



Privacy, Access and Security Services (PASS)
Healthcare Audit Services
Release 1.0

1st Draft Standard for Trial Use Ballot
September 2010

© 2010 Health Level Seven, Inc.
Ann Arbor, MI
All Rights Reserved

Editor	Patrick Pyette (Inpriva) ppyette@inpriva.com
PASS Alpha Project Lead	Don Jorgenson (Inpriva) djorgenson@inpriva.com
PASS Alpha Project Facilitators	Tracy Page (Page Consulting) pageconsulting@gmail.com Gila Pyke (Cognaissance Inc.) gila@cogna.ca
PASS Alpha Project Coordinator	Tabitha Albertson (Inpriva) talbertson@inpriva.com
Project Members	Bill Braithwaite (Anakam) bbraithwaite@anakam.com Laura Bright (Nexj) laura.bright@nexj.com Mike Davis (Veterans Health Administration) Mike.Davis@va.gov Steven Connolly (Apelon) sconnolly@apelon.com Ed Coyne (Veterans Health Administration) Ed.Coyne@va.gov Rob Horn (AGFA) robert.horn@agfa.com Steven Meyer smeyer@computer.org John Moehrke (GE Healthcare) John.Moehrke@med.ge.com Laurie Tull (Anakam) ltull@anakam.com Serafina Versaggi (Eversolve) serafina@eversolve.com

Preface

Note to Readers

This document contains the complete MDA specification stack (i.e. Conceptual Information Model (CIM), Platform Independent Model (CIM), and Platform Specific Model (PSM)) for the Privacy, Access, and Security Services project Audit Service (PASS Audit Service). The document supports the HL7 Services Aware Integration Framework (SAIF), under which this project is governed. Further context is given in the overview section below, but one key point to note is that this specification encompasses at the conceptual level, all of the viewpoints identified by the SAIF.

Changes from Previous Versions

The following is a summary of changes from previous versions:

- Initial version – no changes

Table of Contents

1	INTRODUCTION	8
1.1	DEFINITION	8
1.2	ORGANIZATION	9
1.2.1	<i>Business</i>	9
1.2.2	<i>Informational</i>	10
1.2.3	<i>Computational</i>	10
1.2.4	<i>Engineering</i>	10
1.3	SCOPE	10
2	BUSINESS VIEWPOINT (CONCEPTUAL)	12
2.1	OVERVIEW	12
2.2	BUSINESS MODEL	12
2.3	SCENARIOS	13
2.3.1	<i>Actors</i>	14
2.3.2	<i>Disclosure Scenarios</i>	14
2.3.3	<i>Behavioral Scenarios</i>	16
2.4	USE CASES	16
2.4.1	<i>Use Case Actors</i>	16
2.4.2	<i>Use Case AU-1: Submit Audit Record</i>	17
2.4.3	<i>Use Case AU-2: Retrieve Disclosure Records</i>	17
2.5	HEALTHCARE AUDIT REQUIREMENTS	18
3	INFORMATIONAL VIEWPOINT	21
3.1	CONCEPTUAL LEVEL	21
3.1.1	<i>Business Rules / Constraints</i>	21
3.1.2	<i>Information Model</i>	21
3.1.3	<i>Semantic Signifiers (Normative)</i>	23
3.1.4	<i>Dynamic Model</i>	27
3.2	PLATFORM INDEPENDENT LEVEL	27
3.2.1	<i>Business Rules / Constraints</i>	27
3.2.2	<i>Information Model</i>	27
3.2.3	<i>Semantic Signifiers (Normative)</i>	31
3.2.4	<i>Dynamic Model</i>	46
3.3	PLATFORM SPECIFIC LEVEL	47
3.3.1	<i>Semantic Signifiers</i>	47
	COMPUTATIONAL VIEWPOINT	68

4.1	OVERVIEW	68
4.2	CONCEPTUAL LEVEL	68
4.2.1	<i>Capabilities</i>	68
4.2.2	<i>Collaboration Analysis</i>	70
4.2.3	<i>Conformance</i>	71
4.3	PLATFORM INDEPENDENT MODEL	73
4.3.1	<i>Operations</i>	73
4.3.2	<i>submitAuditRecord</i>	73
4.3.3	<i>requestDisclosureRecords</i>	73
4.3.4	<i>requestAuditRecords</i>	74
4.4	PLATFORM SPECIFIC MODEL	75
4.4.1	<i>Audit Recorder Profile</i>	75
4.4.2	<i>Audit Reporter Profile</i>	76
5	ENGINEERING VIEWPOINT	78
5.1	CONCEPTUAL LEVEL	78
5.1.1	<i>ODP Functions</i>	78
5.1.2	<i>Engineering Roles</i>	78
5.2	PLATFORM INDEPENDENT LEVEL	78
5.2.1	<i>ODP Functions</i>	78
5.2.2	<i>Engineering Roles</i>	79
5.3	PLATFORM SPECIFIC LEVEL	79
5.3.1	<i>ODP Functions</i>	79
5.3.2	<i>Engineering Roles</i>	81
	APPENDIX A - GLOSSARY OF TERMS.....	82
	APPENDIX B – REFERENCE DOCUMENTS.....	84

List of Tables

Table 1 Scenario Actors.....	14
Table 2 Use Case Actors.....	16
Table 3 Healthcare Audit Requirements.....	19
Table 4 CIM - Disclosure Information Request Semantic Signifier.....	24
Table 5 CIM - Action Element Details.....	26
Table 6 CIM - Party Element Details.....	26
Table 7 CIM - InformationReference Element Details.....	26
Table 8 CIM - Patient Element Details.....	26
Table 9 PIM - Disclosure Audit Vocabulary.....	27
Table 10 PIM - Audit Record Request Attributes.....	32
Table 11 PIM - ParticipantCriteria Attributes.....	32
Table 12 PIM - Disclosure Record Request Attributes.....	33
Table 13 PIM - ParticipantCriteria Attributes.....	33
Table 14 PIM - Disclosure Record Response - EventIdentification Attributes.....	35
Table 15 PIM - Disclosure Record Response - Participant Attributes.....	35
Table 16 PIM - Disclosure Record Response - ActiveParticipant Attributes.....	36
Table 17 PIM - Disclosure Record Response - ParticipantObject Attributes.....	36
Table 18 Idealized Disclosure Event Record – Audit Object.....	38
Table 19 Idealized Disclosure Event Record – Audit Event Description.....	39
Table 20 Idealized Disclosure Event Record - Source Participation.....	40
Table 21 Idealized Disclosure Event Record - Releasing Agent Participation.....	41
Table 22 Idealized Disclosure Event Record - Receiving Agent Participation.....	41
Table 23 Idealized Disclosure Event Record - Requestor Participation.....	42
Table 24 Idealized Disclosure Event Record - Destination Participation.....	42
Table 25 Idealized Disclosure Event Record - Audit Source Participation.....	43
Table 26 Idealized Disclosure Event Record - Patient Participation.....	43
Table 27 Idealized Disclosure Event Record - Releasing Custodian/Controller Participation.....	44
Table 28 Idealized Disclosure Event Record - Receiving Custodian/Controller Participation.....	44
Table 29 Idealized Disclosure Event Record - Information Reference Participation.....	45
Table 30 Idealized Disclosure Event Record - Authorization Participation.....	45
Table 31 Submit Audit Record - PIM to PSM Transformation - AuditRecordRequest.....	48
Table 32 Submit Audit Record - PIM to PSM Transformation - DisclosureRecordRequest.....	48
Table 33 Submit Audit Record - PIM to PSM Transformation - AuditRecordResponse.....	49
Table 34 Submit Audit Record - PIM to PSM Transformation - DisclosureRecordResponse.....	49
Table 35 Submit Audit Record - PIM to PSM Transformation - AuditMessage.....	50
Table 36 Security Control Measures – Audit Recorder – Syslog Profile.....	80
Table 37 Security Control Measures – Audit Reporter – SOAP Profile.....	81

List of Figures

<i>Figure 1 Security Audit and Alarm Functions – ISO/IEC 10181-7</i>	12
<i>Figure 2 Audit Service Boundary Diagram</i>	13
<i>Figure 3 Generalized Audit Record Model</i>	21
<i>Figure 4 Generalized Disclosure Event Model</i>	22
<i>Figure 5 CIM - Disclosure Information Request Semantic Signifier</i>	24
<i>Figure 6 CIM - Disclosure Information Response Semantic Signifier</i>	25
<i>Figure 7 PIM - Audit Record Request Semantic Signifier</i>	31
<i>Figure 8 PIM - Disclosure Record Request Semantic Signifier</i>	32
<i>Figure 9 PIM - Audit Record Response Semantic Signifier</i>	34
<i>Figure 10 PIM - Disclosure Record Response Semantic Signifier</i>	37
<i>Figure 11 PSM - HL7 Audit Recorder Profile - Audit Message Schema</i>	54
<i>Figure 12 PSM – HL7 Audit Reporter Profile - RetrieveAuditRecords Schema</i>	64
<i>Figure 13 PSM - HL7 Audit Reporter Profile - RetrieveDisclosureRecords Schema</i>	66
<i>Figure 14 Audit Service Capabilities</i>	70
<i>Figure 15 PIM - Audit Service Operations</i>	73
<i>Figure 16 HL7 Audit Reporter Profile WSDL</i>	76

1 Introduction

The purpose of this specification is to provide the audit service interfaces associated with the patient privacy capabilities, including the content, structure, and functional behavior of security audit information important to patient privacy within the healthcare environment.

- 5 *“Of all security requirements protecting personal health information, among the most important are those relating to audit and logging. These ensure accountability for patients entrusting their information to electronic health record systems and also provide a strong incentive to users of such systems to conform to the policies on the use of these systems. Effective audit and logging can help to uncover misuse of electronic health record systems or of patient data and can help organisations and patients obtain redress against users abusing their access privileges.*
- 10

*Personal health information is regarded by many as among the most confidential of all types of personal information and protecting its confidentiality is essential if patient privacy is to be maintained. In order to protect the consistency of health information, it is also important that its entire life cycle be fully auditable”.*¹

- 15 This document defines the business requirements that are necessary make up a Healthcare Audit Control Service to support accounting of disclosures. This document extends ISO10181-7 Security Audit Framework audit services (managing and recording audit events) to include support for or interaction with other compliance mechanisms, such as Privacy Accounting,

- 20 Technical mechanisms for providing healthcare audit record collection are and have been addressed by other standards bodies and serves to guide this specification. Accordingly, key elements of ISO TS 12052 (DICOM Supplement 95²) and ISO CD 27789, IHE ATNA, The Open Group’s Distributed Audit System (XDAS) preliminary specification, and work from the International Security, Trust, and Privacy Alliance have all been incorporated into this specification³.

1.1 Definition

- 25 *“The Audit Service handles the recording and maintenance of service events from other Services. It captures, into privileged audit logs, necessary audit information to ascertain compliance with governing policies and procedures derived from agreements, an organization’s internal policies, and any applicable law or regulation.”*⁴

The purpose of security audit services is to provide support for:

- 30• the principle of accountability – that is holding users of a system accountable for their actions within the system, and
- Detection of security and privacy policy violations – that is the detection of attempts by unauthorized individuals to access the system and of attempts by authorized users to misuse their access to the system.

