Document Consumer and Document Source Actors to issue the Query, Retrieve and Provide & Register transactions as shown in Figure 1. The transactions are processed by the Document Repository and the Document Registry provided by the cardiology care network.

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

- 385 3. The cardiologist sees the patient. He queries the repository for the patient’s records in reverse chronological order. Available are the Visit note from the PCP, the ECG and prior ECG, the referral letter (all part of the “cardiac assessment” Folder) and the lab results.

The cardiologist performs an ultrasound, dictates a visit note, and orders a nuclear stress test. The visit note and ultrasound images and report are registered as a “cardiologist office visit” submission set and place in the “cardiac assessment” Folder. In addition, the lab report is added to the “cardiac assessment” Folder.

390

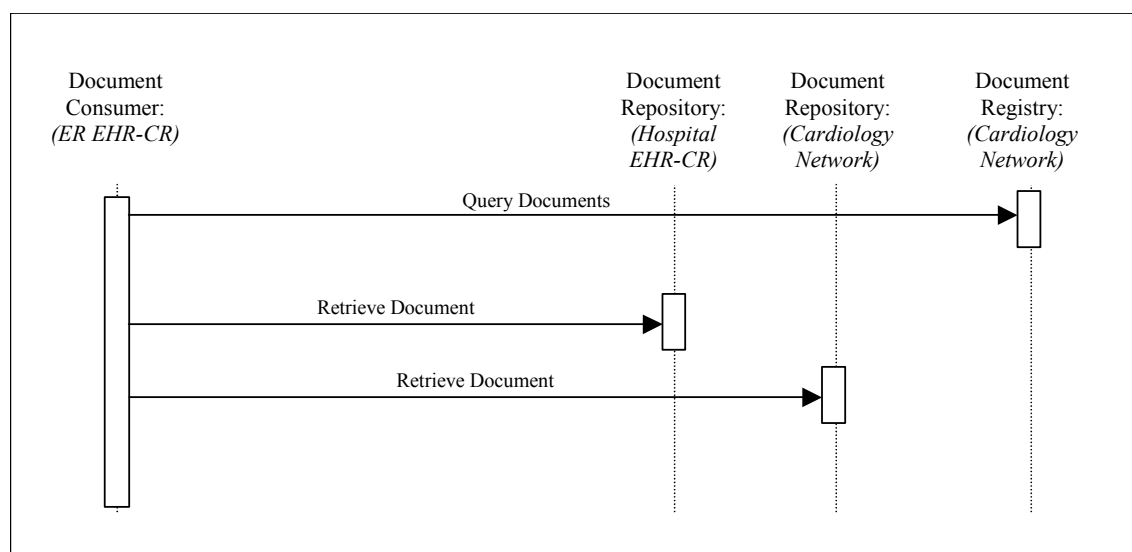


**Figure 10.3-2 Cardiac Patient Management Scenario Transaction Process Flow**

4. The patient is seen at Radiology facility for the nuclear stress test. The test is performed, and the radiologist dictates the report. The nuclear stress test report is registered in a “radiology examination” submission set and associated with the “cardiac assessment” Folder.
5. Although she has a scheduled appointment with her cardiologist in two days, she wakes up with severe chest pain. On the way to work, she decides to go to the emergency room (ER) of her local hospital.

The ER doctor uses the Hospital EHR system to queries the cardiac care network registry and repositories for documents related to the patient in reverse chronological order. Available documents from latest cardiology related Folder are the visit notes from PCP and cardiologist, the recent ECG and past ECG, the lab results, and the ultrasound images and report, and the nuclear stress test images and report

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



**Figure 10.3-3 ER Query Transactions Process Flow**

6. While talking to the ER physician, the cardiologist accesses the cardiac care network from his home office. He queries for all documents related to the patient since the last visit in his office. The nuclear stress test report that he did not previously review is available, along with Lab results and ECG results from the ER. The two physicians determine a plan of care and the cardiologist makes arrangements to see the patient in the hospital.
7. The ER visit notes are submitted as an “emergency department visit” submission set and placed in a newly created “cardiology treatment” Folder along with the earlier lab and ECG results.

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

425 • A cath intervention report is dictated.

  - Patient is returned to monitored care for recovery.
  - Education given to patient and family.
  - Discharge Summary dictated by cardiologist.
  - Cardiologist orders lab tests to be completed prior to scheduled follow-up visit.
- 430 The Admission Assessment, Lab results, Cath intervention report and key images, and Discharge Summary form a “cardiology intervention” submission set, which is registered with the cardiac care network registry for the “cardiac treatment” Folder.
- 435 9. The patient returns to the cardiologist for the post discharge follow-up visit. The result visit note, cardiac rehab and summary letters are placed in a “cardiology office visit” submission set and in the “cardiac treatment” Folder.
10. The patient goes to rehab sessions as scheduled by the cardiologist. The patient recovers and is seen by the PCP and Cardiologist for routine visits.

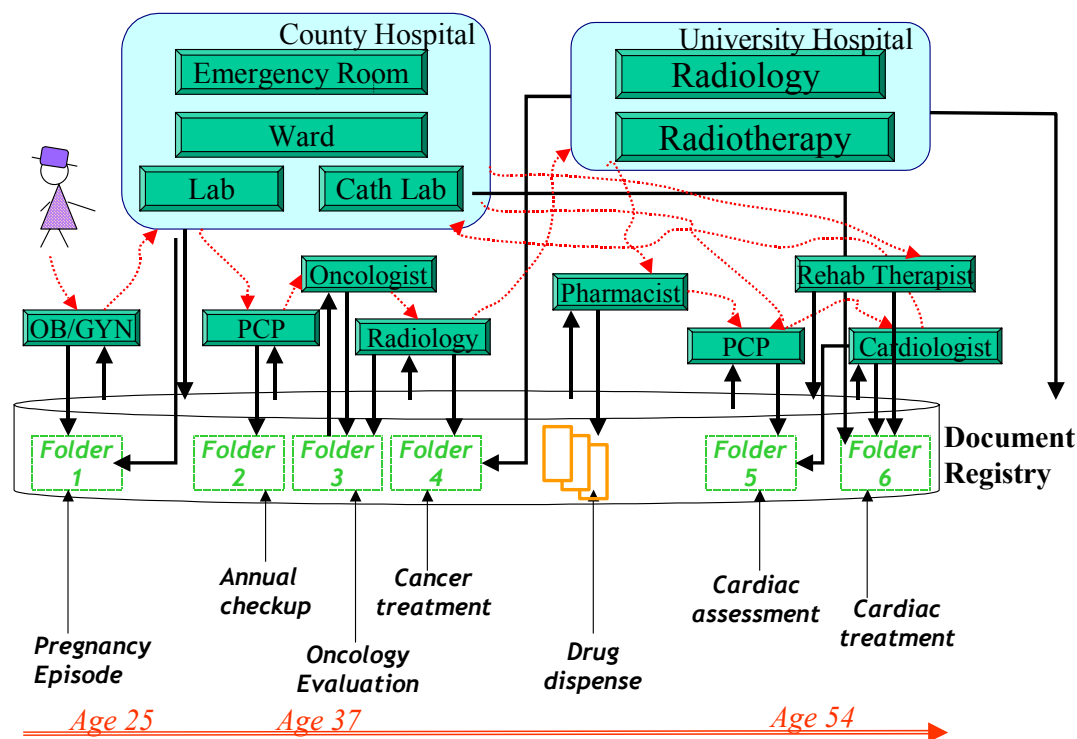
### **Example 2: Longitudinal Patient Care Scenario**

- 440 This scenario spans about 30 years of a patient’s life including a pregnancy, a cancer treatment and a cardiac problem. She stayed within the same community where care was provided to her by a university hospital, a county hospital, a drugstore next to her home, her primary care provider, a private lab, a cardiologist, an oncologist, an ob/gyn, and a physical therapist. In this community, these care providers belong to a care network that has agreed to share patients clinical documents through what this Integration profile calls a Clinical Affinity Domain.
- 445 1. At age 25, she is pregnant and is under the care of her OB/GYN physician. During the course of her pregnancy she made several visits. For each visit her physician made a submission of a set of documents (a visit note and sometimes a lab result, an echo report, etc.). Each one of these submissions is labelled as “pregnancy office visit” and is linked to the same pregnancy episode. Such an episode is identified in this integration profile as
- 450 a Folder with a clinical meaning of “pregnancy episode”.
2. She is admitted to the County Hospital for delivery of the baby. The delivery is uneventful. All pertinent documentation associated with the delivery is submitted by the county hospital as a “in-patient delivery” submission and linked to the same “pregnancy episode” Folder.
- 455 3. The patient is seen by the OB/GYN for follow-up after delivery of baby. In preparing his summary of the pregnancy, the doctor queries the care network registry to list all the documents submitted for this pregnancy Folder selecting the appropriate documents. This summary document is submitted as a “pregnancy summary” submission linked to



460

the “pregnancy episode” Folder. No other submissions of documents will happen in the case of this Folder.



**Figure 10.3-4 Longitudinal Patient Care Scenario Process Flow Overview**

465

4. At age 37, our patient is seen by her Primary Care Provider (PCP) for an annual exam. Based on exam and tests done, the PCP determines that the patient should be referred to an oncologist for further evaluation. Two submissions were made against two Folders: an “annual check-up” and an “Oncology Evaluation”. The “annual check-up” Folder contains an “annual check-up” submission which includes several documents among which the lab report with the abnormal findings. The “oncology evaluation” Folder is created with an “oncology referral” submission which contains a referral letter and the reference to the same lab report.
5. The patient is seen by the Oncologist. The doctor orders a PET/CT scan that is to be done at the University Hospital radiology department. The oncology office visit note is contributed as a single document submission set in the same “oncology evaluation” Folder.
6. The patient goes to the University Hospital and the PET/CT scan is performed. The radiology report and key images are also submitted under the “oncology evaluation” Folder.

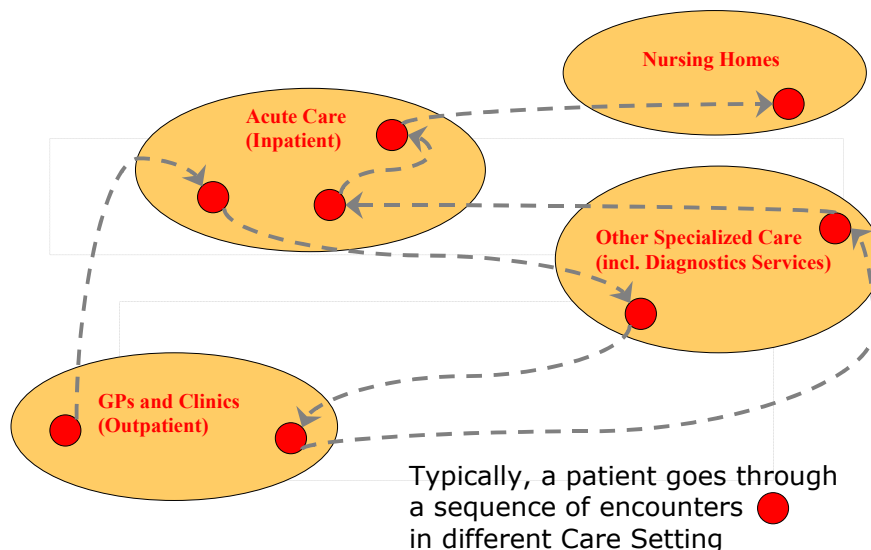
475

- 480 7. The Oncologist reviews the PET/CT report, confirms a cancer diagnosis and decides that surgery is needed. The office visit note is submitted as the first submission of a new Folder for “cancer treatment”.
8. The patient is admitted to the University Hospital for surgery. The tumor is removed and confirmed via pathology to be cancerous. Inpatient documentation results in an “inpatient surgery” submission set to the “cancer treatment” Folder. The patient is discharged with multiple prescriptions.
- 485 9. Each time one of the prescriptions is filled by the local pharmacist, the pharmacy creates a single dispense document in a “drug dispense” submission set. The drug dispense submission sets are not associated with a Folder.
- 490 10. Our patient has 12 follow-up visits for radiotherapy at the University Hospital. Summary documentation of radiotherapy and diagnostic radiology procedures is stored as one or more submission sets under the “cancer treatment” Folder.
11. The patient is seen by the oncologist and released from care with follow-up noted to occur in six months. The oncologist documents a summary of this episode and submits the summary document as a submitted to the “cancer treatment” Folder.
- 495 12. The patient makes annual visits to her PCP. At each visit, he queries the care network registry for all document submissions made during the past year.
13. At age 54, the patient is seen by the PCP complaining of shortness of breath, nausea, tiredness and chest pains. The PCP refers the patient to a cardiologist. See Example 1 for detailed explanation for this episode.

## 10.4 General Principles

### 10.4.1 EHR-CR Concept

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

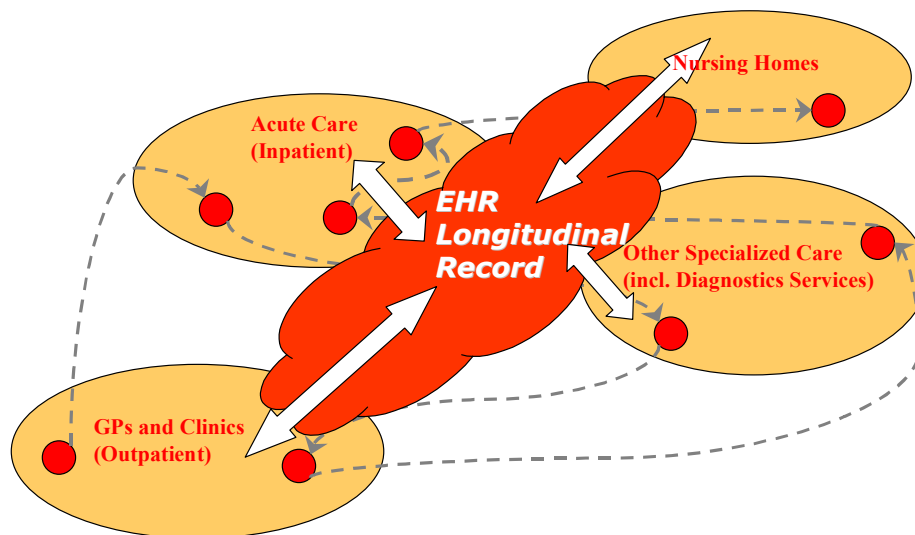


**Figure 10.4.1-1 Sequence of encounters across care delivery organizations**

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

1. EHR-CR as Document Source may only contribute documents in one of the Document Formats that are supported by the XDS Affinity Domain (e.g. CDA Level 1, CDA Level 2 with specific templates, DICOM Composite SOP Classes, ASTM-CCR, etc).
2. EHR-CR as Document Source shall provide clinical information in document types as defined by the XDS Affinity Domain. EHR-CRs as Document Sources are responsible to map their local codes into the affinity domain codes if necessary. This Profile does not require that the EHR-CR as Document Sources and Consumers store and manage their internal information in the form of documents as they are shared throughout the XDS Affinity Domain.

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



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

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

#### 10.4.2 XDS Document Concept

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

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

535 An XDS Document may be human and/or application readable. It is broader than HL7 CDA in that an XDS Document may not only be application readable but also human readable (e.g. a JPEG or PDF document). In either cases, it shall comply with a published standard defining its structure, content and encoding. In addition, IHE intends to define content-oriented Integration Profiles profiling such content standards to be used in conjunction with XDS.

Furthermore:

---

<sup>1)</sup>This concept is defined by the CEN EHRCOM standard.

- 540       1. When submitted for sharing, an XDS Document shall be provided to the Document Repository Actor as an octet stream with an associated MIME type.
- 545       2. When retrieved through the Retrieve Document transaction, it shall be unchanged from the octet stream that was submitted (full fidelity repository).  
Note: An XDS Document may be a MIME multipart document (e.g. an HL7 CDA as its first part followed by attachments as files). The first part of the multi-part contains the primary part of the document, other parts are direct attachments to the primary part. The Document Repository handles this multi-part data set as an “opaque entity”. The Document Repository does not need to analyze or process its multi-part structure nor the content of any parts in the context of the XDS Integration Profile.  
Note: An XDS Document may be retrieved using alternate methods using document specific retrieval methods. Such optional capabilities are not provided in the current specification of XDS, but are possibly candidates for addition as future options this Integration Profiles.
- 550       3. An XDS Document shall be associated with Meta-Data defined by the Document Source. This Meta-Data information shall be placed by the XDS Registry Actor in a XDS Document Entry, and is used for query purposes by XDS Consumer Actors.
- 555       4. The XDS Integration Profile manages XDS Documents as a single unit of information, it does not provide mechanisms to access portions of an XDS Document. Only the Document Sources or Document Consumers have access to the internal information of the XDS Document.
- 560       5. In a Clinical Affinity Domain the Document Registry Actor shall maintain a single document entry for each XDS Document stored by a Document Repository Actor. Duplicate copies of the same XDS Document (with the same unique identifier) may be stored and registered. Registration of an XDS Document with the same unique identifier but a different content is rejected.
- 565       6. An XDS Document will be globally uniquely identified, so that no two XDS Documents with different content shall bear the same Unique Identifier. This Identifier is unique across all Clinical Affinity Domains, which allows potential merger of XDS Document Repositories from different domains, if desired.
- 570       7. For each XDS Document placed in a Document Repository, the XDS Integration Profile specifies the specific Document Meta-data to be registered in the Document Entry of the Clinical Affinity Domain to which the Document Repository belongs. It is the responsibility of the Document Source Actor to ensure that the XDS Document Meta-data reflects the actual content of the associated XDS Document. Neither the Document Repository nor the Document Registry checks this consistency.
- 575       8. The Document Source maintains the following responsibilities over the XDS Documents it has registered:
- a. It has exclusive rights to change the status of any of these Documents from “Approved” to “Deprecated” and to “Deleted”. This responsibility may be shared with the patient depending on the Clinical Affinity Domain policies.

- 580                   b. It has exclusive rights to submit an XDS Document with a “Parent Relationship”  
of replacement for one of its previously submitted document.

### 10.4.3 Submission Request

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

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

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

- 590                   1. Meta-Data to be placed in Document Entries for new XDS Documents being submitted
2. A Submission Set that includes the list of all new XDS Documents being submitted and optionally a list of previously submitted XDS Documents
3. If desired, Folders to be created with the list of included XDS Documents (new document being submitted as well as previously submitted)
- 595                   4. If desired, addition to previously created Folders of lists of XDS Documents (new document being submitted as well as previously submitted)
5. The XDS Document octet stream in a Submission Set conveyed by a Provide and Register transaction.

### 10.4.4 Submission Set

600                   An XDS Submission Set is created by a Document Source Actor when creating a submission request in order to share one or more XDS Documents. It creates a permanent record of a set of new XDS Documents that are being registered or previously registered XDS Documents. These are related to care event(s) provided to a patient by the care delivery organization (EHR-CR) performing the submission request.

- 605                   1. The four fundamental properties of an XDS Submission Set are as follows:
- It is related to care event(s) of a single patient, uniquely identified in the Patient Identification Domain of the XDS Document Registry.
- It includes the list of new XDS Documents included in the Submission Request that results from some care event(s).
- 610                   • It may include a list of pre-existing (i.e. already registered) XDS Documents that have a relationship with the same care event(s).

- A Submission Set has four attributes: the identification of the Document Source Actor, a unique identifier of the Submission Set, a care event(s) time span, and a type code plus its meaning (see section XX).
- 615      2. An XDS Submission Set is created for each submission request. It is related to a single Document Source Actor and is conveyed by a single Provide & Register Document Set transaction or a Register Document Set transactions.
- 620      3. Upon the successful registration of the Submission Set in a Provide & Register Document Set transaction:
- The new XDS Documents included in the XDS Submission Set are available for sharing in an XDS Clinical Affinity Domain.
  - The Submission Set, including the references to these newly registered XDS Documents, the references to the already registered XDS Documents, and the attributes of the Submission Set are available for sharing in an XDS Clinical Affinity Domain.
- 625      4. In case of failure to process a Submission Request, the registration of the Submission Set including the lists of new documents and pre-existing XDS Documents shall not occur and elements of the Submission Set shall not be made visible to Document Consumers.
- 630      5. A Submission Set is assigned a unique identifier by the Document Source. The Document Registry may be queried to find all documents registered in the same XDS Submission Set.
- 630      6. The same XDS Document may be initially registered as part of a single Submission Set but may also be referenced by multiple XDS Submission Sets.

#### **10.4.5 Concept of Folder**

- 635      XDS takes into account a broad range of healthcare delivery organizations (EHR-CR) that are interested to contribute and share documents related to the care of a patient. It therefore does not constrain workflow processes within these EHR-CRs, but provide complete flexibility to relate Documents and Submission Sets to an encounter, a visit, an episode of care, or various other approaches.
- 640      The purpose of an XDS Folder is to provide a collaborative mechanism for several XDS Document Sources to group XDS Documents for a variety of reasons (e.g. a period of care, a problem) and to offer the Document Consumers an easy access to these groups of XDS documents.

The following principles apply to an XDS Folder:

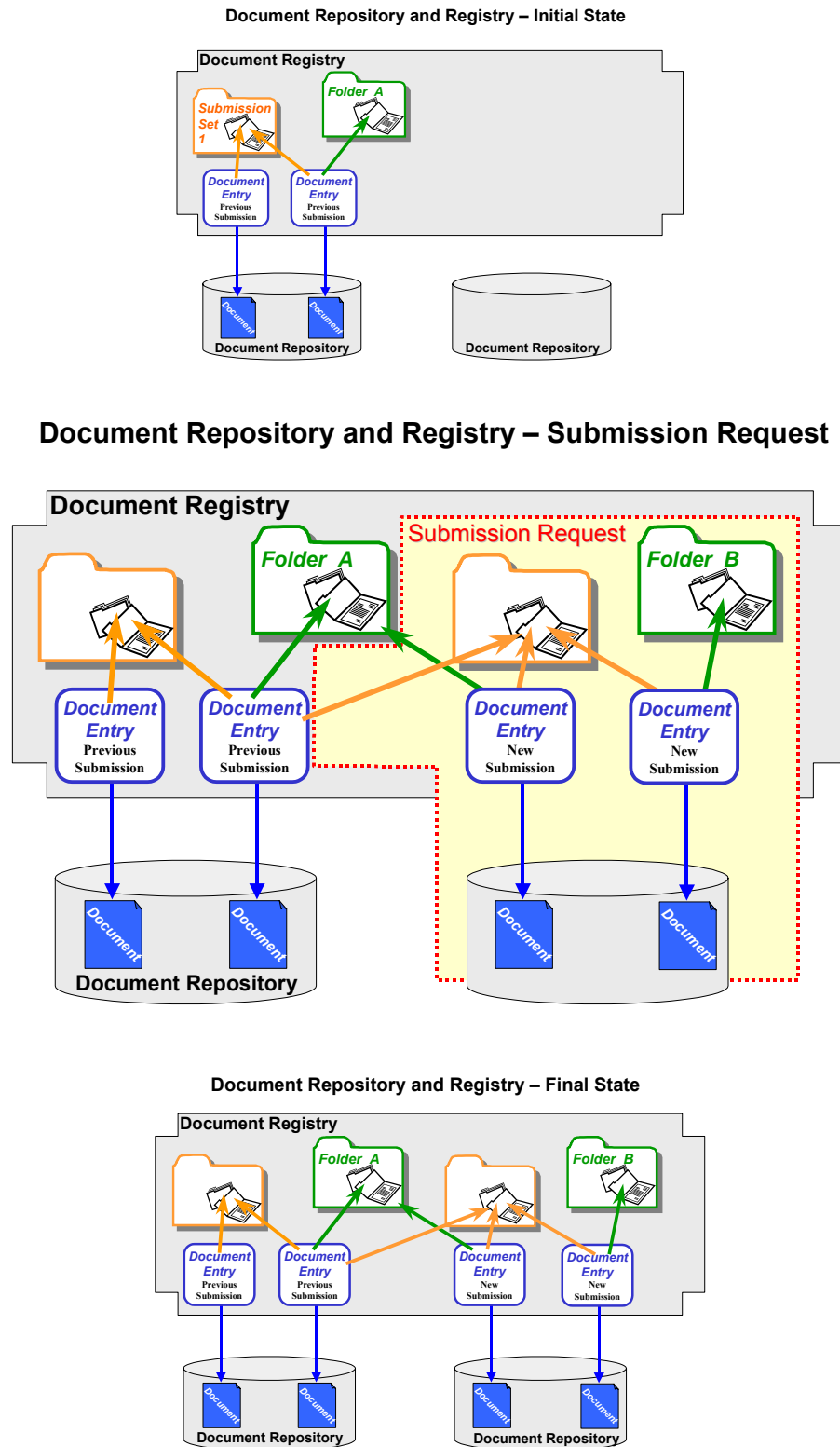
- 645      1. A Folder is a set of XDS Documents related to the care of a single patient.
2. The XDS Documents placed in a Folder may be submitted by one or more Document Source Actors.
3. It is assigned a unique identifier by the Document Source that created the Folder.

- 650 4. XDS Documents may be placed into an existing Folder at any time, as long as they relate to the same patient. The means for Document Source Actors to find existing Folders may be achieved by Queries of the Document Registry or means outside the scope of XDS (e.g. Cross-enterprise workflow, such ePrescription, eReferral, etc).
5. A Folder has the following attributes:
- A human readable name.
  - 655 • A list of codes/meaning. The list of clinical meanings of a Folder is distinct from the clinical meaning of an XDS Submission Set.
  - a time interval (computed from the earliest and latest time intervals of the Submission Set in which the XDS Documents have been first submitted).
6. Once created a Folder is permanently known by the Document Registry.
- 660 7. By querying the Document Registry, a Document Consumer may find all Document Entries placed in the same Folder.
8. Folders creation, placing new and existing Documents in Folders is not recorded as part of the Submission Set. The two concepts are orthogonal.

#### 10.4.6 Example

- 665 The sequence of figures below shows an example of a submission request that includes two new documents, a reference to a preexisting document and the use of two folders. The first figure depicts the initial state of the Document Registry with two existing Documents that have been submitted as part of an earlier submission request along with placing one of these documents into a Folder A. The last figure depicts the resulting state of the Document Registry after the
- 670 Submission Request is successfully processed.

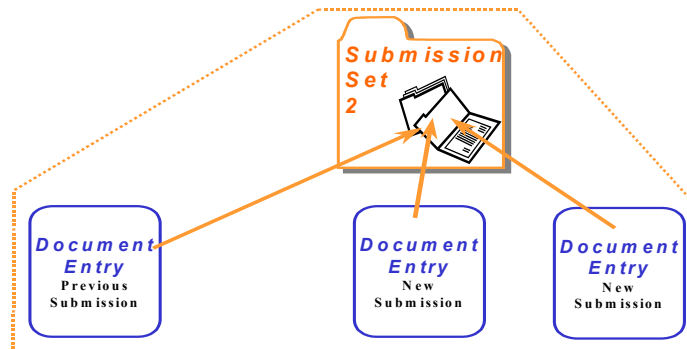




675

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

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



**Figure 10.4.6-2 The logical content of a Submission Set**

### 10.4.7 Concept of an XDS Affinity Domain

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

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

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

3. It includes any number of Document Repository Actors (a distributed configuration is the default, however, a centralized configuration with a grouped Registry/Repository is also supported).
4. It contains an explicit list of Document Consumer and Document Repository actors that participate in document sharing. Addition of a Document Repository or Document Consumer Actor is an administrative act that requires awareness from the Registry and Repositories.
5. There is a chain of trust established between the users (healthcare staff) in each EHR-CR and the Affinity Domain.
6. Document Repositories and Document Consumers may belong to more than one Affinity Domain and share the same or different documents. This is an implementation strategy and will not be further described.
7. The Affinity Domain supports a primary Patient Identification Domain that is used by the Document Source and Consumers to communicate with the Document Registry. When

Document Sources and Consumers in the Affinity Domain belong to different Patient Identifier Registration Domains, the Document Source and Consumers may cross-reference their own Patient Identifier Registration Domains to that of the Registry using the IHE Patient Identifier Cross-referencing Integration Profile.

- 710        8. A Document Source may only contribute documents with Document Codes and Health Facility Codes that draw from a Vocabulary Value Set that is approved by the Affinity Domain.

#### **10.4.8 Other Principles of XDS**

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

- 715        1. When a document is registered with the Document Registry Actor, all references it contains shall either be to:
- Documents that may be found under the management of the XDS Document Registry (by querying the Registry)
  - Documents that are not under the management of the XDS Document Registry. Such  
720        references may be available to the EHR-CR that registered the document that includes the reference. It is beyond the scope of XDS to provide access to such documents internal to the EHR-CR.
- 725        2. The XDS Repositories are not expected to perform any processing or translations on document content. Processing and translation are the responsibility of a Source EHR-CR or Consumer EHR-CR. The analysis, cross-document combination and presentation of document content is outside the scope of the XDS Integration Profile and its actors.
- 730        3. The custodianship for the clinical information contained in a registered document remains with the Source Actor of the EHR-CR. The EHR-LR offers only a “shared space” under the responsibility of each contributing EHR-CR. Replacement or deletion of documents in the EHR-LR may normally only be initiated by the corresponding EHR-CR Source.
- 735        4. When an XDS Document that has already been registered in the XDS Registry of a Clinical Affinity Domain is resubmitted as if it was a new XDS Document with the same Document Unique identifier, this “duplicate submission” is detected by the Repository and/or Registry based on the fact that the XDS Document Unique Identifier already exists in a Document Entry. The Document Registry shall compare the hash key of the resubmitted Document with the hash key of the existing Document. If the hash key matches, the resubmitted XDS Document will be placed in the Repository and a new Document Entry will be created. If the hash key does not match, the submission request  
740        to which that resubmitted Document belongs shall be rejected.

#### 10.4.9 Patient Identification management

Although the central focus of XDS is “documents”, and the sharing of documents, it is critical that each document be reliably associated with the corresponding patient record (or the record target in HL7 CDA).

745 The XDS Registry is not intended to be an authority for patient demographics information. This Integration Profile uses a Patient Identity Source Actor to provide to the XDS Registry a reliable authoritative source of Patient Identifiers for a patient, across the Affinity Domain and time.