¹ ISO CD 27789 Health Informatics – Audit trails for electronic health records

² DICOM Supplement 95 includes key normative elements describing the format of data to be collected and the minimum set of attributes that need to be captured for security auditing in healthcare application systems previously published in the informational IETF RFC 3881 Security Audit and Access Accountability, September 2004.

³ See Appendix B for a complete list of reference documents.

⁴ Source: International Security, Trust and Privacy Alliance: Privacy Management Reference Model Version 2.0, 2009

35 1.2 Organization

The document comprises the four viewpoints identified by the HL7 Services Aware Integration Framework (SAIF) : Business, Informational, Computational, and Engineering. The goal of all SAIF artifacts is to ensure “working interoperability” (WI) between implementations, whether they be document-, message-, or service-based. The concept of working interoperability can be described as “the deterministic exchange of data/information in a manner that preserves shared meaning”. Starting at the conceptual level, the goal is to ensure that specifications are “implementable in a variety of deployment contexts, in a repeatable, comprehensible manner”. The explicit specification of any transform that may be required to allow interoperability between implementations is one of the keys to WI.

Each viewpoint described below is further divided into sections which are at different levels of abstraction. These levels are taken from the Object Management Group (OMG) Model Driven Architecture® (MDA®) specification, namely: Computation Independent Model, Platform Independent Model, and Platform Specific Model.

The following descriptions are taken directly from the OMG’s MDA Guide^{5,6}:

Computation Independent Model

50 The *computation independent viewpoint* focuses on the on the environment of the system, and the requirements for the system; the details of the structure and processing of the system are hidden or as yet undetermined.

Platform Independent Model

55 The *platform independent viewpoint* focuses on the operation of a system while hiding the details necessary for a particular platform. A platform independent view shows that part of the complete specification that does not change from one platform to another. A platform independent view may use a general purpose modeling language, or a language specific to the area in which the system will be used.

Platform Specific Model

60 The *platform specific viewpoint* combines the platform independent viewpoint with an additional focus on the detail of the use of a specific platform by a system.

1.2.1 Business

The Business viewpoint identifies the business context and scoping for the specification and contains the following artifacts:

- 65
- The use cases and scenarios that have been used to scope the work;
 - A set of traceable requirements – informational and functional have been extracted from the use cases and scenarios, or driven out from subsequent analysis.
 - A business object model that identifies objectives and business entities, including the roles that those entities have in executing processes to achieve the stated objectives.

⁵ Object Management Group – MDA Guide v1.0.1 – Document Number: omg/2003-06-01

⁶ The MDA Guide refers to each of the levels of abstraction as Viewpoints. To avoid confusion, these have been renamed to “Models” in the HL7 SAIF material and in this document.

70 1.2.2 Informational

The Informational Viewpoint presents the object model representing the unconstrained information requirements of the system – the major entities and their relationships to each other. This viewpoint also identifies vocabulary concepts that are appropriate for the domain. Artifacts in this viewpoint include:

- A static model, containing the informational objects and invariant schema
- 75 ▪ A dynamic model, identifying allowable state changes to the information objects.

1.2.3 Computational

The Computational viewpoint presents the functional behavior of an Audit Control Service grouped so that the capabilities are distributable and may be exposed through service interfaces. It documents the collaboration analysis performed, identifies service roles and responsibilities, and groups the service capabilities and operational semantics into contracts and profiles.

1.2.4 Engineering

The Engineering viewpoint identifies and captures any relevant platform capabilities, and documents any essential requirements for the distribution of any of the functionality identified.

1.3 Scope

85 This document included all information models and technical service capabilities required to provide healthcare-specific audit services. This includes end-user accountability in cross-organizational or intra-organizational distributed healthcare environments. In this environment, the scope includes those interoperability requirements that inevitably arise when attempting to achieve end-user accountability across diverse systems and their applications.

90 The scope of this document also includes activities that bring together a single composite and harmonized view of all auditable user activities across all systems for analysis and reporting of disclosures.

While the audit service vision is for a broader scope for healthcare audit-related services than currently exists in standards today, we need to point out that this release of the specification is scoped to add two service capabilities. Accordingly, development of this specification is planned as a series of incremental releases, each building upon the previous, however, with each release balloted sequentially (in turn) and independently. Specifically, the following items are included in the scope of this version (Release 1 Privacy):

- Semantics and behavior required to support audit record collection; and
- 100 • Semantics and behavior required to support downstream processing of audit event information, including support for privacy accounting (i.e. accounting for access, use, or disclosure of Personal Health Information (PHI)).

The following additional areas, in scope for the overall vision of the audit specification, will be included in a subsequent release:

- Healthcare-specific requirements to support security Incident management;
- 105 • Surveillance and/or monitoring services;

Out of scope for this specification in this and all planned subsequent releases are:

- The capture and persistence of an audit trail of changes to clinical information;

- Information and functional support for forensic auditing.

110 **2 Business Viewpoint (Conceptual)**

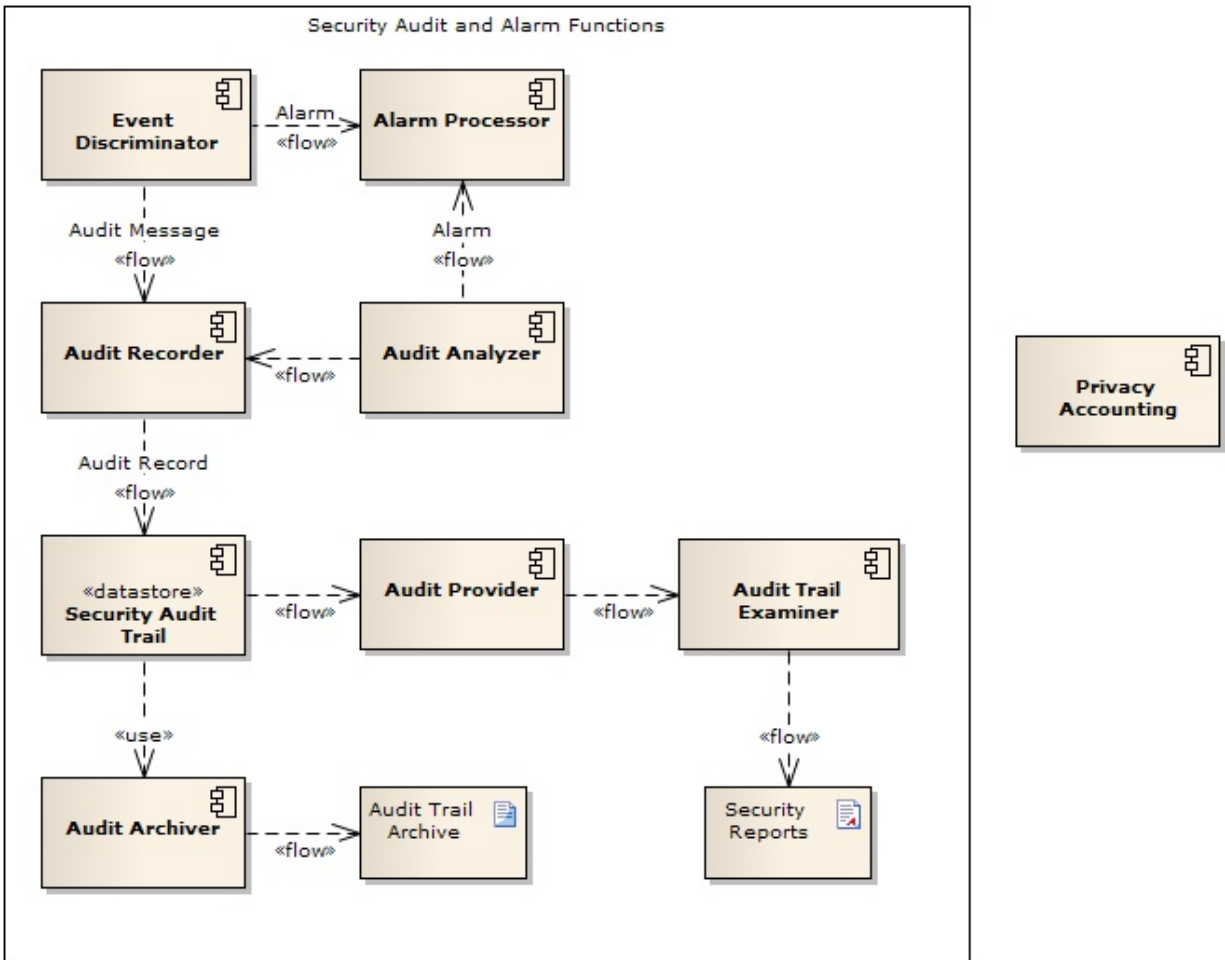
2.1 Overview

The Business Viewpoint identifies the business issues, models, processes, and roles associated with the Disclosure Audit sub-domain of Privacy, Access, and Security Services.

2.2 Business Model

115 ISO 10181-7 has identified the overall security audit and alarm functions as shown in Figure 1, below.

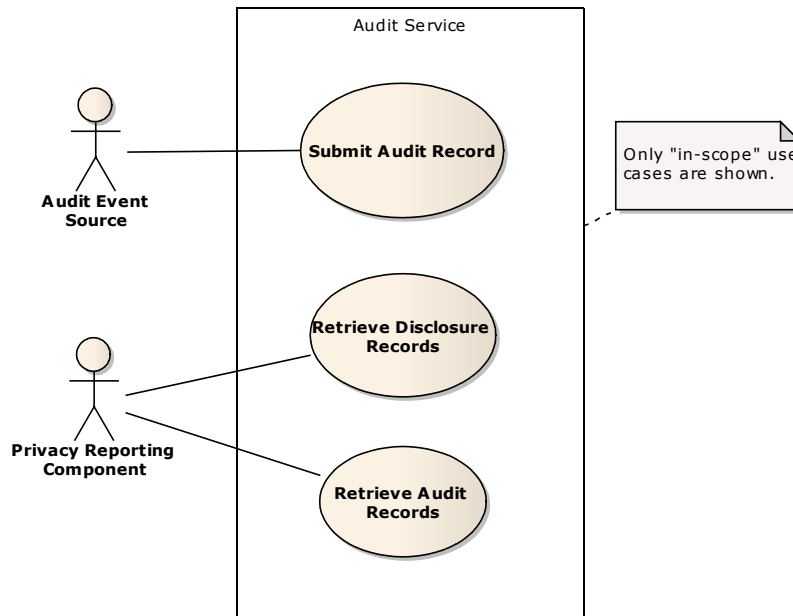
Figure 1 Security Audit and Alarm Functions – ISO/IEC 10181-7



120 This specification focuses on two capabilities – one provided by the Event Discriminator function, and the other provided by the Audit Provider to a generic Privacy Accounting function external to the Security Audit service⁷.