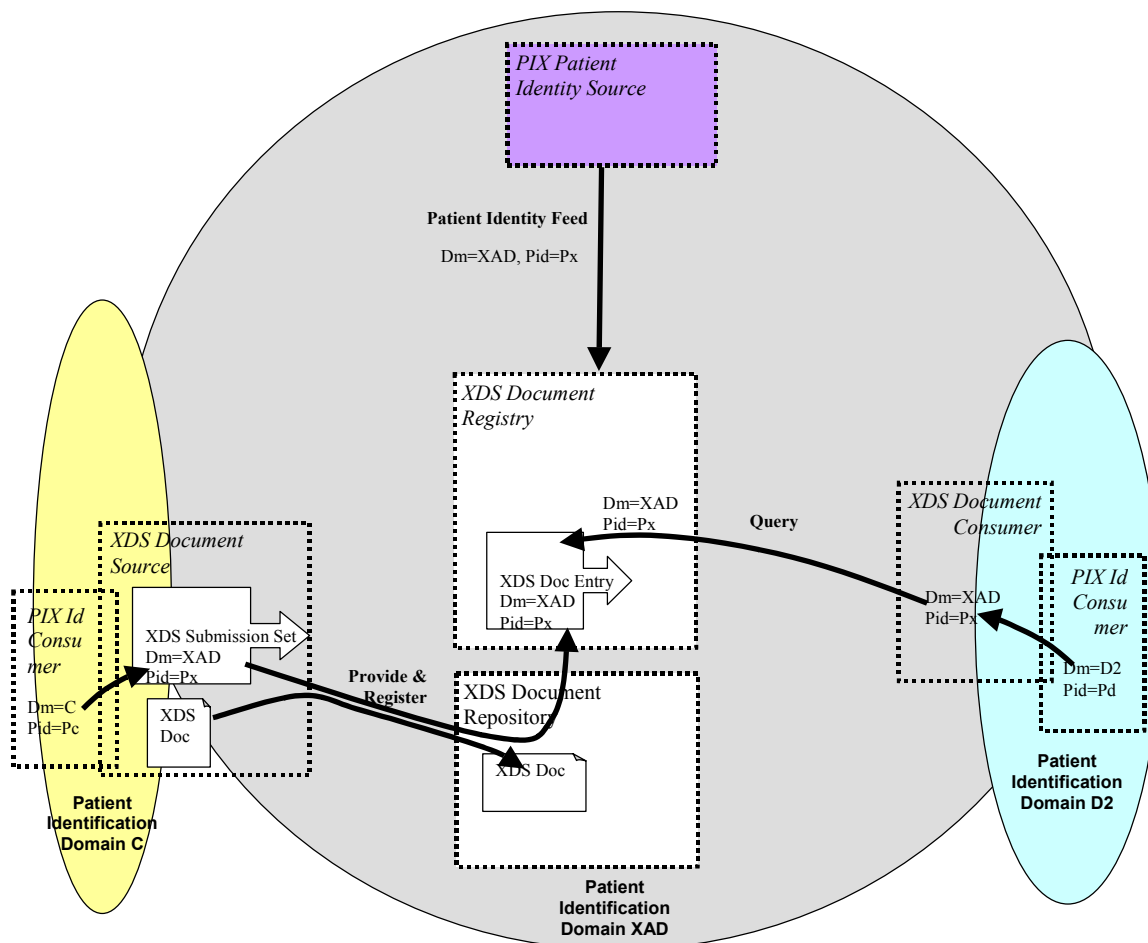
The following principles are defined:

- 750 1. The Patient Identifier Domain managed by the Patient Identifier Source Actor in the Affinity Domain shall be the context for patient identifiers used by the XDS Document Registry to link XDS Documents to a specific Patient. This Patient Identifier Domain is called the XDS Affinity Domain Patient Identifier Domain (XAD-Pid Domain).
2. Submission Requests for Documents related to patients with Identifiers not registered in the XDS Affinity Domain Patient Identifier Domain shall be rejected.
- 755 3. Each Submission Set shall convey the Patient ID in the XAD-Pid Domain. This patient ID is be used to link each document to a patient ID known by the XDS Registry Actor.
4. EHR-CR as a Document Source or Document Consumer may elect to use the XAD-Pid Domain internally or may use its own Patient Identifier Domains. In the later case, the cross-referencing onto the XAD-Pid Domain shall be performed under the responsibility of the Document Source at the time the Submission Set is composed.
- 760 5. A Document Source may choose to perform the cross-referencing of its own patient IDs in that of the XAD-Pid Domain by leveraging the IHE PIX Integration Profile (See Figure). The Patient ID Feed Transaction from the XAD Patient ID Source may be used to provide input to the Patient Identifier Cross-Referencing Manager used by the
- 765 Document Source. The PIX manager may either be internal to the EHR-CRs or be shared across XDS Affinity Domain.
6. All Patient IDs managed in the XDS transactions (either in XAD-Pid Domain or in an EHR-CR Domain) shall include the related Patient Domain ID associated with the patient ID. It is recommended that this unambiguous patient identification be used with Patient
- 770 IDs within the Documents also.
7. Because XDS is Document content neutral, there is no verification by the XDS Repository that the Patient IDs included inside the documents are consistent with the patient IDs managed by the Registry in the document entry related to that document.
- 775 8. The XDS Document Registry will also track the patient ID in the Source EHR-CR Patient Identifier Domains as well the associated demographic info (Surname, Given Name, Sex, Birthdate) for audit and potential check by Document Consumers. But these fields will never be updated and shall not be used as query matching keys.

9. The Document Registry will maintain for any XDS-Document the associated Patient ID in the XAD-Pid Domain. Changes to such Patient IDs may occur under the responsibility of the Patient Identifier Source Actor of the Clinical Affinity Domain:

- When patients' IDs are merged.
- In case of error, when identifying the patient or attributing documents to patients, it may occur that the patient ID in the CAD-Pid Domain changes for a document already submitted.

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



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

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

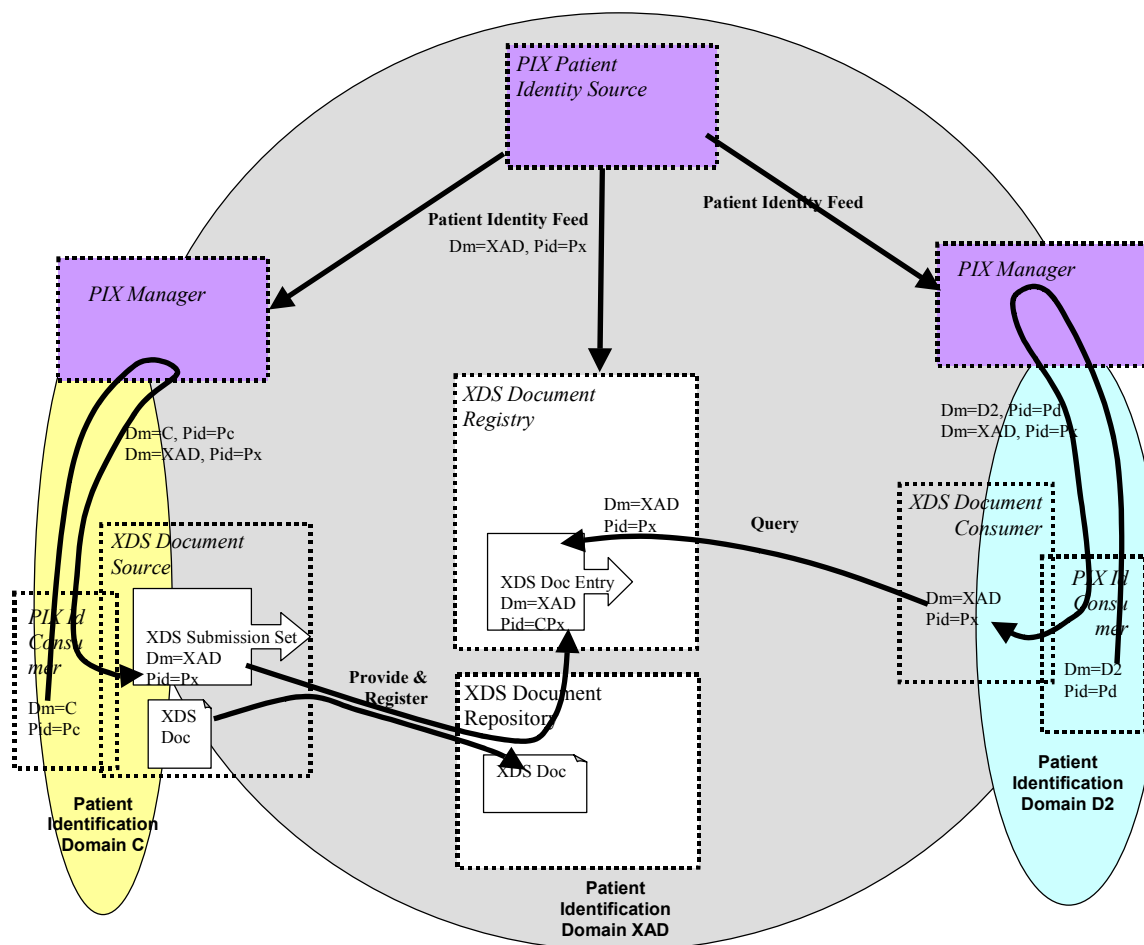


Figure 10.4.9-2 Affinity Domain with patient ID cross-referencing with IHE PIX Managers

#### 10.4.10 XDS Registry Data Model and Attributes

The XDS Integration profile provides means not only to place documents in a repository chosen by the Document Source, but also to place information about this document (or meta-information) in an entry of the Document Registry that manages the Affinity Domain.

The term meta-information reflects that this information is “about” the documents, but not the entire information contained in the document. The fundamental reason for placing this meta-information is to allow finding in a uniform manner one or more such documents by simply

querying the registry. The content and use of this meta-information can be compared to the content of an index card in a library, except that the documents indexed are records for patients in an electronic health domain where predictable queries are necessary.

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

#### 10.4.10.1 XDS Document Registry Data Model

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

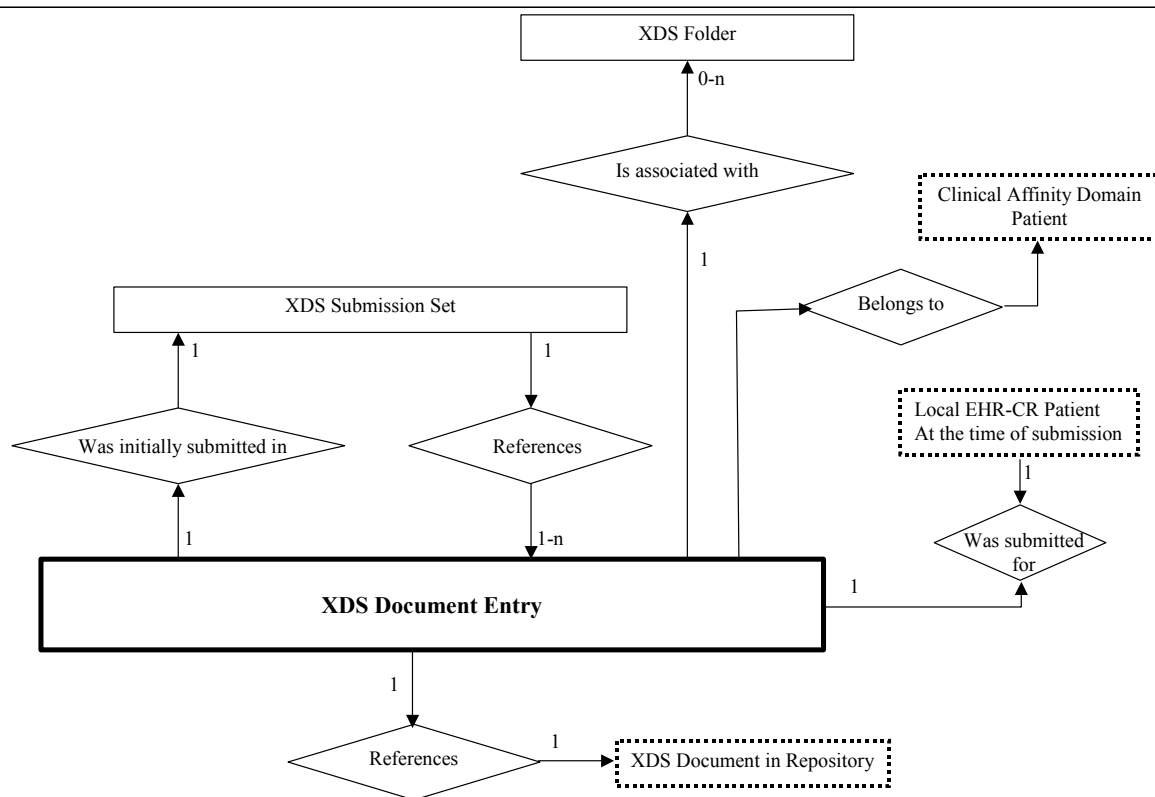
815 **XDS Document Entry:** Information entity managed by a Document Registry Actor that contains a set of meta-data describing the major characteristics of an XDS Document along with a link to the Document Repository Actor where the actual XDS Document may be retrieved.

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

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

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

**XDS Submission Request:** A Submission Request includes one and only one Submission Set, zero or more new XDS Folders and assignment of XDS Documents into new or existing Folders. A Submission Request is processed in an atomic manner by the Document Repository and the Document Registry (i.e. all XDS Documents included or referenced in a Submission Set as well  
835 as the Folders and inclusion of Folders references are registered or none will). This ensures that they are all made available to Document Consumer Actors at the same time.



**Figure 10.4.10-1 XDS Document Registry Data Model**

840

### 10.4.10.2 Attributes of the XDS Document Entries

In this section the attributes of each entity in the above registry data model are identified.

The selection of these attributes and their definitions rely on three primary standards: HL7 CDA Level 1 (CDA Document Header), CEN-EHRCOM and HL7 (Document states). Consideration was also given to the ongoing HL7 CDA Version 2 Document header definition (Dec 2003 Committee Ballot).

845

In the table below, the column “source requirement” states if the attribute is required to be provided by the Document Source at the time of submission.

The column “matching key” states if the attribute is required to be supported by the Registry Actor as a filtering query key when XDS-Documents are queried by a Document Consumer.

850

The column “return key” states if the attribute is commonly used by the Document Consumer when processing query responses. Some attributes are used only as query return attributes, in order to provide enough information to allow the human perusing the query results to decide which documents to retrieve from the Repository.



855 The Attribute name is defined with a prefix such as “XDSDocument” to indicate that this is a document level attribute. Submission set and Folder level attributes are labeled in a similar way.

**Table 10.4.10-2 Attributes of XDS Document Entry**

Attribute	Definition	Source Reqmt	Matching Key	Return Key
XDSDocument.availabilityStatus	<p>An XDS Document shall have one of two availability statuses:</p> <ul style="list-style-type: none"> <li>• Approved</li> <li>• Deprecated</li> </ul> <p>It is always set as Approved as part of the submission of new XDS Documents. It may be changed to Deprecated under the primary responsibility of the Document Source Actor with possible patient supervision.</p> <p>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).</p> <p>This list may be extended in the future.</p>	<p>N/A</p> <p>(It is an operation on the XDS Document Entry)</p>	Required	Commonly checked
XDSDocument.recordTargetId	<p>The recordTargetId represents the patient medical record Identifier as defined by the Document Source Actor. (e.g. Patient Id). This identifier shall be from the Assigning Authority Domain supporting the Affinity Domain in which the Document Registry operates. It shall contain two parts:</p> <ul style="list-style-type: none"> <li>• Authority Domain Id (enforced by the Registry)</li> <li>• An Id in the above domain.</li> </ul> <p>The value of the XDSDocument.recordTargetId shall be the same for all new documents of a Submission Set.</p>	Required	Required	Commonly Used

XDSDocument.uniqueId	<p>(CDA, EHRCOM) 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. This Unique Identifier shall not exceed 128 bytes. The structure and format of this Id shall be consistent with the specification corresponding to the XDSDocumentFormat attribute. (e.g. for a DICOM standard document a 64 character numeric UID, for an HL7 CDA format a serialization of the CDA Document uniqueId plus extension in the form OID+ID, where OID is a 64 digits max, and the ID is a 16 UTF-8 char max).</p> <p>This XDSDocument.uniqueId is intended to respond to the following types of usage:</p> <ol style="list-style-type: none"> <li>1. 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.</li> <li>2. The means to ensure that when a XDS Document is retrieved from the XDS Document Repository using the XDSDocument.URI, the selected XDS Document is the correct one</li> </ol>	Required	Required	Commonly Used
XDSDocument.EntryUUID	The globally unique identifier (may be assigned by either by Source, Repository, Registry) is primarily intended for use as a management identifier (deprecate, delete, references). It shall not be used as a way to externally reference the XDS Document. The XDS DocumentUniqueIdentifier shall be used for that purpose.	N/A	Required	Commonly Used
XDSDocument.URI	The URI of the XDS-Document to be used for retrieval.	N/A	N/A	Commonly Used
XDSDocument.code	(CDA, EHRCOM) The code specifying the particular kind of document (e.g. History and Physical, Discharge Summary, Progress Note). It is preferred that these values be drawn from LOINC. Include scheme and code value in coding scheme.	Required (Affinity Domain vocabulary enforced)	Required	Commonly Used
XDSDocument.codeDisplayName	The name to be displayed for communicating to a human the meaning of the XDSDocument.code	Required	N/A	Commonly Used

# IHE Technical Framework Supplement – Public Comment

XDSDocument.eventCode	<p>(CDA, EHRCOM) Refines, if needed, the XDS-DocumentCode.</p> <p>This represents the main clinical act, such as a colonoscopy or an appendectomy, being documented. In some cases, the event is inherent in the XDSDocument.code, such as a "History and Physical Report" and the procedure being documented is a "History and Physical" act.</p> <p>An event can further specialize the act inherent in the XDSDocument..code, such as where it is simply "Procedure Report" and the procedure was a "colonoscopy". If XDSDocument.eventCode is included, it shall be equivalent to or further specialize the value inherent in the XDSDocument.code, and shall not conflict with the value inherent in the XDSDocument.code, as such a conflict would create an ambiguous situation.</p>	Optional. (No registry enforcement)	Required (Useful for Document Consumer application sub-selection)	Commonly Used for Document Consumer application sub-selection
XDSDocument.EventcodeDisplayNa me	The name to be displayed for communicating to human the meaning of the XDSDocument.eventCode	Required	N/A	Commonly Used
XDSDocument.title	(CDA, EHRCOM) 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 XDSDocument.code (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 XDSDocument.title component shall be used. Max length, 128 bytes, UTF-8.	Optional	N/A	Commonly Used for human sub-selection of relevant documents )
XDSDocument.confidentialityCode	<p>(CDA, EHRCOM) The code specifying the level of confidentiality of the XDS Document. These codes are specific to an Affinity Domain. Enforcement and issues related to highly sensitive documents are beyond the scope of XDS (see security section). This is expected to be addressed in later years.</p> <p>XDSDocument. .confidentialityCode is part of a codification scheme enforced by the Document Registry.</p>	Required	N/A	Commonly Used
XDSDocument.ServiceStartTime	<p>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. This time is expressed as (date/time/UTC).</p> <p>Note: Other times, such as document creation or approval are to be recorded, if needed within the document.</p>	Required	Required	Commonly Used

# IHE Technical Framework Supplement – Public Comment

XDSDocument. 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. 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 XDSDocumentStartTime.	Required	Required	Commonly Used
XDSDocument. languageCode	(CDA) Specifies the human language of character data (whether they be in contents or attribute values). The values of the attribute are language identifiers as described by the IETF (Internet Engineering Task Force) RFC 3066.	Required	N/A	Commonly Used
XDSDocument. authorInstitution	(CDA) Represents a specific healthcare facility under which the human and/or machines authored the document. A specific case is that of care provide as homecare.  <i>Has a sub-structure (e.g. institution name, institution unique Id, etc).</i>	Required (May be unknown)	N/A	Commonly Used
XDSDocument. authorPerson	(CDA) Represents the human and/or machines that authored the document within the XDSDocument.authorInstitution. The document author may be the patient itself.  <i>Has a sub-structure (e.g. person name, unique Id, etc).</i>	Required (May be unknown)	N/A	Commonly Used
XDSDocument. legalAuthenticator	(CDA, EHRCOM) Represents a participant who has legally authenticated or attested the document within the XDSDocument.AuthorInstitution. Legal authentication implies that a document has been signed manually or electronically by the XDSDocument.legalAuthenticator. This attribute may be absent if not applicable.  <i>Has a sub-structure (e.g. person name, unique Id, etc).</i>	Optional	N/A	Commonly Used

# IHE Technical Framework Supplement – Public Comment

XDSDocument. sourceRecordTargetId	<p>The XDSSourceRecordTarget represents the patient medical record Identifier (e.g. Patient Id) in the local patient Identifier Domain of the Document Source Actor. It shall contain two parts:</p> <ul style="list-style-type: none"> <li>• Authority Domain Id</li> <li>• An Id in the above domain (e.g. Patient Id).</li> </ul> <p>This recordTargetId is not intended to be updated once the Document is registered (just as the Document content itself will not be updated without replacing the previous document). As this XDSDocument. sourceRecordTargetId 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 exceptional use for Document Consumer Actors.</p>	Required	N/A	May be used in some cases
XDSDocument. sourceRecordTargetInfo	<p>The sourceRecordTargetInfo represents the patient demographics information to which this document belongs, as the Document Source knew it at the time of Submission.</p> <p>This information in textual form typically includes: Patient Name (Last &amp; First), Patient Sex, and Patient Birth Date. The Clinical Affinity Domain policies may require specific information.</p> <p>This patient information is not intended to be updated once the Document is registered (just as the Document content itself will not be updated without replacing the previous document). As this XDSDocument. sourceRecordTargetInfo 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 exceptional use for Document Consumer Actors.</p>	Required	Optional (This is a multi-value text filled that may be character searchable )	May be used in some cases
XDSDocument. parentDocumentRelationship	(CDA) The type of relationship that the document has with the ParentDocument (e.g. Replace, addendum, or transformation).	Required when applicable	N/A	Commonly Used
XDSDocument. parentDocumentId	<p>(CDA) The identifier of the parent Document entry that represents the source of a document replacement, addendum, or transformation.</p> <p>May identify a document which is unknown by the Document Registry.</p>	Required when XDSDocument. parentDocumentRelationship is present.	N/A	Commonly Used

XSDocument.healthCareFacilityTypeCode	<p>(CDA) This code represents the type of setting of the clinical encounter during which the documented act occurred.</p> <p>In some cases, the setting of the encounter is inherent in the XSDocument.code, such as "Diabetes Clinic Progress Note".</p> <p>HealthCareFacilityTypeCode shall be equivalent to or further specialize the value inherent in the XSDocument.code. For example, where the Document.code is simply "Clinic Progress Note" and the value of healthCareFacilityTypeCode is "cardiology clinic". The value shall not conflict with the value inherent in the XSDocument.code, as such a conflict would create an ambiguous situation.</p>	Required Affinity Domain vocabulary enforced	Required	Commonly Used
XSDocument.formatCode	Code uniquely specifying the format of the document. Along with the XSDocumentCode, it should provide sufficient information to allow any potential XDS Document Consumer Actor to know if it will be capable to process the document. This 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 style sheet).	Required	N/A ?	Commonly Used
XSDocument.size	Size in bytes of the byte stream that was provided in the Register and Provide Transaction and stored by the XDS Repository Actor. This value is computed by the Document Repository Actor and included in the Register Documents Set Transaction.	Required (in the Register Transaction)	N/A	Commonly Used
XSDocument.hash	Hash key of the XDS Document itself. This value is computed by the Document Repository Actor and used by the Document Registry for detecting the improper resubmission of XDS Documents.	Optional	N/A	Commonly Used

#### 10.4.10.3 Attributes of the XDS Submission Set Entries

860

**Table 10.4.10-3 Attributes of XDS Submission Set**

Attribute	Definition	Source Reqmt	Matching Key	Return Key
XDSSubmissionSet.id	Globally unique identifier for the submission-set instance assigned by the Document Source Actor.	Required	Required	Commonly Used
XDSSubmissionSet.sourceId	Globally unique identifier for the instance of the Document Source Actor that contributed the Submission Set.	Required	Required	Commonly Used

XDSSubmissionSet. submissionTime	Point in Time at the Document Source when the Submission Set was created and issued for registration by the Document Source Actor.  This shall be provided by the Document Source (in case of e-mail with significant delay).	Required	Required	Commonly Used
XDSSubmissionSet. contactInfo	Information usable by a human in case there is a need to submit a request for additional information to the Document Source.	Required	N/A	Commonly Used
XDSSubmissionSet. code	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 Affinity Domain.	Required	Required	Commonly Used
XDSSubmissionSet. comments	Comments associated with the Submission Set. Free form text with an Affinity Domain specified usage.	Required	Required	Commonly Used

#### 10.4.10.4 Attributes of the XDS Folder Entries

**Table 10.4.10-4 Attributes of XDS Folder**

Attribute	Definition	Source Reqmt	Matching Key	Return Key
XDSFolder.id	Globally unique identifier for the XDS-Folder in which one or more XDS Documents are placed. It is assigned by the Document Source Actor at the time the XDS Folder is created.	Required	Required	Commonly Used
XDSFolder. lastUpdateTime	Point in Time at the Document Registry when an XDSDocument was registered and placed in the XDS Folder.	N/A	Required.	Commonly Used
XDSFolder. 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 Affinity Domain.  When a new submission request associates XDS Documents (new submission or previously submitted) to an XDS Folder, the Code included in the XDSFolderCodeList 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 a XDS Document is placed in such a Folder	Required	Commonly Used to return entire list.

XDSFolder. codeDisplayNa meList	The list of human readable descriptions of the meaning of each on of the codes present in the XDSFolder.codeList.	Only one code may be assigned to the Folder when a XDS Document is placed in such a Folder	Required	Commonly Used to return entire list.
---------------------------------------	---	--	----------	--------------------------------------

#### 865 10.4.10.5 Document Identification

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

870 The XDS Document Entry includes two separate attributes: a XDSDocument.uniqueId and XDSDocument.URI, a Universal Resource Identifier. The URI is a “self contained” web method that allows any Document Consumer to perform a retrieve operation according to the URI content (See Retrieve transaction, Volume II Section XXXXX). The Document Unique ID is a location independent identifier. As the result of XDS Document migration from one XDS Document Repository to another one within an Affinity Domain, the URI would be changed, but not the Document unique ID.

#### 880 10.4.11 Document Lifecycle

##### 10.4.11.1 Document Availability Status

XDS Document Repository and Registry Actors manage three availability statuses for each XDS Document:

- Approved:** Available for patient care (assumes that it is authenticated, if applicable)
- 885 **Deprecated:** Obsolete, but may still be queried and retrieved
- Deleted:** Obsolete, but shall no longer be present (only a deletion audit trail may remain).

This status is always set as “approved” when an XDS Repository and the XDS Document Registry have successfully processed a submission request.

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



Once submitted with a status of “approved” or available for care, an XDS Document status may be changed to “deprecated” under the primary responsibility of the Document Source Actor with possible patient supervision. It is part of security policies that are beyond the scope of the XDS Integration Profile to have the XDS Repository/Registry enforce this ownership. The reason and responsible party for deprecating a document are tracked as part of the registry audit trail, which is a required capability. Deprecated Documents remain available for Document Consumer Queries. Except for the status change, a deprecated Document Entry meta-data remains the same as when it was in the approved status state.

An Approved or Deprecated Document Entry may have its status changed to “deleted”. This change is associated with the decision to completely remove a document from an XDS Document Repository and its Document Entry from the XDS Document Registry. The Affinity Domain sets the security policies associated with such a special operation.

#### 10.4.11.1 Document Relationships

XDS Documents may be derived from predecessor documents by one of three methods:

- Replacement,
- Addendum or
- Transformation.

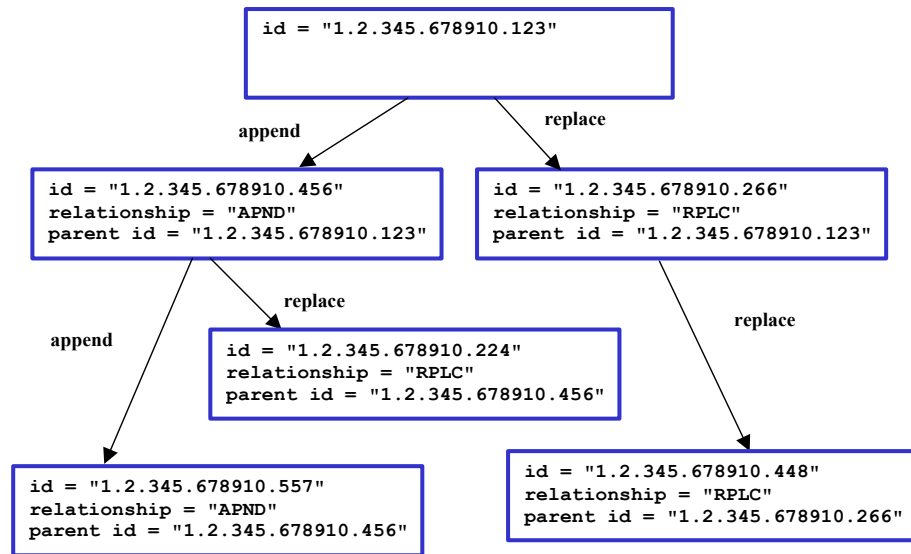
Three types of Parent Relationship are defined to create a record of such a relationship in the XDS Document Registry. The XDSDocument.parentRelationship attribute of such documents contains a code for this relationship. An original document has no parent. Its XDSDocument.parentID and XDSDocument.parentRelationship are thus absent.

A replacement document is a new version of an existing document. The replacement document has a new XDSDocument.ID; its XDSDocument.parentID contains the ID of the Document Entry associated with the previous version of the XDS Document, and XDSDocument.parentRelationship contains the code “RPLC”. The old version shall have its Availability Status changed to Deprecated (i.e. retained for auditing or forensic reasons), or it may be changed to Deleted according to the Affinity Domain policy.

An addendum is a separate XDS Document that references a prior document, and may extend or alter the observations in the prior document. It modifies the parent document, but the parent document remains a valid component of the patient record and remains in the state “approved” or available for care. The addendum XDS Document contains the ID of the previous XDS Document version in XDSDocument.parentID, and its XDSDocument.parentRelationship contains the code “APND”.

A transformed document is derived by a machine translation from some other format. Examples of transformed documents could be CDA documents converted from DICOM Structured Reporting (SR) reports, or a rendering of a report into a presentation format such as PDF. The addendum XDS Document contains the ID of the previous version in XDSDocument.parentID, and its XDSDocument.parentRelationship contains the code “XFRM”. Affinity Domains may define rules that determine whether or not a transformed XDS Document replaces the source,

but typically this would not be the case. If it is, an additional XSDDocument.parentRelationship of type “RPLC” is to be used.



*Adapted from HL7 CDA Release 2*

**Table 10.4.10-5 Example of Document Relationships**

935

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

940

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

945

950

### 10.4.12 Document Query

Query return info shall be either:

- a list of XDS Document Entries

- 955       • a list of XDS Document Entries This would allow a XDS Document Consumer to receive a potentially long list of matching entries and to request them by subsets. The Proposal is to not introduce this more advanced type of queries in this basic XDS Integration Profile.

Query filtering info shall be either:

- 960       • The query matching keys shall be one or more attributes as identified in the Attribute Table above in the column “query matching key” using classical logical operators (=, >, <, AND, OR & NOT).
- It is strongly recommended to limit the matching keys to a small number of primary matching keys flagged in the Attribute Table.

#### **10.4.13 Transport Modes**

- 965       The XDS Integration Profile will provide two modes of transport for all of its transactions where meaningful. In the “on-line mode” the transaction between two actors (computer applications) requires their simultaneous presence (e.g. an HTTP GET). In the “off-line mode” the transaction between the two actors (computer applications) does not require their simultaneous presence (e.g. a store and forward e-mail exchange)
- 970       1. For the on-line mode, the use of an HTTP based protocol is considered with specific XML formatted error codes.
2. For the off-line mode, the use of SMTP Client is considered. Body of the e-mail message should contain a simple notice (in English/ASCII), fixed subject line, address should be used for automated processing. An attachment formatted in the local language should
- 975       contain instructions. Transaction should be included in a separate attachment.

#### **10.4.7.1 Off-Line transaction mode**

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

- 980       The Document Registry should be designed to be on-line all the time (unless grouped with a Document Repository). Therefore, for process flow case 3 (Direct Patient Transfer/Referral) where the Registry and Repository Actors are grouped with the Document Consumer, either on-line or off-line modes may be supported.