⁷ See ISO/IEC 10181-7/ITU-T Rec. X.816(1995 E) for details

Figure 2 Audit Service Boundary Diagram



The Audit Service Boundary Diagram above identifies only the capabilities of the Audit Service that are in scope for this release of the specification. The capabilities are:

- 125
- Submit Audit Record – a capability to accept audit event records from one or more Audit Event Sources (including the Audit Service itself), and
 - Retrieve Disclosure Records – a capability to retrieve information relating specifically to the disclosure of personally identifiable health information based upon some set of input criteria relevant to the disclosure. In relation to ISO 10181-7, the audit function that would be response
 - 130 for this capability would be the “audit trail examiner”.
 - Retrieve Audit Records – a capability to retrieve information relating to the access of privacy-related health information based upon some set of input criteria relevant to disclosure. In relation to ISO 10181-7, the audit function that would be response for this capability would be the “audit trail examiner”.

135 2.3 Scenarios

During the business analysis, a number of healthcare-specific scenarios were examined that were thought to have Audit implications. This section is divided into two parts: the first identifying different scenarios that were used to drive out semantic requirements; the second part dealing with scenarios which expose behavioral requirements.

140 N.B. The following list of scenarios is by no means exhaustive; it is intended to portray the breadth and types of disclosures that were considered during the analysis.

2.3.1 Actors

Table 1 Scenario Actors

Allan Ancestor	a living relative of Adam Everyman
Adam Everyman	a Patient
Eve Everywoman	a Patient
Alana Admitting	a hospital admitting/discharge clerk
Dr. Carol Consult	a consulting internal medicine specialist.
Ernest Emt	an emergency medicine technician working for Ace Ambulance.
Jane Janitor	GHH maintenance staff member.
Dr. Patricia Primary	a primary care physician in a group practice.
Dr. Henry Heart	a cardiologist.
Dr. Eric Emergency	an emergency room physician with Good Health Hospital
Nurse Nightingale	a nurse with Doctor's Inc.
Dr. Oldman	a primary care provider
Dr. Eric Younger	a primary care provider.

145 2.3.2 Disclosure Scenarios

Some or all of the following scenarios are situations where local policy may consider these to be disclosures that result in an obligation to submit an audit record.

Scenario 1

150 Nurse Nightingale (Doctors Inc) faxed a summary record for Adam Everyman to Dr. Heart (Have A Heart Inc.) as part of a referral by Dr. Primary.

Scenario 2

155 Adam Everyman arrives at Dr. Heart's clinic, is given a battery of tests. Dr. Heart evaluates the results of Adam's tests in combination with Hearts observations and provides a provisional diagnosis and a recommended care plan. The resulting report and test results are exported to a CD and given to Adam to deliver to Dr. Primary on his next scheduled visit.

Scenario 3

Adam returns to Dr. Primary and delivers the CD to Nurse Nightingale, who loads the information into Doctors, Inc. EMR system. When Dr. Primary sees Adam in an exam room, the returned referral information is on screen and available for Dr. Primary to view.

160 **Scenario 4**

Upon discharge from GHH, Alana Admitting sent an electronic copy of the discharge summary to Eve Everywoman's PCP, Dr. Primary, a physician with Primary Care, Inc.

Scenario 5

Dr. Primary reported her laptop; containing unencrypted patient information was stolen from her car.

165 **Scenario 6**

Dr. Primary retrieves Eve Everywoman's medical history from the regional repository (e.g. RHIO, HIE, or EHR). The repository contains information from many different sources/controllers/custodians.

Scenario 7

170 Nurse Nightingale (Doctors Inc) couriers a summary record for Adam Everyman to Dr. Heart (Have A Heart Inc.) as part of a referral by Dr. Primary.

Scenario 8

Dr. Heart asks an external consultant (Dr. Consult) to review and comment on Heart's treatment plan for Adam Everyman, while Dr. Consult is meeting with Dr. Heart.

Scenario 9

175 Jane Janitor overhears Dr. Heart and Dr. Consult talking about Adam Everyman's condition.

Scenario 10

Dr. Eric Younger purchases the clinical practice of retiring Dr. Oldman.

Scenario 11

180 Adam Everyman is using a remote blood glucose monitor to upload that information to his PHR. Adam has given Dr. Younger permission to retrieve that information order to provide treatment. Younger's Admin Assistant sets up the EMR system to retrieve the blood glucose information from the PHR and place it in Adam's records in the EMR.

Scenario 12

185 Eve Everywoman experiences severe chest pain while driving. She uses her OnStar subscription to call for assistance. Eve tells the Onstar operator about her symptoms who enters the information into his system, and uses that system to dispatch a Ace Ambulance, a local ambulance company, providing them with the information obtained from Eve.

Scenario 13

190 Ernest Emt is dispatched from Ace Ambulance. He picks up Eve and transports her to Good Health Hospital, monitoring her vital signs during the trip. Upon arrival at GHH, Ernest relays the information that they received from Onstar, as well as the information that was collected while enroute to Nurse Nightingale.

Scenario 14

195 Dr. Heart suspects that his patient, Adam Everyman, has a heart condition where detailed records of certain family members may confirm diagnosis and help guide treatment. Dr. Heart requests relevant records from Dr. Primary, the primary care physician for Allen Ancestor. Dr. Primary sends all of Allen Ancestor's medical records that may be related to Dr. Heart.

Scenario 15

200 Dr. Primary has received the results of laboratory tests on Adam that indicate that Adam has contracted tuberculosis. The jurisdiction in which Dr. Primary practices requires that all positive tuberculosis tests be forwarded to the regional public health office for follow up. Dr. Primary does not require Adam's consent (express or implied)

2.3.3 Behavioral Scenarios

Note: The scenarios that follow are examples to support the use case. They are not exhaustive.

205 **A discharge summary is sent to another party**

As part of the discharge process at Good Health Hospital, Alana Admitting confirms the name and address of her primary care physician, Dr. Patricia Primary, with Eva. Once complete, Alana forwards the discharge summary electronically to the secure email address listed for Dr. Primary. The system that Alana uses determines that forwarding information is an auditable event and as a result, creates an audit event record that it submits to a known Audit Repository.

A request for privacy accounting information occurs

Eve's PHR system maintains a list of organizations that have Eve's PHI. Eve logs into her PHR and requests a disclosure accounting report from each of those organizations.

215 Upon receipt of Eve's request, the Compliance Office of Good Health Hospital undertakes the production of the report using their new Healthcare Compliance system. The HC system issues a service request to the Healthcare Audit Repository for audit records meeting certain criteria. The Healthcare Audit Repository returns what information that it has that matches the criteria.

2.4 Use Cases

220 The use cases presented below reflect those identified during the initial phase of the PASS Audit project work.

2.4.1 Use Case Actors

The use cases consider Audit Service interactions with two external actors:

Table 2 Use Case Actors

Audit Event Source:	Any appropriately authorized source of healthcare audit records. The Audit Event Source can be a component of the Audit Service itself.
Privacy Accounting Component:	Any appropriately authorized requestor of information relating to the collection, use, and/or disclosure of personal information or personal health information.

225 2.4.2 Use Case AU-1: Submit Audit Record⁸

Description

Invoke a function to submit a record of an auditable event.

Assumptions

- 230 • In order for an audit trail to effectively support one or more distributed Audit Event Sources, those Sources, and all Audit Service components must maintain consistent time from a designated authoritative time service. The accuracy requirement of the coordinated timekeeping is a policy decision.
- Appropriate security controls are in place to ensure that adequate protection of the audit event information both in transit and at rest.

235 **Actors**

Audit Event Source

Trigger Event

The use case is triggered when one or more records of auditable events are ready to be transmitted⁹.

Pre-conditions

- 240 • The audit event source has been configured with the endpoint address of the Audit Service(s).

Post-conditions

- The Audit Service has accepted the audit event record(s).

2.4.3 Use Case AU-2: Retrieve Disclosure Records¹⁰

Description

- 245 Provide a mechanism to extract information to support downstream production of accounting of disclosure reports. Return disclosure records that may subsequently be used to identify disclosure of PHI.

⁸ An instance of the refinement of this use case into specifications at the Platform Specific level has been completed as DICOM Supplement 95 (ISO TS 12052), and the Record Audit Event transaction of the IHE ATNA specification (see Appendix B). These specifications are referenced in this document in the appropriate sections.

⁹ The use case is not necessarily triggered by the occurrence of an auditable event, although it can be. Generally, the Audit Event Source determines when conditions are appropriate to submit the audit event information.

¹⁰ See HL7 Composite Privacy Domain Analysis Model DSTU, December 9, 2009 – pg 56 – Accounting of Disclosures.

Assumptions

- 250 • Complete privacy accounting extends beyond the scope of the events captured by any electronic health system and includes handling of PHI that is not in electronic form. As a result the Audit Service may not be sole source of information required to enable the production of downstream reports.
- This capability will not have the ability to directly detect all potentially non-compliant behavior; however it can be used to support the identification of such behavior.
- 255 • We expect that the data provided by this capability will be supplemented by mechanisms that will allow identities in the record to be resolved.

Actors

- Audit Record Repository
- Privacy Accounting Component

Trigger Event

260 The use case is triggered by a request for disclosure information.

Pre-conditions

- The Privacy Accounting component has the appropriate authority to access the capability.

Post-conditions

- All available information that satisfies the request criteria has been returned to the invoking Actor.

265 **2.5 Healthcare Audit Requirements**

The table below summarizes all of the functional and interoperability requirements identified through review and analysis of the scenarios and use cases presented above.

270 Requirements for use case UA-01 have not been identified, as those requirements have been identified and satisfied in other standards¹¹. The focus of this work is on use case AU-02, which deals with retrieving information to support healthcare disclosure accounting processes.

Note 1: Where the requirements in Table 1 below identify healthcare-specific functionality or semantic content, those requirements are reflected in the Conformance section of this document.

¹¹ ISO TS 12052/DICOM Supplement 95 and IHE Record Audit Event section of the IHE ATNA specifications.

Table 3 Healthcare Audit Requirements

ID	Requirement	Functional / Interop.	Healthcare Specific? Y/N
	<p>The capability must be able to request and retrieve information obtained from audit event information that would support disclosure accounting.</p> <p>Specifically, an authorized client must be able to retrieve the following information if it is contained within, or can be determined by information contained within one or more audit event records held by the Audit Service:</p> <ul style="list-style-type: none"> Data and time of disclosure; Reason for disclosure; Description of the information disclosed; Identity of the person requesting access; Identity and verification of the party receiving the information; Identity of the party disclosing the information; <p>and</p> <ul style="list-style-type: none"> Verification method of the requesting party's identification. <p>Source: ASTM E 2147-01 (Reapproved 2009)</p>	F	Y ¹²
	Must be able to retrieve and request information obtained from audit event information that would support disclosure accounting, where the subject of record exists or can be determined.	F	Y
	Must have the ability to establish mutually-authenticated communication channels.	I	N
	The Audit Service must have the ability to validate that any request has been appropriately authorized, based upon implementation policy.	F	N
	The Audit Service must have the ability to deny a request where validation of the authorization credentials associated with that request fail.	F	N
	The Audit Service shall support the protection of audit event information in transit across networks as required by organizational policy.	I	N

¹² While the concept of disclosure is not healthcare specific, the definition of disclosure and the information requirements identified are healthcare specific.