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

- (1) Delivery receipts from the end-user, and
- (2) Delivery failure notices from intermediate store-and-forward SMTP servers.

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

This off-line transaction mode will support the Register and Provide/Transfer Transactions. However, the Query Transactions will only use the on-line transport. It is not decided if the Retrieve Transactions will only use the on-line transport or needs an off-line transport mode.

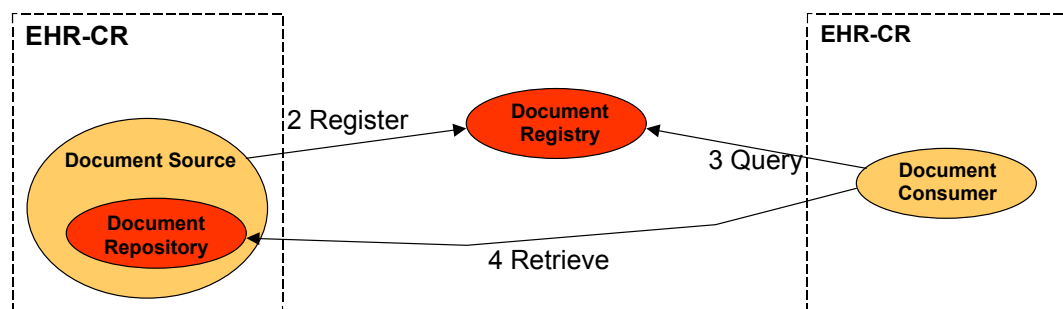
## 10.5 Implementation Strategies

995 The XDS Integration profile addresses three major process flow cases reflecting different groupings of actors within an EHR-CR as well as different configurations of the EHR-LR. This range of use cases reflects the need to accommodate a variety of workflows and configurations. These use cases may coexist in some environments.

1000 ➤ case 1: Repository at the Source. The Document Source Actor is also the Document Repository Actor for the documents it creates and registers in the Document Registry.

When an EHR-CR completes a phase of care for a patient it decides to register a submission-set of documents in a Document Repository Actor with which it is grouped (same system). Then it registers this set of documents (newly created and prior documents of interest) with the Document Registry Actor[2].

1005 Any other Document Consumer Actor may query the Document Registry Actor find out about documents related to all phases of care for the patient [4]. It may choose to retrieve some of these documents from any Document Repository Actor [5].



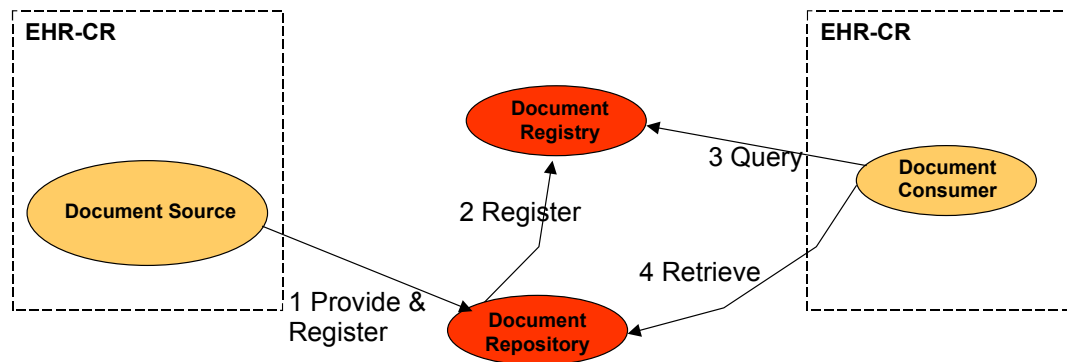
**Table 10.5-1 Implementation Strategy with Repository at the Source**

1010

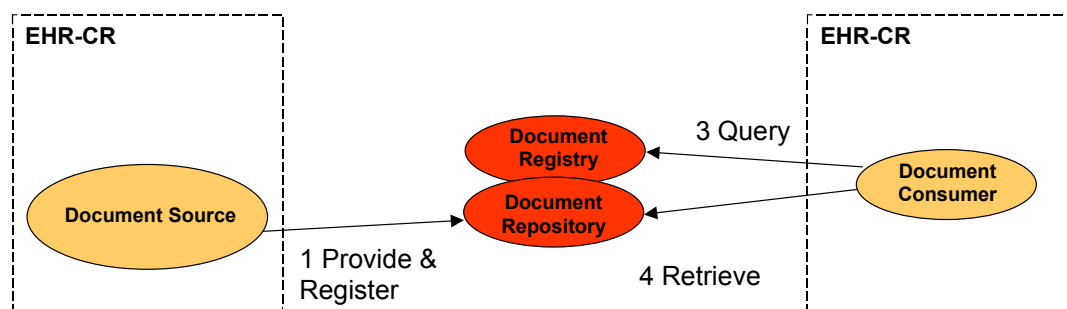
➤ case 2: Third Party Repository. The EHR-CR does not wish to be a Document Repository Actor, but rather uses the services of a third party Document Repository Actor to which it entrusts the documents it creates. First it provides both the registration and the set of documents to this Document Repository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

1015

Any other Document Consumer Actor may query the Document Registry Actor, find out about documents related to all phases of care for the patient [4]. It may choose to retrieve some of these documents from any Document Repository Actor [5].



**Table 10.5-2 Implementation Strategy with 3<sup>rd</sup> party distributed repositories**



**Table 10.5-3 Implementation Strategy with 3<sup>rd</sup> party central repository**

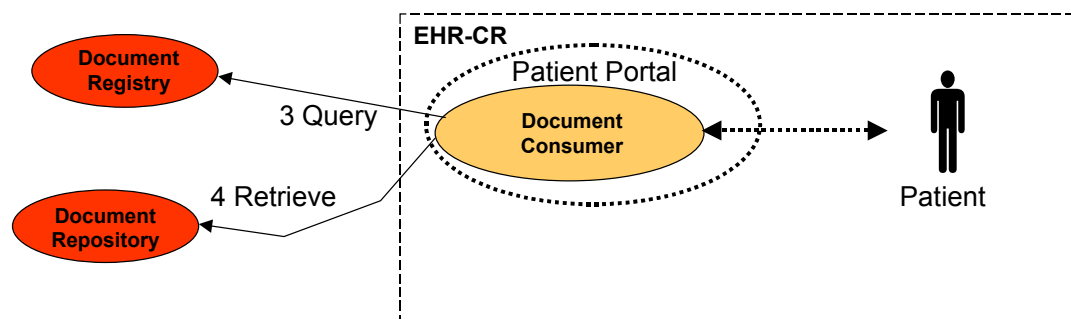
- case 3: Direct Patient transfer-Referral. The Document Source Actor completes a phase of care for a patient. It decides to directly provide and register [1] the set of documents (newly created and prior documents of interest) with a Document Repository [2] that has been grouped along with the Document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

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



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

- case 4: Patient Access. The Document Consumer Actor may also support the patient's access to the patient's own health record with query [3] and retrieve of documents [4]. This is achieved through access via a specific EHR-CR implementation. A patient driven care delivery record (EHR-CR) could be seen as a portal that would provide the specialized application support needed.



**Table 10.5-5 Support of patient Access through a portal**

Such an EHR-CR (Patient Portal) may also be extended to support a Document Consumer grouped with a Document Source to provide more advanced services such as: the self-contribution to own care or home care, or to the patient its record portability between two EHR-LR Affinity Domains.

As it is beyond the scope of the XDS Integration Profile to address the internal implementation of an EHR-CR, the transactions between such a patient portal and the patient are beyond the scope of this Integration Profile.

1055 *Add the following section to Volume 1 of the IHE ITI Technical framework*

## **Appendix XDS-A. XDS Security Environment**

### **Security and privacy**

1060 The coordinating the security and privacy policies of all the affinity group members may be a challenge. An agreement is needed on security procedures, goals, auditing, record keeping, etc. This can result in changes to other enterprise policies, such as human resources procedures. Affinity group members are delegating full responsibility for their published data to the other members of the affinity group. This relationship requires a close ongoing partnership that ensures ongoing maintenance of policies, procedures, and activities. If laws change, relevant policies must be adjusted throughout the group. Corporate changes to group members affect the policies. Security events must be managed as a group. This must be managed as a long-term activity, not a one-time event.

Particular problem areas are likely to be:

- 1070 • Authorized access and modification policies. The details of access policies are likely to have enterprise differences and conflicts that must be resolved. The affinity group relationships also introduce new policy requirements. For example, changes to employment (e.g. employee hiring and firing) must now include suitably rapid notifications to other affinity group members. Changes to privacy restrictions (e.g. divorces) now require full affinity group notifications, not merely enterprise notifications.
- 1075 • Audit trail and access record keeping are often quite sensitive internal enterprise activities that must now be appropriately coordinated with the full affinity group.
- Changes to laws and regulations now affect not only the policies of the individual enterprises; they also must be reflected in the affinity group relationship contracts, policies, and procedures.
- 1080 • Patient access and patient identity management. Patients usually have insecure computers. Patients often object to security procedures.
- Transborder communication of PHI presents legal and regulatory issues.

Appendix A in volume II goes into more detail listing many of the threats, objectives, policies, and mitigations that need to be coordinated among affinity group members.

1085

## Volume 2 – Transactions

### Open Issues – XDS Volume 2

1. Appendix XDS-B – Registry Initialization and XDS-CZ – Affinity Domain Initialization need to be written.
2. Pull together requirements for XDS registry adaptor function (volume 2 material?)
3. Need date/time format (Is XML Schema format ok ?)
4. Complete class diagram in “real UML”.
5. Need new transactions for Deprecate and Delete
6. Need two appendices with XML Schema for Provide&Register (Appendix XDS-D) and Query Response (Appendix XDS-E) transactions.
7. The Query Transaction supports a broad range of uses. Future extensions to this profile may introduce restrictions or specified the use of canned queries. Proposals for simplification of the search mechanism are requested.
8. It has not been resolved, if Document Source and Document Repository Actors shall be offered the option to choose to implement either one or both of those protocol selections, or if one of them should be required. Input is sought.

*Add the following section to Volume 2 of the IHE ITI Technical framework*

### 1090 3.14 Register Document Set

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

#### 3.14.1 Scope

1095 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:

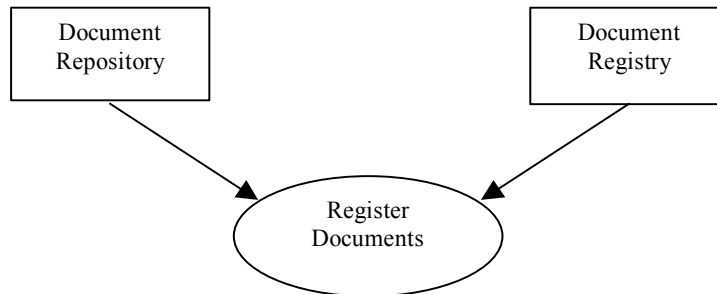
- Metadata describing zero or more new documents
- XDS Submission Set definition along with the linkage to new documents and references to existing documents

1100



- XDS Folder definitions along with linkage to new or existing documents

### 3.14.2 Use Case Roles



1105 **Actor:** Document Repository

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

**Actor:** Document Registry

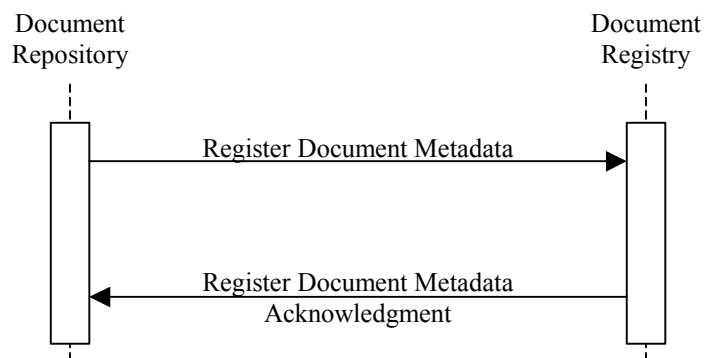
**Role:** A document indexing system that receives and stores document metadata.

### 3.14.3 Referenced Standards

1110	ebRIM	OASIS/ebXML Registry Information Model v2.0
	ebRS	OASIS/ebXML Registry Services Specifications v2.0
	HTTP	HyperText Transfer Protocol HTTP/1.1 (IETF RFC2616)
	CDA	HL7 Clinical Document Architecture
	EHRcom	EHR Communication Standard – CEN 13606

1115

### 3.14.4 Interaction Diagram



### **3.14.4.1 Register Document Metadata**

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

#### **1120 3.14.4.1.1 Trigger Events**

The Register Document Metadata message is triggered when:

1. A Document Repository wants to register metadata for a set of documents it holds.
2. The Repository Actor receives a Provide and Register transaction (ITI-15)

#### **3.14.4.1.2 Message Semantics**

1125 The following sections specify the mapping of XDS concepts to ebRS and ebRIM semantics:

1. Document
2. Submission Request
3. Submission Set
4. Folder
5. Document Relationships

1130

Metadata definitions to support the above are discussed as follows:

6. Document
7. Submission Request
8. Submission Set
9. Folder

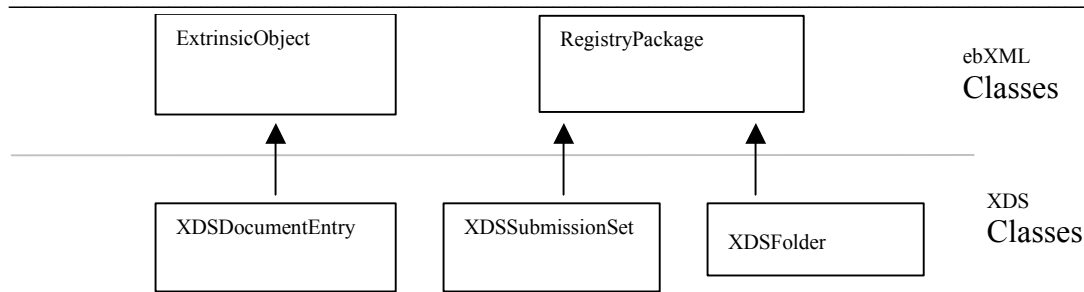
1135

In addition the following topics are discussed:

10. Protocol requirements
11. XDS registry adapter function
12. Security Requirements

#### **1140 3.14.4.1.2.1 Class Diagram**

*Editors note: This diagram is to be replaced by a UML diagram.*



**Figure 3.14.1-1 ebRIM Class Diagram of the Register Document Metadata**

1145 The XDSDocumentEntry class is derived from the ebRIM ExtrinsicObject class. The XDSSubmissionSet and XDSFolder classes are derived from the ebRIM RegistryPackage class. Since the ebRIM standard does not allow for subclassing the RegistryPackage class, these two classes are implemented as RegistryPackage with respectively XDSSubmissionSet and XDSFolder classifications.

#### 3.14.4.1.2.1 Document Specification

1150 A new registry object type is declared as a subclass of ExtrinsicObject. Its name is XDSDocumentEntry. An object of this type in the XDS registry is used to represent a document in an XDS repository.

1155 An XDSDocumentEntry object in the registry contains a reference to a single document in a single repository. Every document held in a cooperating repository is represented by a single XDSDocumentEntry in the registry.

Note: A repository may hold documents that are not indexed in the registry.

Appendix XDS-B defines the metadata to initialize an ebXML registry to serve as a XDS registry.

#### 3.14.4.1.2.2 Submission Request Specification

1160 This section applies to both the Register Document Set transaction and the Provide and Register Document Set transaction.

A Submission Request is the collection of information that is transferred to an XDS Document Registry or Repository.

1165 Appropriate protocol bindings used to transfer this content between systems are described in section 3.14.4.1.2.10.

There are two types of submission requests: Registry Submission Request and Repository Submission Request.

##### 3.14.4.1.2.2.1 Registry Submission Request

1170 A Registry Submission Request is the collection of metadata transferred between a Document Repository Actor and a Document Registry Actor in a single SubmitObjectsRequest. This request contains:

- A collection of metadata to be stored in the registry
- A single Submission Set, contained within the metadata, organizing the metadata

This request is part of the Register Document Set transaction.

#### 1175 **3.14.4.1.2.2.2 Repository Submission Request**

A Repository Submission Request is the collection of metadata and documents transferred between a Document Source Actor and a Document Repository Actor in a single SubmitObjectsRequest. This request contains:

- A collection of metadata to be stored in the registry
- 1180 • A single Submission Set, contained within the metadata, organizing the metadata
- Zero or more documents; each document is represented by an XDSDocumentEntry object in the metadata

This request is part of the Provide and Register Document Set transaction that is specified in Section 3.15.

1185 Unless otherwise stated, the Submission Set requirements specified hereafter apply to both types of Submission Requests

#### **3.14.4.1.2.2.3 Atomicity Requirements for Submission Requests**

1190 Submission requests are atomic operations. The result of a Submission Request is to update 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 is managed by a XDS registry adaptor function through a state transition using the status attribute, specifically using the default value of **Submitted** and then the value **Approved** for the following three kinds of objects:
  - XDSSubmissionSet (RegistryPackage object type)
  - 1195 • XDSFolder (RegistryPackage object type)
  - XDSDocumentEntry (subclass of ExtrinsicObject)
2. Other types of registry objects can be included in Submission Requests. If an error occurs storing documents in the repository then all documents stored as part of the Repository Submission Request may be removed.
- 1200 3. If an error occurs storing metadata in the registry then:
  - All metadata stored as part of the Registry Submission Request is removed from the registry
  - All documents stored as part of the Repository Submission Request may be removed. This only applies if the Registry Submission Request is a result of a
  - 1205 Repository Submission Request.
4. Registry queries from the Registry Query transaction shall not find Submission Sets or XDSDocumentEntry objects until after the atomic operation that creates them has

1210 completed successfully. This shall be accomplished by setting the **status** attribute to **Approved** on the Submission Set object and on each XDSDocumentEntry object contained within the Submission Set.

1215 **Note:** There are two common implementation scenarios for rolling back a Submission Request atomic transaction. 1) The registry adaptor function (Internal to The XDS Registry Actor) generating the submission has maintained a list of object UUIDs that make up the Submission Request and can use the list to delete from registry and 2) registry adaptor function (Internal to The XDS Registry Actor) generating the submission has not maintained state and must discover through query the UUIDs of the Submission Set and its contents.

#### 3.14.4.1.2.2.4 Other Properties of Submission Requests

A Submission Request may contain metadata beyond the Submission Set and XDSDocumentEntry objects:

- 1220 • XDSFolder objects
- Associations linking XDSDocumentEntry objects to XDSFolder objects. There are no restrictions on whether the XDSDocumentEntry objects or XDSFolder objects are in this Submission Request.
- 1225 • Associations linking existing (already contained in the registry) XDSDocumentEntry objects to the Submission Set RegistryPackage contained in this Submission Request. If such an association is included then it shall not have a slot named SubmissionSetStatus. The use of this slot is restricted by the definition of Submission Set below.
- Other associations and classifications not described above.

1230 **Note:** Associations linking XDSFolder objects into other XDSFolder objects creating a hierarchy of folders may or may not be within the scope of this Integration Profile.

#### 3.14.4.1.2.3 Submission Set Specifications

Submission Sets exist for these reasons:

- 1235 • Make a permanent record in the registry of XDSDocumentEntry objects that were submitted together.
- Attach a set of attributes to this submission.
- Allow the inclusion of existing XDSDocumentEntry objects that are relevant to the context defined by the attributes of the submission.

1240 Submission Sets provide support for the management of the atomicity requirements imposed by Submission Requests. When an XDSDocumentEntry object is submitted as part of a Submission Set it shall include an association object to link it to the Submission Set. This association object shall have a slot named **SubmissionSetStatus** with value **Original**. This differentiates this association from one that is created to link an existing document into a Submission Set as is discussed next.

1245 It is possible to resubmit old documents as part of a Submission Set. There are several conditions that result:

- 1250 • An existing XDSDocumentEntry object is to be linked into the XDSSubmissionSet. This happens when an older document (document metadata already contained in the registry) has been found that has relevance to this Submission Set and the context defined by the attributes attached to the Submission Set. This is represented in the current Submission Request as an Association object that links this existing XDSDocumentEntry to this Submission Set.
- 1255 • A document with its associated metadata is 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. This is a duplicate encoding/recording of a document, which is acceptable within this profile.
- 1260 • A document with its associated metadata is part of a Repository Submission Request. A document with the same XDSDocument.uniqueID is present in the repository but the XDSDocument.hash is different. This is an error and the Submission Request shall be rejected.
- A document with its associated metadata is part of a Registry Submission Request. A XDSDocumentEntry object with the same XDSDocument.uniqueID is present in the registry but, the XDSDocument.hash is different. This is an error and the Submission Request shall be rejected. [XDS registry adaptor function]
- 1265 An XDS SubmissionSet is a RegistryPackage, classified as XDSSubmissionSet that is used to bundle XDSDocumentEntry objects.

#### 3.14.4.1.2.4 Folder Specification

An XDS Folder is a RegistryPackage, classified as XDSFolder that is used to bundle XDSDocumentEntry objects.

- 1270 XDS Folder objects are not part of a Submission Set, so there is no linkage between XDSSubmissionSet objects and XDSFolder objects.

#### 3.14.4.1.2.5 Document Relationships

- 1275 XDS Documents may be derived from predecessor documents by one of three methods: Replacement, Addendum or Transformation. The XDSDocument.parentDocumentRelationship of such documents contains a code for this relationship. This code is equivalent to the HL7 CDA Release 1 as document\_relationship.code, and in CDA Release 2 drafts as relatedDocument.typeCode. The enumerated value set for XDSDocument.parentDocumentRelationship is presented below:

1280 **Table 3.14.4.1-1 Value set for relatedDocument.typeCode (CNE)**

Code	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.

*Adapted from HL7 CDA Release 2, Committee Ballot 2*

See ITI TF-1: 10.4.11.1 for further detail on the use and meaning of document relationships.

### 3.14.4.1.2.6 Document Definition Metadata

1285 The XDSDocumentEntry object type is created by adding a new ClassificationNode to the ObjectType Classification Scheme<sup>2</sup>.

The XDSDocumentStub object type is created by adding a new ClassificationNode to the ObjectType Classification Scheme. See XDSDocument.parentDocumentRelationship attribute in table below for background.

1290 The following metadata elements are used to describe an XDS Document. They are provided by the Document Source Actor in the Provide and Register Document Set transaction. They are provided by the Document Repository Actor in the Register Document Metadata transaction if this transaction is used outside the context of a Provide and Register Document Set transaction.

Each attribute shown below is an attribute on the XDSDocumentEntry object.

1295 Volume 1 of this supplement (ITI TF-1: 10.4.10.2) specifies which attributes are required and which are optional.

**Table 3.14.4.1-2 Document Metadata Attribute Definition**

XDS Attribute Name	EbRIM Attribute Type	Comments
XDSDocument.availabilityStatus	ebRIM Status attribute	Use existing status attribute: <b>Approved:</b> Available for patient care <b>Deprecated:</b> Obsolete
XDSDocument.recordTargetId	External Id	This is the XDS Affinity Domain patient identifier. This is coded as OID+PatientId (the two strings separated with a "+" character). OID is 64 characters ASCII (numeric plus period). PatientId is 64 bytes UTF-8.

<sup>2</sup> The specific requirement in ebRIM that object types be user extendable was introduced after version 2.0.

XDSDocument .uniqueId	External Id	Assigned by Document Source. Size limited to 128 bytes (printable characters only). See section 3.14.4.1.2.6.2 for the specification of the format and encoding depending on the document standard used for the XDS Document content.
XDSDocument .documentEntryUUID	ebRIM specified internal UUID	
XDSDocument.URI	External Link	External Link name is XDSDocument.URI to be used for retrieving the document from the Repository (ITI-17 Retrieve Document transaction)
XDSDocument .code	External Classification	Enforcement happens in XDS registry adaptor function.
XDSDocument.codeDisplayNa me	Slot	
XDSDocument .eventCode	External Classification	XDS Affinity Domain specific
XDSDocument .eventCodeDisplayName	Slot	XDS Affinity Domain specific
XDSDocument.title	ebRIM Title attribute	
XDSDocument .confidentialityCode	External Classification	XDS Affinity Domain specific
XDSDocument .serviceStartTime	Slot	For point in time this holds serviceTime. Time encoding format must sort correctly as a string. Time encoding format is XMLSchema dateTime format. Example: 2004-12-25T23:50:50.
XDSDocument .serviceStopTime	Slot	For point in time this holds serviceTime, the value shall be same as serviceStartTime. XDS registry adapter function verifies serviceStartTime <= serviceStopTime.
XDSDocument .languageCode	Slot	XDS Affinity Domain specific
XDSDocument.authorInstitution	Slot	HL7V2 XON data type (Slot object limits length)
XDSDocument .authorPerson	Slot	HL7V2 XCN data type (Slot object limits length)
XDSDocument .legalAuthenticator	Slot	Multivalued slot. Substructure comes from HL7 V2 serialization. (XCN)
XDSDocument .sourceRecordTargetId	Slot	OID+extension (cf. XDSDocument. recordTargetId)
XDSDocument .sourceRecordTargetInfo	Slot	UTF-8, Multi-valued. XDS Affinity Domain specific.



XDSDocument.parentDocumentRelationship	Association Type	Extends Association types with 3 new values (APND, RPLC, XFRM). RPLC could be encoded with registry Replaces, others need to be custom.
XDSDocument.parentDocumentId	Association	If parent document is in registry then code as association. If not then create stub document object to anchor other end of association. Create new object type XDSDocumentStub to support this. Meaning: document stub represents document metadata that is not in registry but need an object to point at to support parentDocumentRelationship. This association is coded with a type from parentDocumentRelationship.
XDSDocument.healthCare FacilityTypeCode	External Classification	XDS Affinity Domain specific
XDSDocument.formatCode	External Classification	XDS Affinity Domain specific
XDSDocument.size	Slot	Size in Bytes of the document as retrieved from the URI.
XDSDocument.hash	Slot	Uses SHA1 hash algorithm.

#### 3.14.4.1.2.6.1 XDSDocument.formatCode

1300 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 XDSDocument.formatCode. This code will identify document format parameters, e.g., MIME type, necessary for interoperability. Rules about handling the formatCode are necessary but are not imposed by this profile. In the future IHE content specific Integration Profiles may be created  
1305 that specify these rules.

For more detail see definition of XDSDocument.formatCode in section 10.4.10.2 of Volume 1.

#### 3.14.4.1.2.6.2 XDSDocument.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+ optional extension ID for HL7 CDA, SOP  
1310 Instance UID for DICOM composite objects). This attribute shall not to exceed 128 bytes that should be used as an opaque (Document Consumers, Registries, Repositories shall not attempt to interpret its content) and globally unique identifier for the XDS Document.

#### 3.14.4.1.2.7 Submission Request Metadata

1315 Table 3.14.4.1-3 Submission Request Metadata Attribute Definitions

Attribute	Attribute Type	Comments
RegistryEntry.status	String	The ebXML registry status attribute is used to manage transactions required by Submission Requests.

### 3.14.4.1.2.8 Submission Set Metadata

1320 The following metadata elements are used to describe an XDS Submission Set. They are provided by the Document Source Actor in the Provide and Register Document Set transaction. They are provided by the Document Repository Actor in the Register Document Metadata transaction if this transaction 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 Submission Set.

1325 Volume 1 of this supplement specifies which attributes are required and which are optional.

**Table 3.14.4.1-4 Submission Set Metadata Attribute Definitions**

Attribute	Attribute Type	Comments
XDSSubmissionSet.Id	External Id	
XDSSubmissionSet.SourceId	External Id	
XDSSubmissionSet.submission Time	Slot	Time encoding format is XMLSchema dateTime format. Example: 2004-12-25T23:50:50.
XDSSubmissionSet.ContactInfo	Slot	Multi-valued, UTF-8. Used by XDS Affinity Domain.
XDSSubmissionSet.code	External Classification	XDS Affinity Domain specific
XDSSubmissionSet.comments	ebRIM Description attribute	Use specific to XDS Affinity Domain

### 3.14.4.1.2.9 Folder Metadata

1330 The following metadata elements are used to describe an XDS Folder. They are provided by the Document Source Actor in the Provide and Register Document Set transaction. They are provided by the Document Repository Actor in the Register Document Metadata transaction if this transaction 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.

1335 Volume 1 of this supplement specifies which attributes are required and which are optional.

**Table 3.14.4.1-5 Folder Metadata Attribute Definitions**

Attribute	Attribute Type	Comments
XDSFolder.id	External Id	
XDSFolder.lastUpdateTime	Slot	Value maintained by XDS registry adaptor function. Time encoding format is XMLSchema dateTime format. Example: 2004-12-25T23:50:50.
XDSFolder.codeList	External Classification(s)	Multi-Valued. XDS Affinity Domain specific
XDSFolder.codeDisplayNameList	Slot	Multi-valued. Each value is coded as first three components of CWE datatype. CWE datatype includes code from above codeList.

### 3.14.4.1.2.10 Protocol Requirements

1340 SOAP with Attachments shall be used as the protocol between the Document Repository and the Document Registry.

### 3.14.4.1.2.11 XDS Registry adapter function

*Editor: Need to refine text of this section and pull together all requirements for XDS registry adaptor function and clarify if this is volume 2 material.*

1345 The XDS registry adaptor function is a set of functions that are not intrinsic to an ebXML registry, but specified by XDS in order to support healthcare specific adaptations. It is beyond the scope of IHE to specify such a registry adaptor implementation in relationship to ebXML implementations. It is only identified to facilitate the understanding of XDS by readers familiar with ebXML. This adaptor function includes the following:

- Accept Patient Identity Feed transactions from Patient Identity Source Actor
- 1350 • Validate in Register Document Set Transactions that XDSDocument.recordTargetId (Patient IDs) are using a registered patient identifier domain and if in the XDS Affinity Domain patient Id domain, that the patient is known.
- Validate in Register Document Set Transactions that submitted metadata meets XDS Registry specification
- 1355 • Validate in Register Document Set Transactions that submitted metadata meets XDS Affinity Domain enforced specification (e.g. Code values managed as External Classifications).
- Ensure that metadata stored as part of the Registry Submission Request is removed from the registry if the SubmitObjectRequest to the registry fails. (See ITI TF-2: 3.14.4.1.2.2.3
- 1360 Atomicity Requirements for Submission Requests).

#### **3.14.4.1.2.12 Security Requirements**

This 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 affinity domain Audit Repository Actor.

- 1365 The use of of ATNA along with XDS does require that each member of the Affinity Domain does have audit and security mechanisms in place. See appendix ITI TF-1: Appendix XDS-A and ITI-TF-2: Appendix XDS-F.

Note: The ATNA Integration Profile is under Public Comment along with XDS until July 15<sup>th</sup>.

#### **3.14.4.1.3 Expected Actions**

- 1370 Upon receipt of a Register Document Metadata message, the Document Registry shall do the following:

- Accept all valid SubmitObjectsRequests (perform adaptor function validation) and store the contained metadata in the registry as per [ebRIM][ebRS].
- Update the registry with the contained metadata
- 1375 • Return a RegistryResponse message given the status of the operation.

If the registry rejects the metadata then:

- An error is returned
- The error status includes an error message
- The request is rolled back

#### **1380 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 responds with:

- Register Document Metadata Acknowledgment

- 1385 This message corresponds to the RequestResponse message defined in ebRS.

##### **3.14.4.2.2 Message Semantics**

The RequestResponse ebRS 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.