ID	Requirement	Functional / Interop.	Healthcare Specific? Y/N
	Where the information elements described in Requirement 1 cannot be determined directly from the audit records contained within the Audit Service, the Audit Service should provide any information that may be relevant from its existing audit repository.	I	N

3 Informational Viewpoint

275 3.1 Conceptual Level

3.1.1 Business Rules / Constraints

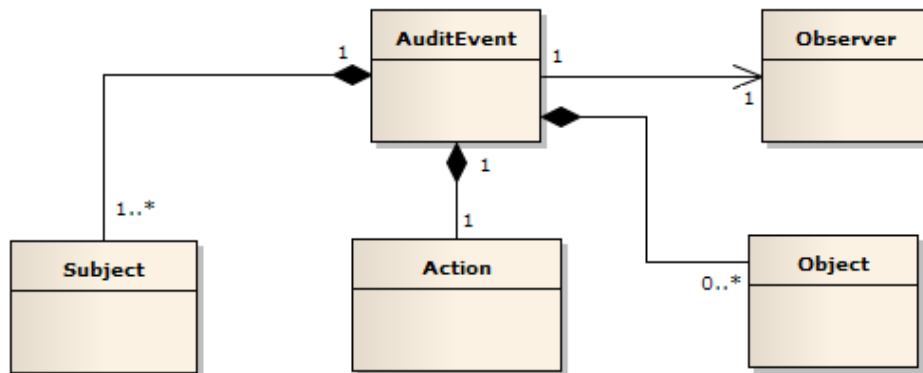
280 Business rules and constraints are identified in both DICOM Supplement 95 and in various IHE specifications, and are based on specific clinical or information system transactions. A mapping of the business rules for the population of audit event records associated with HL7 Acts is out of scope of this specification but would be a valuable resource to implementers.

3.1.2 Information Model

Generalized Audit Event

285 During the operation of any healthcare information system, many events that have a security or privacy impact may be recognized and recorded by the system. Events can be triggered by human users, connected information systems, devices, etc. A generalized model of a suitable audit recording of an event is shown below. This model is a generalization of the current DICOM Supplement 95 healthcare audit event schema, which is based upon the IETF RFC 3881 specification and is referenced by the IHE ATNA profile.

Figure 3 Generalized Audit Record Model



290

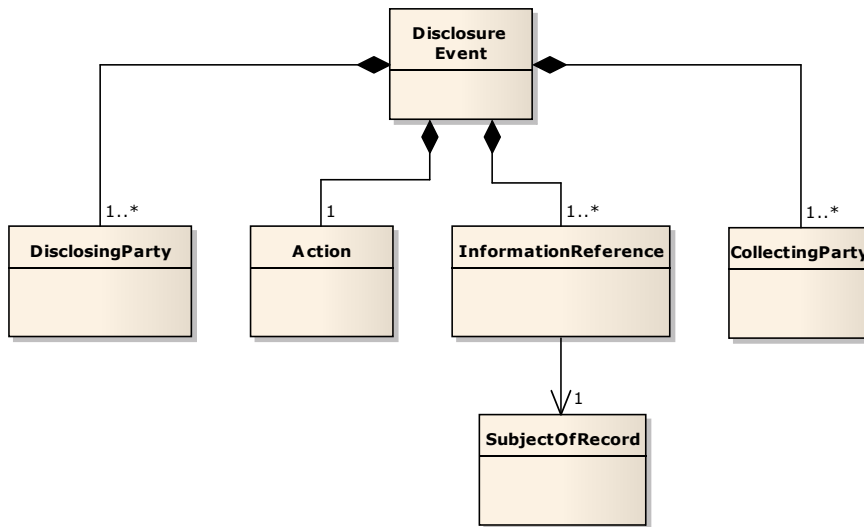
In the generalized audit event model, each Audit Event is characterized by:

- One or more Subjects – users, systems, devices, etc. that actively participated in the activity;
- One or more Observers – usually active components that observe and record the activity;
- Action – the event Information that describes the activity that occurred;
- 295 Zero or more Objects – entities that were acted upon or were involved in some passive way in the activity.

The model shown above is consistent with the DICOM Supplement 95 schema, as well as the preliminary Open Group XDAS work.

Generalized Disclosure Event

300 Figure 4 Generalized Disclosure Event Model



A disclosure event can be characterized as illustrated in Figure 4, above. The general properties of a disclosure event are:

- 305
- The Action that describes the Event.
 - The Disclosing Party is identified – this is the party that had custody and control of the information prior to the disclosure. The disclosing party can include systems, devices, individuals and the organization responsible for the disclosure.
 - The Collecting Party is identified – this is the party to whom the information was disclosed. As with Disclosing Party, this can include system, devices, individuals, and the organization.
- 310
- A reference to one or more Information Object(s) that were disclosed.
 - The identity of the person to whom the Information Object(s) refer.

In some cases (e.g. breaches), the Collecting Party may be unknown, and/or may be multiple parties. In the former case, the fact that the Collecting Party is unknown should be captured. In the latter case, multiple Disclosure Events could be said to have occurred simultaneously and each should be recorded separately if known.

315

Transformation of one or more audit event records into a definitive disclosure event record is only possible if all of the required information is available. This is a situation that does not occur in the real world with any great regularity, and the assumption is that the audit event records can only provide support for the identification of Disclosure Events rather than produce Disclosure Events with any accuracy, unless the observing entity has the capacity to make that determination.

320

3.1.3 Semantic Signifiers (Normative)

325 A semantic signifier is used to specify constraints on the information constructs that are the payloads in service capabilities. It is the identification of a named set of information descriptions (e.g. semantic signifiers) that are supported by one or more operations. The reference points for associated conformance statements occur at the computational model interface where the semantic signifier is specified as an input or output required by the contract.

Relationship to Composite Security and Privacy Domain Analysis Model (S&P DAM)

330 The following semantic signifier elements are referenced directly from the S&P DAM¹³:

- InformationReference
- SubjectOfReference
- Patient

335 Party is a higher level of abstraction than any class in the S&P DAM. Party includes people, organizations, and devices

The following entities are included in semantic signifiers that are not included in the S&P DAM:

- A person who does not have a system userid is not contained within the model;
- An organization that is not a provider organization is not contained within the model.

340 In reality, external entities with business relationships with the disclosing person or organization can have PHI disclosed to them legitimately, and there are any number of unauthorized disclosures that can occur that not been modeling in the S&P DAM.

- Neither service components nor devices are contained within the model.

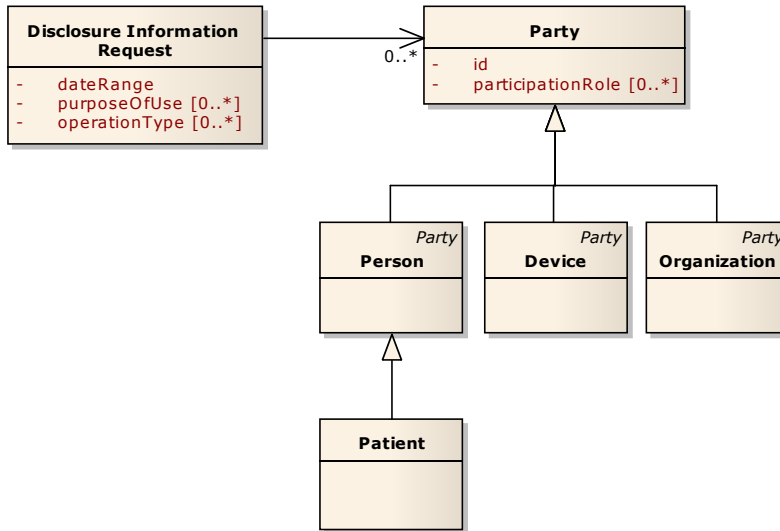
345 Service components and devices originate a great number of disclosures in the real world; however the focus for the S&P DAM is on policy definition and resolution and has not as of yet modeled these relationships.

¹³ HL7 Security and Privacy Domain Analysis Model – DSTU Ballot – May 2010

Disclosure Information Request

This semantic signifier defines the criteria by which the Audit Service will select and process audit events in order to support the identification of disclosure events.

Figure 5 CIM - Disclosure Information Request Semantic Signifier



350

The table below describes the elements and some of the key attributes of each element of the Disclosure Information Request. These are not intended to be a complete set of attributes at the conceptual level, and are only intended to be illustrative.

Table 4 CIM - Disclosure Information Request Semantic Signifier

Element	Attribute	Description
DisclosureInformationRequest		The container for the request semantic signifier.c
	dateRange	The start and end dates for which event information is being requested.
	purposeOfUse	A list containing zero or more purposes which may have been recorded as part of an auditable event.
	operationType	An optional, multi-valued attribute that represent the kinds of actions that are of interest. See S&P DAM OperationType.
Party		An entity that has some participation in the event, whether direct or indirect, active or passive.
	id	The identifier by which the party is known.
	participationRole	Values that indicate the role(s) that the party played in the disclosure (or potential disclosure).

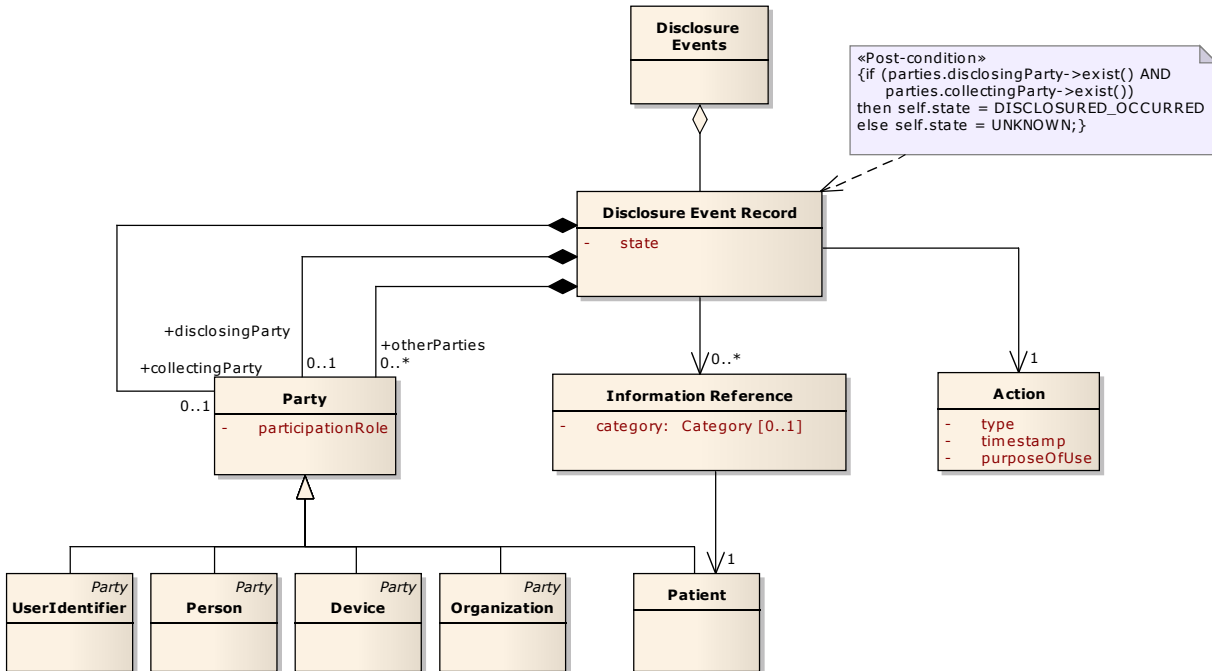
355

Disclosure Information Response

360 Figure 6 below illustrates the conceptual semantic signifier associated with the response to a request for Disclosure Audit Events at the conceptual level. The response contains a set of Disclosure Event records, each of which has some relationship to the patient identified in the request and whose other attributes match the criteria specified in the request.