##### **1390 3.14.4.2.3 Expected Actions**

There are no expected actions.



---

*Add the following section to Volume 2 of the IHE ITI Technical framework*

---

### 3.15 Provide&Register Document Set

1395 This section corresponds to Transaction ITI-15 of the IHE Technical Framework.  
Provide&Register Document Set is used by the Document Source Actor to provide a set of documents to the Document Repository Actor and to request that the repository store these documents and then register them with the Document Registry Actor.

1400 The Provide&Register Document Set transaction covers only the interaction between the Document Source and Document Repository Actors. The interaction between the Document Repository and the Document Registry is described separately in the Register Document Set Transaction (ITI-14).

1405 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 Repository and XDS Registry is hidden.

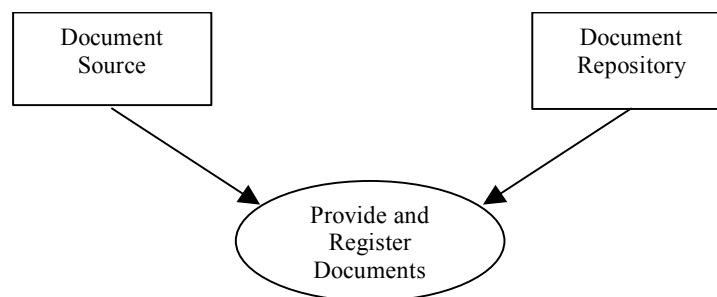
#### 3.15.1 Scope

The Provider&Register Document Set transaction passes a Repository Submission Request (see ITI TF-2: 3.14.4.1.2.2.2) from a Document Source to a Document Registry Actor.

1410 A Provider and Registry 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
- Folder definitions along with linkage to new or existing documents
- 1415 • 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.

1420 **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
- Forwards the enhanced metadata to the Document Registry.

1425

### 3.15.3 Referenced Standards

ebMS OASIS/ebXML Messaging Services Specifications v2.0

ebRIM OASIS/ebXML Registry Information Model v2.0

ebRS OASIS/ebXML Registry Services Specifications v2.0

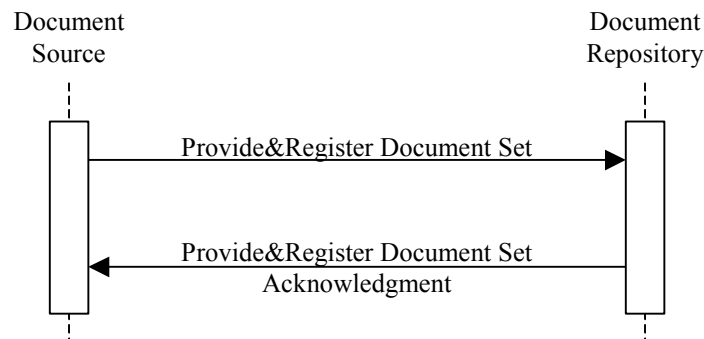
1430 HTTP HyperText Transfer Protocol HTTP/1.1 (IETF RFC2616)

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



1435

#### 3.15.4.1 Provide&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.

##### 1440 3.15.4.1.1 Trigger Events

The Document Source Actor, 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 Repository Actor and
- The associated metadata to the Document Registry.

1445 **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)

1450 **3.15.4.1.2.1 Metadata**

The Register Document Set message shall include the metadata attributes (as defined in section 3.14.4.1.2.6) that will be forwarded by the XDS Document Repository Actor to Registry Actor using the Register Document Set Transaction (ITI-14). Volume 1 (ITI TF-1: 10.4.10.2) specifies which attributes are required and which are optional.

1455 The Document Source supplies all necessary registry object attributes with the exception of the **XDSDocument.URI** attribute of an XDSDocumentEntry that must be assigned by the Document Repository. Therefore, the Document Repository Actor must add this attribute to the metadata before initiating the Register Document Metadata transaction to the registry.

**3.15.4.1.2.2 Security Requirements**

1460 Relevant security requirements are discussed in the Register Document transaction (see ITI TF-1: 3.14.4.1.2.12).

**3.15.4.1.2.3 Protocol Selection**

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

- 1465
- On-line – the Document Source Actor constructs a direct connection (i.e, socket) to the Document Repository Actor.
  - Off-line – the Document Source Actor connects to the Document Repository via SMTP.

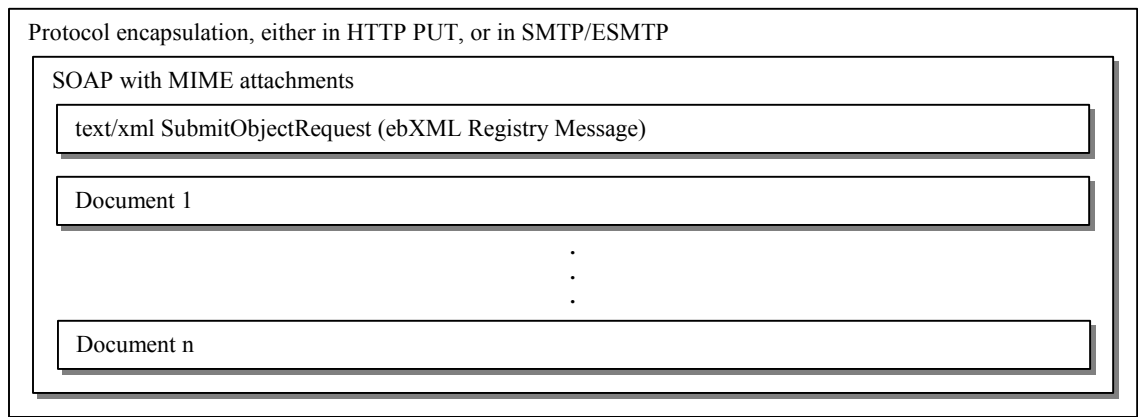
Note: It has not been resolved, if Document Source and Document Repository Actors shall be offered the option to choose to implement either one or both of those protocol selections, or if one of them should be required.

1470 **3.15.4.1.2.3.1 On-Line Protocol Binding**

**3.15.4.1.2.3.1.1 General structure and header**

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**

### 3.15.4.1.2.3.1.1 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 documents<sup>3</sup>.

The multipart packaging transmits the MIME-type of each part. The metadata part must be of type text/xml. Parts containing documents destined for the Document Repository can have any MIME type, either single part or multipart (see Annex XX Managing Multipart Documents). 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 ExtrinsicObjects. An ExtrinsicObject is a registry object that represents a repository document within the registry. Each ExtrinsicObject will contain an id attribute. The value of the id attribute will match exactly one Content-Id header in one part of the multipart package. This is how metadata is linked to an associated document within the message.

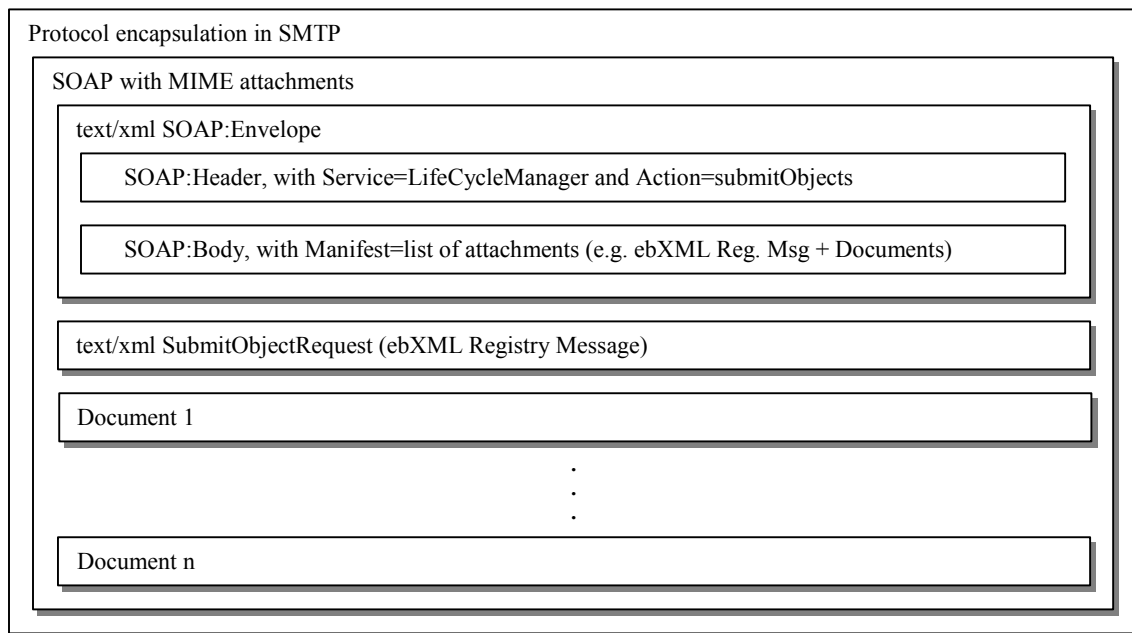
### 3.15.4.1.2.3.2 Off-Line Protocol Binding

#### 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

<sup>3</sup> 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.

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.



**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.
- 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 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 of the ebMS header is UTF-8.

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

- 1525 • 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	Description
eb:From/eb:PartId	Identification of the message sender (its email address, preceded by <a href="#">mailto:</a> )
eb:From/eb:Role	<a href="http://www.ihe.net/roles/iti/xds/DocumentSource">http://www.ihe.net/roles/iti/xds/DocumentSource</a>
eb:To/eb:PartId	Identification of intended recipient of the message (its email address, preceded by <a href="#">mailto:</a> )
eb:To/eb:Role	<a href="http://www.ihe.net/roles/iti/xds/DocumentRepository">http://www.ihe.net/roles/iti/xds/DocumentRepository</a>
eb:CPAId	Identification of a Collaboration Protocol Agreement between the sender and receiver. This will 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:PartId and the eb:To/eb:PartId, separated by the hyphen character (-).
eb:ConversationId	In the absence of a local trading partner agreement, must 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 submissionSet (corresponds to the XDSSubmissionSet Title).

eb:AckRequested	Optional in ebMS, required here to indicate the repository shall acknowledge the message. This element has the following attributes: SOAP:mustUnderstand="1" eb:version="2.0" eb:signed="false"
-----------------	---

- 1530
- List of references to document, in /SOAP:Envelope/ SOAP:Header/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, <a href="#">cid:</a> 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 <a href="http://www.ihe.net/roles/iti/xds/SubmitObjectsRequest">http://www.ihe.net/roles/iti/xds/SubmitObjectsRequest</a>
eb:Schema	Shall be present only for the first reference, and has following attributes: eb:location= <a href="http://www.ihe.net/schemas/iti/xds/SubmitObjectsRequest">http://www.ihe.net/schemas/iti/xds/SubmitObjectsRequest</a> eb:version=1.0
eb:Description	To be set to the XDSDocument.title. However, for the first reference, shall be set to the meaning of SubmitObjectsRequest in the local language (i.e. lang="en-GB", "Provide and Register Document Set Metadata").

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

### 1535 3.15.4.1.2.3.2.2 Associated documents

See the section "Associated documents" in the On-Line Binding (ITI TF-2: 3.15.4.1.2.5.2). 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.

### 3.15.4.1.3 Expected Actions

- 1540 The Document Repository Actor will receive this off-line message. Each document within the message will be stored into the repository. A detected failure will result in an error result message being returned to the Document Source Actor thus terminating this transaction.

As each document is stored into the repository one identifiers must be created:

1. A URI that can be used to reference the document via an HTTP service.

1545 The Document Repository Actor will modify the received registry metadata. Each ExtrinsicObject, which represents a document deposited in the repository, will have added to it the above URI. A Register Document Set transaction will be issued to the XDS Document Registry.

#### **3.15.4.2 Provide&Register Document Set Acknowledgment**

1550 The Document Repository sends a Provide&Register Document Set Acknowledgment when the processing of a Provide&Register Document Set is complete. This message is identical to the RegistryResponse message specified in ebRS. It SHALL be conveyed in the same protocol than the request (On-Line vs. Of-Line).

##### **3.15.4.2.1 Trigger Events**

1555 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

1560 • 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.

1565 Additional relevant semantics for both the repository and registry are described in the Register Document Set transaction.

##### **3.15.4.2.3 Expected Actions**

There are no expected actions.

---

*Add the following section to Volume 2 of the IHE ITI Technical framework*

---

### 3.16 Query Registry

1570 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.

1575       Note:     This is a very general query mechanism that allows very broad use. Future extensions to this profile may introduce restrictions or specified the use of canned queries. Proposals for restricting the search mechanism are requested.

#### 3.16.1 Scope

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

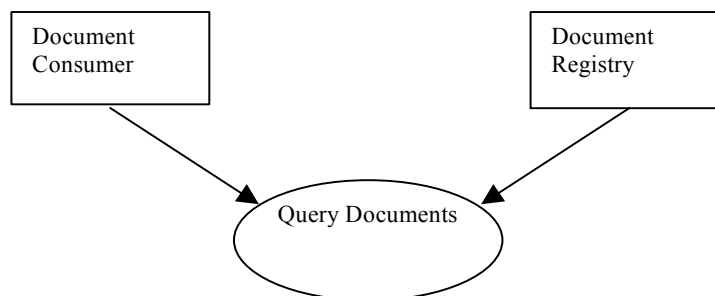
- 1580       • Query by patient (Id) for a time interval, by document type(s), by practice setting(s), by authoring physician (Id)
- Query by Document Source
- Query for XDS Folders updated during a time interval
- Query for all documents in a Folder or Submission Set
- Query by time of submission

1585 Any metadata defined in this profile (see section ITI TF-1: 10.4.10.1, XDS Registry Entry Attributes) can be the target of a query. This transaction will document the basic syntax and semantics of XDS Registry Queries.

All queries return lists of metadata or registry UUIDs of XDS Document Entries.

#### 3.16.2 Use Case Roles

1590



**Actor:** Document Consumer

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

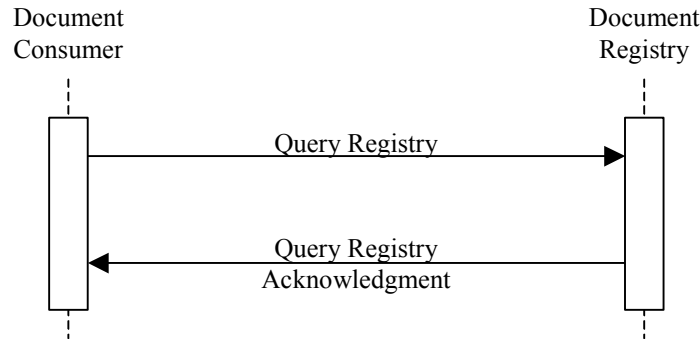
1595 **Actor:** Document Registry

**Role:** Receives Query Document messages and internally processes them.

### 3.16.3 Referenced Standard

ebRS                      OASIS/ebXML Registry Services Specifications v2.0

### 3.16.4 Interaction Diagram



#### 3.16.4.1 Query Registry

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

This profile specifies the use of SQL as a query language to the registry. There are 2 significant parameters to an AdHocQueryRequest:

- returnType
- SQL query text

##### 3.16.4.1.2.1 Parameter returnType

This profile 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

##### 3.16.4.1.2.2 SQL query text

The SQL queries written against a registry 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.

---

1620 **3.16.4.1.3 Expected Actions**

The registry returns a Query Message Acknowledgment.

**3.16.4.1.4 Example Queries****3.16.4.1.4.1 Query for Patient Documents in Date Range**

1625 The following query searches for Approved documents with patientId equal to 123 and documentTime between 1 January 2004 and 1 May 2004.