The semantic signifier recognizes that Disclosing and Receiving Parties, as described in the Generalized Disclosure Event Model are the same kinds of entities, with different participation roles and has identified the differences as relationship specifiers on the Audit Record itself.

Figure 6 CIM - Disclosure Information Response Semantic Signifier



365

Disclosure Events

This class acts as the container of the audit event records that identifies disclosure events, either directly asserted disclosures with complete information, or events where disclosures may have potentially occurred, but all of the information necessary to make that determination is not available.

370 Disclosure Event Record

375 Contains a single event, whether an actual disclosure or a potential disclosure. A Disclosure Event Record may or may not be complete (i.e. it may be a potential disclosure). Conceptually, we can use an attribute such as state to further classify the record. In practice, the copying of IHLI onto portable media may or may constitute a disclosure, depending on the recipient of the portable media. Further information may be required that is not available from the Audit Service in order to determine whether the event was a disclosure according to the policies established within the particular jurisdiction and organization.

Action

The Action class specifies the details of the event.

Table 5 CIM - Action Element Details

Attribute	Description
type	A value that indicates the type of event. (See S&P DAM – OperationType)
timestamp	The nominal time assigned to the event. For a disclosure, this can be any instant of time during the disclosure process, where information left the custody and control of the disclosing party.
purposeOfUse	The legitimate use(s) for which the disclosed information can subsequently be used.

380 Party

Party identifies the entities that were involved in the event.

Table 6 CIM - Party Element Details

Attribute	Description
participationRole	A multi-valued attribute that indicates the role(s) that the party played in the disclosure (or potential disclosure).

385 Each instance of Party may contain additional attributes that are associated with the particular subclass as described in the S&P DAM, or in the HL7 Reference Information Model. The attributes will be returned if they have been collected in the source audit record. Specific participationRoles relevant to information disclosure can be found in the Platform Independent Model section of the Information Viewpoint, on page 27

InformationReference

390 The InformationReference identifies the information that was involved in the event and potentially disclosed.

Table 7 CIM - InformationReference Element Details

Attribute	Description
category	An optional attribute that indicates a categorization of the information involved.

Patient

The Patient is the subject of the information reference and must be one of the patients referred to in the request.

395 Table 8 CIM - Patient Element Details

Attribute	Description
patientId	A unique identifier for the patient to whom the information refers. This must match one of the patientId attributes contained in the request.

3.1.4 Dynamic Model

Not applicable.

3.2 Platform Independent Level

400 3.2.1 Business Rules / Constraints

Business rules and constraints are identified in both DICOM Supplement 95 and in various IHE specifications, and are based on specific clinical or information system transactions. See Appendix B for those references.

3.2.2 Information Model

405 DICOM Supplement 95 and the IHE ATNA profile specifications provide the basis for the platform independent model, which has been transformed into UML for the convenience of the reader.

Vocabulary

410 Table 9, below identifies concepts and contains a high level description of those concepts that are required to support the scenarios identified in the Business Viewpoint. The Structure Name column refers to elements in the Disclosure Record Request and Response semantic signifiers described in section 3.2.3.

Table 9 PIM - Disclosure Audit Vocabulary

Structure Name	Concept	Description
Participant.role ParticipantCriteria.role	Authorization	The entity on who's authority the Personal Information was released.
	Destination	Ref: [DICOM95]
	Information Reference	Metadata which describes the Personal Information which was the subject of this audit event.
	Patient	An individual to whom the Information Reference pertains.
	Receiving Agent	The individual that received information described in this audit event.
	Receiving Custodian/Controller	The person or organization that has legal responsibility for maintaining the privacy and security of the received information.
	Receiving Node	A system or device that the

Structure Name	Concept	Description
		information was transmitted to.
	Releasing Agent	The individual that was responsible for releasing the information.
	Releasing Custodian/Controller	The person or organization that had the legal responsibility for the privacy and security of the information prior to its release.
	Releasing Node	The system or device that transmitted the information.
	Requestor	The person, organization, system, or device that was responsible for originating the request to transfer information.
	Source	Ref: [DICOM95]
	Audit Source	The entity (person, system, or device) that observed and recorded the event.
EventIdentification.purposeOfUse ¹⁴ DisclosureRecordRequest.purposeOfUse	Clinical care provision to an individual subject of care	To inform persons or processes responsible for providing health care services to the subject of care
	Emergency care provision to an individual subject of care	To inform persons needing to provide health care services to the subject of care urgently, possibly requiring consent and over-ride policies distinct from those pertaining to Purpose 1 above
	Support of care activities within the provider organisation for an individual subject of care	To inform persons or processes enabling others to provide health care services to the subject of care, by coordinating activities and/or facilities
	Enabling the financing of care provision to an individual subject of care	To inform persons or processes responsible for enabling the availability of funds and/or

¹⁴ Vocabulary described in this table section are taken directly from ISO DTS 14265 – Health Informatics — Classification of purposes for processing personal health information

Structure Name	Concept	Description
		permissions from a funding party for providing health care services to the subject of care
	Health service management and quality assurance	To inform persons or processes responsible for determining the availability, quality, safety, equity and cost-effectiveness of health care services
	Education	To support the learning and professional development of health care professionals
	Public Health Surveillance, Disease Control	To inform persons or processes with responsibility to monitor populations or sub-populations for significant health events and then intervene to provide health care or preventive care services to relevant individuals
	Public safety emergency	To inform persons with responsibility for the protection of the public in a situation in which there is considered to be a significant risk to members of the public, possibly requiring consent and over-ride policies distinct from those pertaining to Purpose 7 above.

Structure Name	Concept	Description
	Population health management	To inform persons or processes with responsibility to monitor populations or sub-populations for health events, trends or outcomes in order to inform relevant strategy and policy
	Research	To support the discovery of generalisable knowledge
	Market Studies	To support the discovery of product or organization specific knowledge
	Law Enforcement	To inform persons or processes responsible for enforcing jurisdictional legislation, or undertaking legal or forensic investigation
	Subject of Care Uses	To inform the subject of care or his or her legally authorized agent in support of the subject of care's own interests
	Unspecified ¹⁵	Disclosure on the basis of authorizations not requiring a purpose to be declared.
	Unknown ¹⁶	No indication as to the purpose of use has been identified. N.B. Other concepts may be added to this list to meet local needs.
EventIdentification.category DisclosureRecordRequest.eventCategory	Disclosure	Indicates that the audit event record has been identified as describing a disclosure according to local policy, regulation, or law.
	Not a disclosure	Indicates that the audit record describes a release of information that was identified as not being a legal disclosure.
	Disclosure not	No attempt has been made by the Audit Source to determine

¹⁵ The definition has been modified from the original ISO draft definition to remove "or purposes for which the other categories in this clause do not apply".

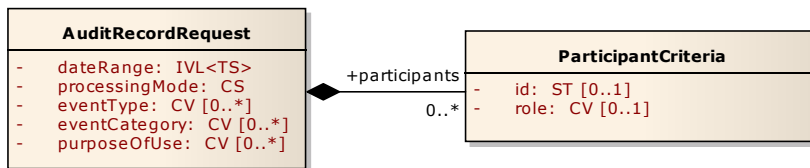
¹⁶ Added by the PASS Audit project team.

Structure Name	Concept	Description
	determined	whether the event represents a disclosure.
	Disclosure unknown	No information is available regarding the disclosure status of this audit event.
	DICOM Supplement 95 table ccc2 values	See [DICOM95]
	IHE Transaction Identifiers	See Audit Considerations for each transaction identified in [IHE-ITI 2A], [IHE-ITI 2B], and [IHE-ITI 3]
EventIdentification.type DisclosureRecordRequest.eventType	DICOM Supplement 95 table ccc1 values	See [DICOM95]
	IHE table ccc1 values	See section 3.20.7.5 of [IHE-ITI-2A]
DisclosureRecordRequest.processingMode	Strict	A straightforward selection of audit event records based upon the criteria is requested to be performed.
Participant.type	DICOM Supplement 95	See [DICOM95]

3.2.3 Semantic Signifiers (Normative)

415 **Audit Record Request**

Figure 7 PIM - Audit Record Request Semantic Signifier



The Audit Record Request is the container class for a message requesting a set of audit event records that are related to an actual or potential disclosure from the Audit Service. The request includes zero or more ParticipantCriteria elements to be used in the request.

420

Table 10 PIM - Audit Record Request Attributes

Attribute	Description
dateRange	A mandatory date interval that denotes the date and time of any audit event records to be included in the response. A starting date is required. Requiring a date range to be specified helps to ensure that: <ul style="list-style-type: none"> information disclosed by the Audit Service is minimized to that which is absolutely necessary, and the commissioning agent has responsibility for the information requested and subsequently disclosed.
processingMode	An indication to the service implementation as to how the request is to be processed. Allows future flexibility in the service behavior. Additional processing modes may be defined and the associated behavior documented at a later date.
eventType	An optional list of values which identify the types of operations of interest.
eventCategory	An optional list of categories of events. This specification, DICOM Supplement 95 and IHE ATNA all provide vocabulary to support the category.
purposeOfUse	An optional list of the purpose(s) of use identified in the audit records.

ParticipantCriteria

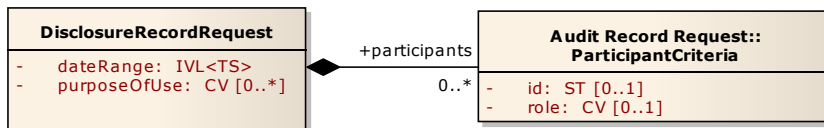
ParticipantCriteria defines the criteria that will be used by the Retrieve Audit Records capability to filter the audit records returned in the response.

425 Table 11 PIM - ParticipantCriteria Attributes

Attribute	Description
id	This is an optional identifier, as expected to be recorded in one or more audit records, of a particular event participant. The identified participant can be active, passive, or an audit source.
role	An optional participant role (e.g. Requestor)

Disclosure Record Request

Figure 8 PIM - Disclosure Record Request Semantic Signifier



430 The Disclosure Record Request is the container class for a message requesting a set of disclosure audit event records from the Audit Service. The request includes zero or more ParticipantCriteria elements to

be used in the request.

Table 12 PIM - Disclosure Record Request Attributes

Attribute	Description
dateRange	A mandatory date interval that denotes the date and time of any audit event records to be included in the response. A starting date is required.
purposeOfUse	An optional list of the purpose(s) of use identified in the audit records.

ParticipantCriteria

435 ParticipantCriteria defines the criteria that will be used by the Retrieve Audit Records capability to filter the audit records returned in the response.

Table 13 PIM - ParticipantCriteria Attributes

Attribute	Description
id	This is an optional identifier, as expected to be recorded in one or more audit records, of a particular event participant. The identified participant can be active, passive, or an audit source.
role	An optional participant role (e.g. Requestor)

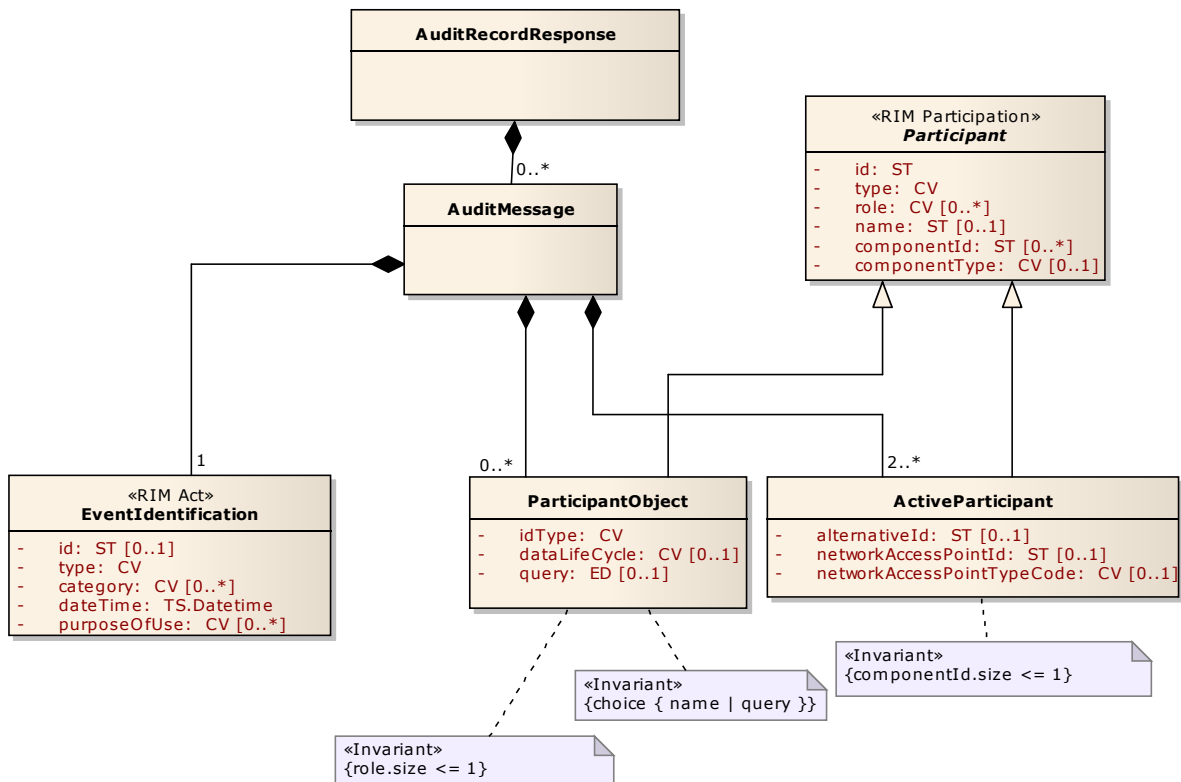
Audit Record Response

The figure below describes the semantic signifier associated with the response to a successful service invocation on both "Retrieve Disclosure Records" and "Retrieve Disclosure-Related Records" capability.

440 DisclosureRecordResponse is the container class that includes the set of disclosure-related records that match the criteria indicated in the Disclosure Record Request and as specified for the Request Disclosure Records service interface in the Computational Viewpoint.

445 EventIdentification and Participant classes can be considered renamed, constrained and extended classes derived from the HL7 RIM Act and Participation backbone classes respectively. RIM Entity/Role class instances associated with Participant instances are referenced through Participant instance attribute values.

Figure 9 PIM - Audit Record Response Semantic Signifier



AuditMessage

450 AuditMessage defines a single auditable event. AuditMessage is expressed through instances of EventIdentification, Active Participant, Participant, and AuditSourceIdentification classes. The AuditMessage reflects HL7 RIM abstract data types, vocabulary and grammar conventions.

N.B. The descriptions associated with attributes align with those from the IHE ATNA profile, which in turn refers to DICOM Supplement 95 and RFC 3881.

455 **EventIdentification**

EventIdentification is the part of the auditable event that describes what was done.

Table 14 PIM - Disclosure Record Response - EventIdentification Attributes

Attribute	Description
id	An optional identifier of the audit event. This may be used as a correlation identifier in the case were a single event resulted in multiple audit event records being generated.
type	The identity of the type of audit event that is described by this instance of AuditMessage.
category	An optional list of coded concepts that can be used to further specialize or generalize the event identifier.
dateTime	The date and time that the event took place as described in DICOM Supplement 95 (ISO TS 12052).
purposeOfUse	An optional value indicating the legitimate purpose for which the information referenced in this audit event can be subsequently used.

Participant

460 This abstract class describes all of the entities associated with the auditable event, whether active or not. As shown in the UML diagram above, Participant acts as the superclass of both ActiveParticipant and ParticipantObject.

Table 15 PIM - Disclosure Record Response - Participant Attributes

Attribute	Description
id	A required attribute that identifies the participant.
role	An optional list of coded roles played by this participant in the event. These include participation roles (e.g. disclosing agent, patient, etc.) as well as those assigned by a Role-Based Access Control (RBAC) security system where appropriate.
type	A concept that specifies the type of entity that is described by this Participant.
name	An optional human-readable name for the Participant.
componentId	An optional, multi-valued attribute containing the identification of any sub-components associated with the participant.
componentType	An optional indicator of the type of sub-component referenced in the componentId attribute.

465 **ActiveParticipant**

This class documents a person or system component that was actively involved from the perspective of accountability for the event. It inherits all of the attributes of the Participant class.

Table 16 PIM - Disclosure Record Response - ActiveParticipant Attributes

Attribute	Description
alternateId	An optional unique identifier. The attribute can be used within an enterprise for authentication purposes, or when the ActiveParticipant plays the role of Audit Source, may serve to further qualify the id attribute.
networkAccessPointId	The logical network identifier associated with the participant.
networkAccessPointTypeCode	The type of network access point associated with the networkAccessPointId.

ParticipantObject

470 The ParticipantObject class describes all of the entities associated with the auditable event, including references to the information potentially disclosed and to the patient.

Table 17 PIM - Disclosure Record Response - ParticipantObject Attributes

Attribute	Description
idType	A coded concept representing the type of value that is being used to identify the participant.
dataLifeCycle	For information reference objects, can indicate the lifecycle state that the information was in at the time of the event.
query	An optional attribute, specifically for query participants. The actual query used. Name and query attributes are mutually exclusive.

Disclosure Record Response

475 The figure below describes the semantic signifier associated with the response to a successful service invocation on both “Retrieve Disclosure Records” capability.

DisclosureRecordResponse is the container class that includes the set of disclosure records that match the criteria indicated in the Disclosure Record Request and as specified for the Request Disclosure Records service interface in the Computational Viewpoint.

480 The model is identical to the Audit Record Response in all areas with the following conformance-related exceptions:

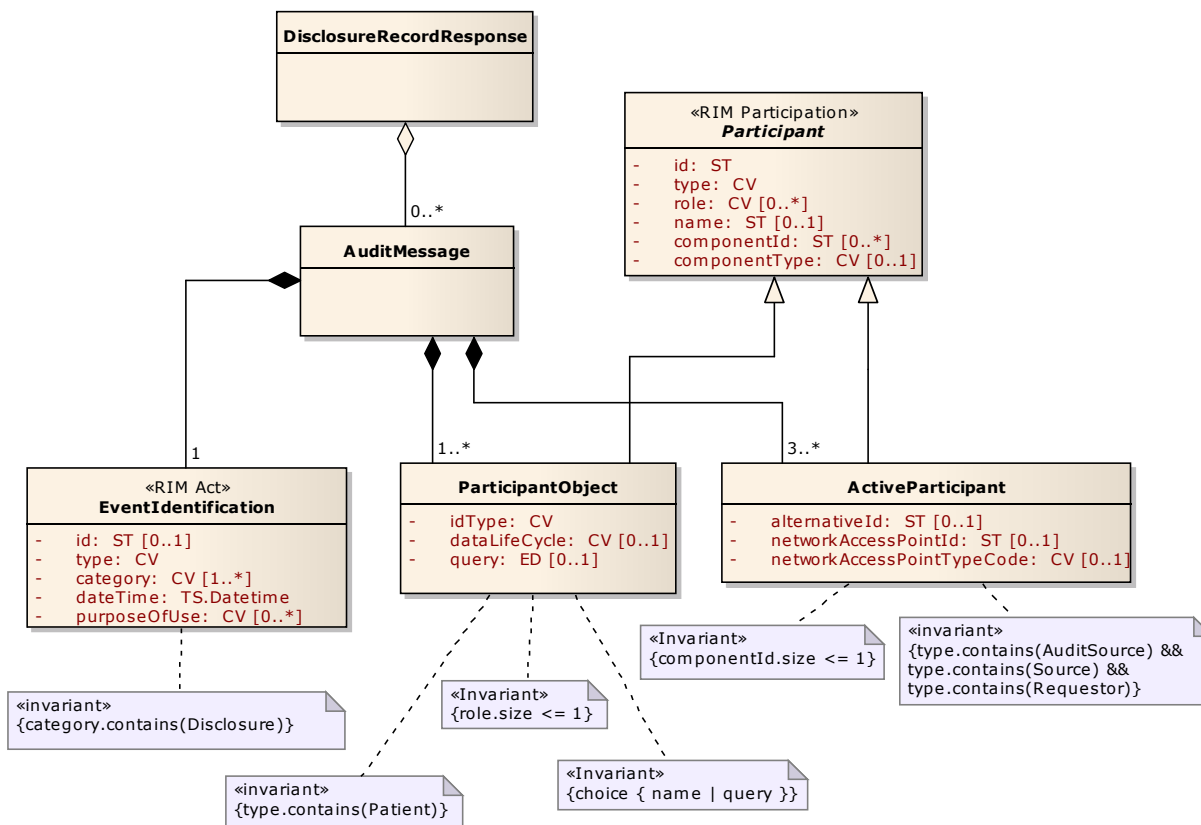
- <CONF-1> A ParticipantObject element representing the Patient shall be contained within each instance of AuditMessage.
- <CONF-2> There shall be a minimum of three (3) ActiveParticipant objects:
- <CONF-3> An ActiveParticipant element describing a Source role shall exist for each AuditMessage returned.
- <CONF-4> An ActiveParticipant element describing an Audit Source role shall exist for each

AuditMessage returned.

<CONF-5> An ActiveParticipant element describing a Requestor role shall exist for each AuditMessage returned.

490

Figure 10 PIM - Disclosure Record Response Semantic Signifier



Idealized Disclosure Record

495 The following tables describe an instance of an audit record which documents a disclosure event specified in a format consistent with the IHE ATNA profile and the DICOM Supplement 95 specification. The scenarios described in the Business Viewpoint have identified the participating roles that would be relevant in a privacy context.

500 **N.B.** One or more Participants identified below may not be available from information contained within the Audit Service while additional Participants may be described. All information related to an event should be returned by the service.