SELECT * FROM ExtrinsicObject doc, ExternalIdentifier ei, Slot docTime WHERE	The select must include ExtrinsicObject representing the document and attributes representing the patientId and documentTime
doc.objectType=XSDSDocumentEntry AND	The objectType must be XSDSDocumentEntry. XSDSDocumentEntry will be coded as a UUID.
	Match the patient id (recordTargetId)
ei.identificationScheme=XDSRecordTargetId AND	XDSRecordTargetId is the classification scheme that defines the recordTargetId attribute in XDS. This name will be replaced by a UUID in the query.
ei.registryObject=doc.id AND	This external Id belongs to this document.
ei.value='123' AND	The patient Id matches
	Validate the time range
docTime.parent=doc.id AND	The document time is stored in a slot. Check the linkage between the slot and the document object.
docTime.name='serviceTime' AND	The slot name is serviceTime.
docTime.value > '20040101' AND docTime.value &lt; '20040501' AND	The documentTime must be in requested range. Note the encoding of less-than using the &lt; sequence so it does not conflict with the XML within which this query is embedded. The time is coded as a sting and not a number so sort order determines performance of comparison operators.
doc.Status='Approved'	Find only approved documents.



**3.16.4.1.4.2 Query for all Discharge Summaries for a Patient**

1630 In this query we want all discharge summaries for a patient whose patientId is 123. It is presumed we have already established a Classification Scheme representing document types and there is a node within the Classification Scheme with the name 'Discharge Summary' that identifies the document type we want.

SELECT * FROM ExtrinsicObject doc WHERE	
doc.id in (SELECT doc.id FROM ExtrinsicObject doc, ExternalIdentifier ei WHERE doc.objectType=XDSDocumentEntry AND ei.identificationScheme=XDSRecordTargetId AND ei.registryObject=doc.id AND ei.value='123') AND	Select all documents for our patient. This subordinate query is constructed from the elements of the previous query example. Again, XDSRecordTargetId must be replaced by the UUID. The query could be extended to include discovering the UUID for XDSRecordTargetId.
doc.id in (SELECT classifiedObject FROM Classification WHERE classificationNode IN (SELECT id FROM ClassificationNode WHERE path = '/XDSDocumentTypes/Discharge Summary')) AND	Document is classified as a Discharge Summary
doc.Status='Approved'	Only find approved documents.

1635 **3.16.4.1.4.3 Query the contents of an XDS Folder**

An XDS Folder can hold 3 distinct types of objects:

1. XDS Folders (Registry Package object)
2. XDSDocumentEntry objects
3. Submission Sets (Registry Package object)

1640 For later processing, such as creating a display of the contents, it is necessary to know the type of all the objects returned since each type is displayed differently. A separate query will be used for each type.

1645 XDS Folders and Submission Sets are similar in that they are implemented as Registry Packages and their type is determined by classifications. XDSDocumentEntry objects are a subtype of ExtrinsicObjects, their typed coded via the objectType attribute

1650 The identity of the target XDS Folder is shown symbolically as currentXDSFolder. In a real application, this would be a raw UUID from a prior query. Also shown symbolically are XDSFolder and XDSSubmissionSet, the classification nodes representing Folders and Submission Sets. These would normally be coded as raw UUIDs from a prior query or have a query coded as an IN predicate to find them.

#### Query for XDS Folders

SELECT * FROM RegistryPackage folder, Classification c, Association a WHERE	
a.sourceObject=currentXDSFolder AND	Folder is a member of currentXDSFolder
a.associationType='HasMember' AND	
a.targetObject=folder.id AND	
c.classifiedObject=folder.id AND	Folder is classified as XDSFolder
c.classificationNode=XDSFolder AND	XDSFolder is replaced by the raw UUID
Folder.status='Approved'	Folders must be approved.

#### Query for XDSDocumentEntry objects

SELECT eo.id FROM ExtrinsicObject eo, Association a WHERE	
a.sourceObject=currentXDSFolder AND	ExtrinsicObject is a member of currentXDSFolder
a.associationType='HasMember' AND	
a.targetObject=eo.id AND	
eo.objectType=XDSDocumentEntry AND	Extrinsic Object is type XDSDocumentEntry where XDSDocumentEntry is replaced by the raw UUID
eo.status='Approved'	

#### 1655 Query for Submission Set objects

SELECT eo.id FROM ExtrinsicObject eo, Association a WHERE	
---	--

a.sourceObject=currentXDSFolder AND	ExtrinsicObject is a member of currentXDSFolder
a.associationType='HasMember' AND	
a.targetObject=eo.id AND	
eo.objectType=XDSSubmissionSet	Extrinsic Object is type XDSSubmissionSet where XDSSubmissionSet is replaced by the raw UUID
eo.status='Approved'	

### 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.

#### 1660 3.16.4.1.2 Message Semantics

The Query Registry Acknowledgement (AdhocQueryResponse) is returned in one of three forms:

1. List of ObjectRefs
2. Registry metadata describing objects found by query
- 1665 3. Error message

#### 3.16.4.2.3 Expected Actions

The query transaction is complete. The Document Consumer may then generate new queries from returned data, use returned data, or retrieve documents from the repository.

---

*Add the following section to Volume 2 of the IHE ITI Technical framework*

---

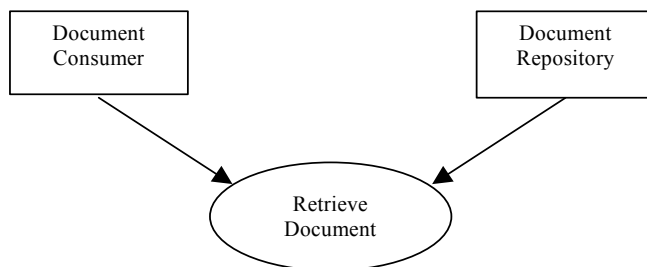
1670 **3.17 Retrieve Document**

This section corresponds to Transaction ITI-17 of the IHE Technical Framework. The Document Consumer and Document Repository actors use transaction ITI-17.

**3.17.1 Scope**

1675 This transaction is used by the Document Consumer to retrieve a document from the Document Repository. The Document Consumer Actor has already obtained the URI information from the Document Registry by means of the Query Registry transaction.

**3.17.2 Use Case Roles**



**Actor:** Document Consumer

1680 **Role:** Obtains document.

**Actor:** Document Repository

**Role:** Provides documents.

**3.17.3 Referenced Standard**

HTTP Hyper Text Transfer Protocol HTTP 1.1 (RFC 2616)

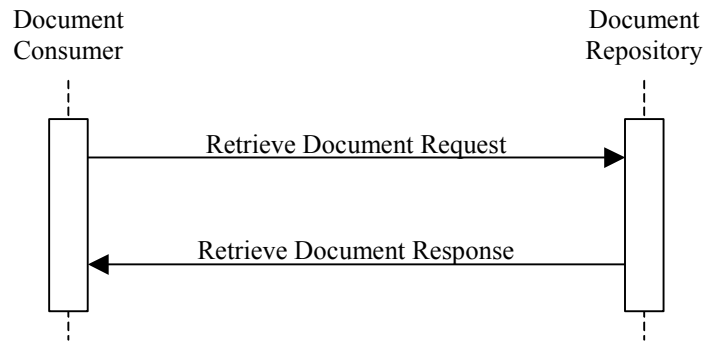
1685 MIME Multipurpose Internet Message Extensions (RFC 2045 to RFC 2049)

SMTP Simple Mail Transfer Protocol (RFC 2821)

Multipart/Related The MIME Multipart/Related Content-type (RFC 2387)

---

### 3.17.4 Interaction Diagram



#### 1690 3.17.4.1 Retrieve Document Request

##### 3.17.4.1.1 Trigger Events

The Document Consumer obtains document URIs via the

- Query Registry transaction.

##### 3.17.4.1.2 Message Semantics

1695 The URI specifies the protocol and protocol parameters that are to be used to retrieve the document. The Document Repository Actor shall support the following parameters for protocol in the URI:

- HTTP

The details of URI handling are specified in [HTTP].

1700 The Document Repository Actor shall fully implement support for any protocol parameters that are defined by [HTTP].

##### 3.17.4.1.3 Expected Actions

A Retrieve Document Response will be generated in return. The details specified in [HTTP].

#### 3.17.4.2 Retrieve Document Response

##### 1705 3.17.4.2.1 Trigger Events

This message is triggered by the:

- Retrieve Document Request.

##### 3.17.4.2.2 Message Semantics

The message semantics are specified in [HTTP].

1710 **3.17.4.2.3 Expected Actions**

None

---

*Add the following section to Volume 2 of the IHE ITI Technical framework*

---

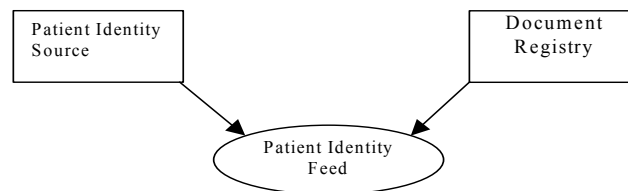
### 3.18 Patient Identity Feed

This section corresponds to Transaction 18 of the IHE IT Infrastructure Technical Framework. Transaction 18 is used by the Patient Identity Source and Document Registry actors.

#### 3.18.1 Scope

This transaction communicates the 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.

#### 3.18.2 Use Case Roles



**Actor:** Patient Identity Source

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

**Actor:** Document Registry

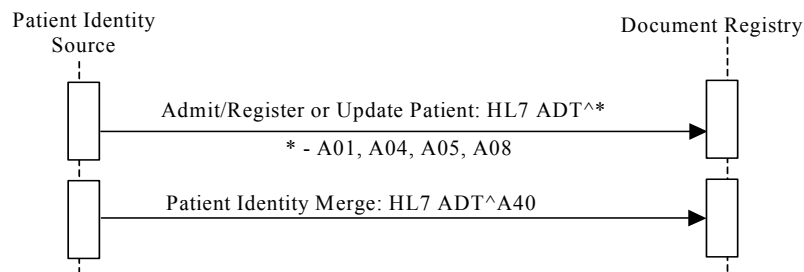
**Role:** Uses patient identifiers provided to ensure that XDS Documents metadata registered is associated with a known patient and tracks any changes relevant to its operation (e.g. merge).

#### 3.18.3 Referenced Standards

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

- HL7 version 2.3.1 was selected for this transaction as it provides a broader potential base of Patient Identity Source Actors capable of participating in the profiles associated with this transaction.

#### 3.18.4 Interaction Diagram



1735

---

**Figure 3.18-1 Patient Identity Sequence**

The above messages are identical to those specified in Transaction (ITI TF-2: 3.8).



<i>Add the following section to Volume 2 of the IHE ITI Technical framework</i>
---

## **Appendix XDS-B – Required Registry Initialization**

This section has not yet been written. Contributions are expected from Public Comment

1740

## **Appendix XDS-C – Affinity Domain Initialization**

This section has not yet been written. Contributions are expected from Public Comment

## **Appendix XDS-D – Example of Provide and Register XML Schema**

1745 This section has not yet been written. Contributions are expected from Public Comment

## **Appendix XDS-E – Example of Query Response XML Schema**

This section has not yet been written. Contributions are expected from Public Comment

*Add the following section to Volume 2 of the IHE ITI Technical framework*

## 1750 **Appendix XDS-F – XDS Security Environment**

This Appendix expands on the summary provided in the XDS Volume 1 specification (ITI TF-1: Appendix XDS-A).

1755 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.

1760 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 group. 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.

### 1765 **A.1 Security Environment**

#### **A.1.1 THREATS**

Specific threats to the overall XDS system are listed below. These threats are identified using the Common Criteria nomenclature. Most of these are mitigated by policies, procedures, and technologies that are not unique to XDS and do not require any special XDS considerations.

1770 Many of these mitigations do require that the parties within the XDS affinity group have agreement on details of how they will work together.

- **T.ADMIN\_ERROR** Improper administration may result in defeat of specific security features.
- 1775 • **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.
- 1780 • **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.

- 1785
  - **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.
- 1790
  - **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 an entity on another machine on the same network.
- 1795
  - **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.
- 1800
  - **T.POOR\_DESIGN** Unintentional or intentional errors in requirement specification, design or 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.
- 1805
  - **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 group and communicate with authorized users who incorrectly believe they are communicating with authorized members.
- 1810
  - **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.
- 1815
  - **T.UNAUTH\_ACCESS** Unauthorized access to data by a user may occur. This includes access via 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.

- 
- 1820      • **T.UNDETECTED\_ACTIONS**      Failure of the XDS components to detect and record unauthorized 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.
  - 1825      • **T.USER\_CORRUPT**      User data may be lost or tampered with by other users.

### A.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.
- 1835      • **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)
- 1840      • **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).
- 1845      • **P.DECLARATIVE\_SECURITY**      The system shall allow the administrator to define security related rules. Examples include defining access control policies and password expiration restriction.
- 1850      • **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.)
- 1855      • **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.

- 1860 • **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.
- 1865 • **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.

### **A.1.3 SECURITY USAGE ASSUMPTIONS**

1870 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.
- 1875 • **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.
- **A.OPERATION** It is assumed that networks, firewalls, etc. are deployed and maintained to meet appropriate network security levels.
- 1880 • **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 user authentication. The key management maybe done manually or automatically depending on the availability of appropriate technology.

## **A.2 Security Objectives**

1885 This section defines the security objectives for the XDS environment. These objectives are suitable to 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.

1890

### **A.2.1 XDS COMPONENT SECURITY OBJECTIVES**

- 
- 1895

    - **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 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.
  - 1900

    - **O.ADMIN\_TRAINED** The XDS components will provide authorized Administrators with the necessary information for secure management and operation.
    - **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)
  - 1905

    - **O.AUDIT\_PROTECTION** Each XDS component will provide the capability to protect audit 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)
  - 1910

    - **O.CONFIG\_MGMT** All changes to the components and its development evidence will be tracked and controlled.
    - **O.DECLARATIVE\_SECURITY** The components will allow security functions and access control to be defined by the authorized administrator.
  - 1915

    - **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 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.
  - 1920

    - **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)
  - 1925

    - **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.

- 1930
  - **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.
- 1935
  - **O.INTRUSION\_DETECTION** The XDS components will ensure intrusion of malicious software (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.
- 1940
  - **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 obtained without a protection compromise, such as from system failure or discontinuity.
- 1945
  - **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 media such as hard disk shall be secured during service and repair.
- 1950
  - **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.
- 1955
  - **O.TRAINED\_USERS** The XDS environment will provide authorized users with the necessary 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.)
- 1960
  - **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.

## 1965 A.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.
- 1970 • **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.
- 1975 • **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.

## A.3 Functional Environment

1980 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:

- 1985 1. **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.
2. **Repository** – This functional organization is responsible for providing query services 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 documents.
- 1990 3. **Registry** - This functional organization is responsible for providing query services to readers. The creator has delegated responsibility to the registry to provide adequate protection for a subset of the PHI. This subset is called the metadata.
4. **Reader** – This functional organization is providing healthcare services that make use of data that is contained in the metadata and the documents.

1995

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



- 
- 2000 against the threat of disaster, it need not be concerned with the disaster related policies of the reader.
- 2005 “**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.
- 2010 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.
- 2015 “**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:
- 2020 a. **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 propagate 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.
  - 2025 b. **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.
  - 2030 c. **P.ObjectAuthorization** – The policies regarding creation and modification of access rights often differ.

2035 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

2040 by the registry and repository to only those readers that have policies and mitigations that are acceptable to the creator.

Mitigations for differences include the following:

- 2045 a. 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.
- 2050 b. 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.
- 2055 c. Trusted third party inspections and audits can sometimes deal with reconciliation of differences in P.Account and P.Trace.
- 2060 d. 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 registry, but it reduces the combinatorial explosion of policy combinations between creators, repositories, registries, and readers into a linear growth in complexity.
- 2065 e. The “approved delegation” may go further into identification of persons, but this is only a viable path when all parties have policies that easily support delegation of personal responsibility. Persons are usually required to comply with organizational policies, and organizations generally use roles rather than 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).

2070 These mitigations do not directly change the technical requirements for the XDS transactions. They are 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.