Table 18 Idealized Disclosure Event Record – Audit Object

Audit Object
Event (Disclosure)
Active Participants ¹⁷
Source (Releasing Object/Node) (1..n)
Releasing Agent (0..1)
Receiving Agent (0..1)
Destination (Receiving Object/Node) (0..n)
Requestor (1) – <i>Distinct Active Participant only required if no other Active Participant is identified specifically as a Requestor.</i>
Audit Source (1) – <i>Distinct Audit Source only required if no other Active Participant is identified specifically as an Audit Source.</i>
Participant Objects
Patient (1)
Releasing Custodian/Controller (0..1)
Receiving Custodian/Controller (0..1)
Information Reference (0..n)
Authorization (0..1)

Where:

¹⁷ At least one ActiveParticipant must have the element UserIsRequestor set.

Table 19 Idealized Disclosure Event Record – Audit Event Description

	Field Name	Opt	Value Constraints
Event AuditMessage/ EventIdentification	type	M	Export
	eventDateTime	M	not specialized
	category	M	Disclosure NoDisclosure <No Value> where: Disclosure: Only if the audit event source can authoritatively determine a legal disclosure has occurred. NoDisclosure: Only if the audit event source can authoritatively determine that a legal disclosure has not occurred. <No Value> Otherwise
	purposeOfUse	MC	The purpose(s) for which the information referenced in the audit event was released. This attribute must be populated if known. N.B. Where purposeOfUse is populated, and no Authorization Participant Object exists, the purposeOfUse has been assumed.

505

Table 20 Idealized Disclosure Event Record - Source Participation

	Field Name	Opt	Value Constraints
Source AuditMessage/ ActiveParticipant	Id	M	The process, task, or other ID as used within the local operating system in the local system logs if disclosure was digital.
	role	M	Source. In addition, any Access Control role(s) the entity was operating under during the course of this event, as well as the participation role that the entity played in the event.
	type	U	<i>Not specialized</i>
	alternativeId	U	<i>not specialized</i>
	name	U	<i>not specialized</i>
	userIsRequestor	M	<i>not specialized</i> - One of the ActiveParticipants must be identified as the Requestor.
	networkAccessPointTypeCode	M	The type of NetworkAccessPointID: machine (DNS) name, or IP address
	networkAccessPointId	M	The fully qualified machine name or IP address
	componentId	U	<i>not specialized</i>
	componentType	U	<i>not specialized</i>

Table 21 Idealized Disclosure Event Record - Releasing Agent Participation

	Field Name	Opt	Value Constraints
Releasing Agent (if known) AuditMessage/ ActiveParticipant	Id	M	Identity of the human that was responsible for the release of information.
	Role	M	Releasing Agent. In addition, any Access Control role(s) the entity held during the course of this event, as well as the participation role that the entity played in the event.
	Type	U	<i>not specialized</i>
	alternativeId	U	<i>not specialized</i>
	Name	U	<i>not specialized</i>
	networkAccessPointTypeCode	N/A	
	networkAccessPointId	N/A	
	componentId	N/A	
componentType	N/A		

510 Table 22 Idealized Disclosure Event Record - Receiving Agent Participation

	Field Name	Opt	Value Constraints
Receiving Agent (if known) AuditMessage/ ActiveParticipant	Id	M	Identity of the human that was responsible for the receipt of information.
	Role	M	Receiving Agent. In addition, any Access Control role(s) the entity was operating under during the course of this event, as well as the participation role that the entity played in the event.
	Type	U	<i>not specialized</i>
	alternativeId	U	<i>not specialized</i>
	Name	U	<i>not specialized</i>
	networkAccessPointTypeCode	N/A	
	networkAccessPointId	N/A	
	componentId	N/A	
componentType	N/A		

Table 23 Idealized Disclosure Event Record - Requestor Participation

	Field Name	Opt	Value Constraints
Requestor (only if no other Active Participant is Requestor) AuditMessage/ ActiveParticipant	Id	M	Identity of the human that requested the information
	Role	M	Requestor. In addition, any Access Control role(s) the entity was operating under during the course of this event, as well as any other participation role(s) that the entity played in the event.
	Type	U	not specialized
	alternativeId	U	not specialized
	Name	U	not specialized
	networkAccessPointTypeCode	N/A	
	networkAccessPointId	N/A	
	componentId	N/A	
componentType	N/A		

Table 24 Idealized Disclosure Event Record - Destination Participation

	Field Name	Opt	Value Constraints
Destination AuditMessage/ ActiveParticipant	Id	M	not specialized
	Role	M	Destination. In addition, any Access Control role(s) the entity was operating under during the course of this event, as well as the participation role that the entity played in the event.
	Type	U	not specialized
	alternativeId	U	not specialized
	Name	U	not specialized
	networkAccessPointTypeCode	M	The type of NetworkAccessPointID: machine (DNS) name, or IP address
	networkAccessPointId	M	The fully qualified machine name or IP address
	componentId	U	not specialized
	componentType	U	not specialized

515

Table 25 Idealized Disclosure Event Record - Audit Source Participation

	Field Name	Opt	Value Constraints
Audit Source AuditMessage/ AuditSource	Id	U	<i>not specialized</i>
	Role	M	Audit Source. In addition, any Access Control role(s) the entity was operating under during the course of this event, as well as the participation role that the entity played in the event.
	Type	U	<i>not specialized</i>
	alternativeId	U	<i>not specialized</i>
	Name	U	<i>not specialized</i>
	networkAccessPointTypeCode	M	The type of NetworkAccessPointID: machine (DNS) name, or IP address
	networkAccessPointId	M	The fully qualified machine name or IP address
	componentId	U	<i>not specialized</i>
	componentType	U	<i>not specialized</i>

Table 26 Idealized Disclosure Event Record - Patient Participation

	Field Name	Opt	Value Constraints
Patient AuditMessage/ ParticipantObject	Id	M	The patient ID
	Role	M	Patient
	Type	M	Person
	dataLifeCycle	N/A	<i>not specialized</i>
	idType	M	The type of Patient identifier
	Name	U	<i>not specialized</i>
	Query	U	<i>not specialized</i>
	componentId	U	<i>not specialized</i>
	componentType	U	<i>not specialized</i>

520

Table 27 Idealized Disclosure Event Record - Releasing Custodian/Controller Participation

	Field Name	Opt	Value Constraints
Releasing Custodian / Controller (if known) AuditMessage/ ParticipantObject	Id	M	The organization identifier
	Role	M	Releasing Custodian/Controller
	Type	M	Organization
	<i>dataLifeCycle</i>	N/A	
	idType	M	The type of Organization identifier
	<i>Name</i>	U	<i>not specialized</i>
	<i>Query</i>	U	<i>not specialized</i>
	<i>componentId</i>	U	<i>not specialized</i>
	<i>componentType</i>	U	<i>not specialized</i>

Table 28 Idealized Disclosure Event Record - Receiving Custodian/Controller Participation

	Field Name	Opt	Value Constraints
Receiving Custodian / Controller (if known) (AuditMessage/ ParticipantObject)	Id	M	The organization identifier
	Role	M	Receiving Custodian/Controller
	Type	M	Organization
	<i>dataLifeCycle</i>	N/A	
	idType	M	The type of Organization identifier
	<i>Name</i>	U	<i>not specialized</i>
	<i>Query</i>	U	<i>not specialized</i>
	<i>componentId</i>	U	<i>not specialized</i>
	<i>componentType</i>	U	<i>not specialized</i>

	Field Name	Opt	Value Constraints
Information Reference (AuditMessage/ ParticipantObject)	Id	M	An identifier that uniquely identifies the information bundle that was disclosed for an individual patient.
	Role	M	Appropriate to the type of information referenced
	Type	M	System Object
	<i>dataLifeCycle</i>	U	<i>not specialized</i>
	idType	M	<i>not specialized</i>
	Name	U	<i>not specialized</i>
	Query	U	<i>not specialized</i>
	<i>componentId</i>	MC	<i>If the information bundle contains known and identifiable sub-components, this attribute must contain the list of the identifiers of those sub-components.</i>
	<i>componentType</i>	MC	<i>If componentId contains information, this attribute must contain the type of sub-components identified.</i>

The Authorization participant identifies the person, organization, or policy decision that ensured that the disclosure was authorized.

Table 30 Idealized Disclosure Event Record - Authorization Participation

	Field Name	Opt	Value Constraints
Authorization (if known) (AuditMessage/ ParticipantObject)	Id	M	The unique identity off the Authorizing entity
	Role	M	Appropriate for the type of entity referenced
	Type	M	<i>not specialized.</i>
	<i>dataLifeCycle</i>	N/A	
	idType	M	The type of entity identifier contained in the "id" attribute
	Name	U	<i>not specialized</i>
	Query	N/A	
	<i>componentId</i>	N/A	
	<i>componentType</i>	N/A	

The Opt column in the tables above describes the optionality of attributes and is consistent with similar tables in [DICOM95-2010] and [IHE-ITI-2A]. The following values are used:

M – Mandatory – the attribute must be supplied,

C – Conditional – the attribute is optional.

535 MC – Mandatory Conditional – the value must be supplied if some condition is met,

U – (User) Optional – equivalent to Conditional.

N/A – The attribute is not applicable in this context

3.2.4 Dynamic Model

540 The records describing auditable events are static, and in fact most healthcare audit standards specify that the audit record log should be made immutable. No dynamic model is applicable.

3.3 Platform Specific Level

3.3.1 Semantic Signifiers

Submit Audit Record

545 This semantic signifier leverages and extends the IHE ITI-20 transaction as the basis for communicating audit event information to and from the Audit Service. The IHE ITI-20 transaction is based upon DICOM Supplement 95, and both of them on the work done in RFC 3881. The schema defined herein extends the existing work, with two additions, specifically:

- An optional “purposeOfUse” attribute on the EventIdentification element, and
- An optional “ActiveParticipantTypeCode” attribute on the ActiveParticipant element.

Transformations

550 <CONF-6> Tables 31 to 34, below define normative PIM to PSM transformations to identify the relationships between the Platform Independent Model describing the AuditMessage semantic content and the AuditMessage schema as defined herein.

Table 31 Submit Audit Record - PIM to PSM Transformation - AuditRecordRequest

Signifier	PIM Classifier	PIM Attribute	PSM Classifier	PSM Attribute	PIM -> PSM Transformation
AuditRecordRequest	AuditRecordRequest		RetrieveAuditRecords.Request		Rename classifier
		dateRange		dateRange	As is
		processingMode		processingMode	As is
		eventType		EventId	Rename attribute
		eventCategory		EventType	Rename attribute
		purposeOfUse		purposeOfUse	As is
	ParticipantCriteria		ParticipantCriteria		As is
		id		id	As is
		role		role	As is

Table 32 Submit Audit Record - PIM to PSM Transformation - DisclosureRecordRequest

Signifier	PIM Classifier	PIM Attribute	HL7/ATNA Classifier	HL7/ATNA Attribute	PIM -> PSM Transformation
DisclosureRecordRequest	DisclosureRecordRequest		RetrieveAuditRecords.Request		Rename classifier
		dateRange		dateRante	As is
		purposeOfUse		purposeOfUse	As is
	ParticipantCriteria		ParticipantCriteria		As is
		id		id	As is
		role		role	As is

555

Table 33 Submit Audit Record - PIM to PSM Transformation - AuditRecordResponse

Signifier	PIM Classifier	PIM Attribute	HL7/ATNA Classifier	HL7/ATNA Attribute	PIM -> PSM Transformation
AuditRecordResponse	AuditRecordResponse		RetrieveAuditRecords.Response		Rename classifier
	AuditMessage		AuditMessage		As is

Table 34 Submit Audit Record - PIM to PSM Transformation - DisclosureRecordResponse

Signifier	PIM Classifier	PIM Attribute	HL7/ATNA Classifier	HL7/ATNA Attribute	PIM -> PSM Transformation
DisclosureRecordResponse	DisclosureRecordResponse		RetrieveDisclosureRecords.Response		Rename classifier
	AuditMessage		AuditMessage		As is

560 Table 35 Submit Audit Record - PIM to PSM Transformation - AuditMessage

Signifier	PIM Classifier	PIM Attribute	HL7/ATNA Classifier	HL7/ATNA Attribute	PIM -> PSM Transformation	
AuditMessage	EventIdentification		EventIdentification		As is	
		id			No transformation	
		type		EventId	Rename attribute	
		category		EventType	Rename attribute	
		dateTime		EventDateTime	Rename attribute	
		purposeOfUse		PurposeOfUse	Rename attribute	
	ParticipantObject		ParticipantObjectIdentification			Rename classifier
		id		ParticipantObjectID	Rename attribute	
		type		ParticipantObjectTypeCode	Rename attribute	
		role		ParticipantObjectTypeCodeRole	Rename attribute	
		name		ParticipantObjectName	Rename attribute	
		idType		ParticipantObjectIDTypeCode	Rename attribute	
		dataLifeCycle		ParticipantObjectDataLifeCycle	Rename attribute	
		query		ParticipantObjectQuery	Rename attribute	
		componentId		MPPS.UID	Rename attribute if componentType == MPPS	
		componentId		Accession.Number	Rename attribute if componentType == Accession	

	componentId	SOPClass.UID	Rename attribute if componentType == SOPClass
	componentId	ParticipantObjectContainsStudy.StudyIDs.UID	Rename attribute if componentType == ParticipantObjectContainsStudy
	componentType		Used to in componentId transformation.
ActiveParticipantObject		ActiveParticipant	Rename classifier if role does not contain Audit Source
	id	UserID	Rename attribute
	type	ActiveParticipantTypeCode	Rename attribute
	role	RoleIDCode	Rename attribute
	name	UserName	Rename attribute
	alternativeId	AlternativeUserID	Rename attribute
	networkAccessPointId	NetworkAccessPointID	Rename attribute
	networkAccessPointTypeCode	NetworkAccessPointTypeCode	Rename attribute
	componentId	MediaIdentifier	Rename attribute
	componentType	MediaType	Rename attribute
ActiveParticipantObject		AuditSourceIdentification	Rename classifier if role contains Audit Source
	id	AuditSourceID	Rename attribute
	type	code	Rename attribute

	role	Used to select transform classifier
	name	No transformation
	alternativeId	AuditEnterpriseSiteID Rename attribute
	networkAccessPointId	No transformation
	networkAccessPointTypeCode	No transformation
	componentId	No transformation
	componentType	No transformation

Audit Recorder Profile - Audit Message

<CONF-7> Any Audit Service implementation that claims conformance to the HL7 Audit Recorder Profile shall provide the ability for a client to invoke the operation using the AuditMessage schema as defined in Figure 11 PSM - HL7 Audit Recorder Profile - Audit Message Schema, below.

565

Figure 11 PSM - HL7 Audit Recorder Profile - Audit Message Schema

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">
  <!-- Translation and extension of the DICOM Supplement 95 Schema (March 2010) -->
  <xs:element name="AuditMessage" type="AuditMessageType"/>
<!-- The basic message -->
  <xs:complexType name="AuditMessageType">
    <xs:sequence>
      <xs:element ref="EventIdentification"/>
      <xs:element maxOccurs="unbounded" ref="ActiveParticipant"/>
      <xs:element ref="AuditSourceIdentification"/>
      <xs:element minOccurs="0" maxOccurs="unbounded"
ref="ParticipantObjectIdentification"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="EventIdentification" type="EventIdentificationContents"/>
  <xs:element name="ActiveParticipant" type="ActiveParticipantContents"/>
  <xs:element name="AuditSourceIdentification">
    <xs:complexType>
      <xs:attributeGroup ref="AuditSourceIdentificationContents"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="ParticipantObjectIdentification"
type="ParticipantObjectIdentificationContents"/>

<!--
  This defines the coded value type. It can be replaced by customization. OID
  pattern is not used because
  many implementations do not support pattern yet. This is split this was to
  simplify pattern substitution
  where specific code value constraints are made, and uses where only a code is
  used rather than the entire set.
-->
  <xs:attributeGroup name="other-csd-attributes">
    <xs:attribute name="codeSystemName" use="required" type="xs:token"/>
    <xs:attribute name="displayName" type="xs:token"/>
    <xs:attribute name="originalText" use="required" type="xs:token"/>
  </xs:attributeGroup>
  <!-- Note: this also corresponds to DICOM "Meaning" -->
  <xs:attributeGroup name="CodedValueType">
    <xs:attribute name="csd-code" use="required" type="xs:token"/>
    <xs:attributeGroup ref="other-csd-attributes"/>
  </xs:attributeGroup>

  <!-- Define the event identification, used later -->
  <xs:complexType name="EventIdentificationContents">
    <xs:sequence>
      <xs:element ref="EventID"/>
      <xs:element minOccurs="0" maxOccurs="unbounded" ref="EventTypeCode"/>
      <xs:element minOccurs="0" ref="EventOutcomeDescription"/>
      <!-- HL7 Extension -->
      <xs:element minOccurs="0" maxOccurs="unbounded" name="PurposeOfUse">
        <xs:complexType>
          <xs:attributeGroup ref="CodedValueType"/>
        </xs:complexType>
      </xs:element>
      <!-- End of HL7 Extension -->
    </xs:sequence>
    <xs:attribute name="EventActionCode">
      <xs:simpleType>
        <xs:restriction base="xs:token">

```

```

    <xs:enumeration value="C">
      <xs:annotation>
        <xs:documentation>Create</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="R">
      <xs:annotation>
        <xs:documentation>Read</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="U">
      <xs:annotation>
        <xs:documentation>Update</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="D">
      <xs:annotation>
        <xs:documentation>Delete</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="E">
      <xs:annotation>
        <xs:documentation>Execute</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="EventDateTime" use="required" type="xs:dateTime"/>
<xs:attribute name="EventOutcomeIndicator" use="required">
  <xs:simpleType>
    <xs:restriction base="xs:token">
      <xs:enumeration value="0">
        <xs:annotation>
          <xs:documentation>Nominal Success (use if status otherwise unknown or
ambiguous)</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="4">
        <xs:annotation>
          <xs:documentation>Minor failure (per reporting application
definition)</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="8">
        <xs:annotation>
          <xs:documentation>Serious failure (per reporting application
definition)</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="12">
        <xs:annotation>
          <xs:documentation>Major failure, (reporting application now
unavailable)</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
</xs:complexType>
<xs:element name="EventID">
  <xs:complexType>
    <xs:attributeGroup ref="CodedValueType"/>
  </xs:complexType>
</xs:element>

```

```

<xs:element name="EventTypeCode">
  <xs:complexType>
    <xs:attributeGroup ref="CodedValueType"/>
  </xs:complexType>
</xs:element>
<xs:element name="EventOutcomeDescription" type="xs:string"/>

<!--
  Define AuditSourceIdentification, used later
  Note: This includes one constraint that cannot be represented yet in RNC. The
  use of a token other
  than the specified codes is permitted only if the codeSystemName is
  present.
  Note: This has no elements, only attributes.
-->
<xs:attributeGroup name="AuditSourceIdentificationContents">
  <xs:attribute name="code" use="required">
    <xs:simpleType>
      <xs:union>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="1">
              <xs:annotation>
                <xs:documentation>End-user display device, diagnostic
device</xs:documentation>
              </xs:annotation>
            </xs:enumeration>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="2">
              <xs:annotation>
                <xs:documentation>Data acquisition device or
instrument</xs:documentation>
              </xs:annotation>
            </xs:enumeration>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="3">
              <xs:annotation>
                <xs:documentation>web Server process or thread</xs:documentation>
              </xs:annotation>
            </xs:enumeration>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="4">
              <xs:annotation>
                <xs:documentation>Application Server process or
thread</xs:documentation>
              </xs:annotation>
            </xs:enumeration>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="5">
              <xs:annotation>
                <xs:documentation>Database Server process or
thread</xs:documentation>
              </xs:annotation>
            </xs:enumeration>
          </xs:restriction>
        </xs:simpleType>
      </xs:union>
    </xs:attribute>
  </xs:attributeGroup>

```

```

        </xs:annotation>
    </xs:enumeration>
</xs:restriction>
</xs:simpleType>
<xs:simpleType>
    <xs:restriction base="xs:token">
        <xs:enumeration value="6">
            <xs:annotation>
                <xs:documentation>Security server, e.g., a domain
controller</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
    </xs:restriction>
</xs:simpleType>
<xs:simpleType>
    <xs:restriction base="xs:token">
        <xs:enumeration value="7">
            <xs:annotation>
                <xs:documentation>ISO level 1-3 network component</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
    </xs:restriction>
</xs:simpleType>
<xs:simpleType>
    <xs:restriction base="xs:token">
        <xs:enumeration value="8">
            <xs:annotation>
                <xs:documentation>ISO level 4-6 operating
software</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
    </xs:restriction>
</xs:simpleType>
<xs:simpleType>
    <xs:restriction base="xs:token">
        <xs:enumeration value="9">
            <xs:annotation>
                <xs:documentation>External Source, other, or
unknown</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
    </xs:restriction>
</xs:simpleType>
<xs:restriction base="xs:token"/>
</xs:simpleType>
</xs:union>
</xs:simpleType>
</xs:attribute>

    <xs:attribute name="codeSystemName" type="xs:token">
        <xs:annotation>
            <xs:documentation>If these are present, they define the meaning of
code</xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attribute name="displayName" type="xs:token"/>
    <xs:attribute name="originalText" type="xs:token"/>

    <xs:attribute name="AuditEnterpriseSiteID" type="xs:token"/>

    <xs:attribute name="AuditSourceID" use="required" type="xs:token"/>
</xs:attributeGroup>
<!-- Define ActiveParticipantType, used later -->
<xs:complexType name="ActiveParticipantContents">

```

```

<xs:sequence>
  <xs:element minOccurs="0" maxOccurs="unbounded" ref="RoleIDCode"/>
  <xs:element minOccurs="0" ref="MediaIdentifier"/>
</xs:sequence>
<xs:attribute name="UserID" use="required"/>
<xs:attribute name="ActiveParticipantObjectTypeCode">
  <xs:simpleType>
    <xs:restriction base="xs:token">
      <xs:enumeration value="1">
        <xs:annotation>
          <xs:documentation>Person</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="2">
        <xs:annotation>
          <xs:documentation>System object</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="3">
        <xs:annotation>
          <xs:documentation>Organization</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="4">
        <xs:annotation>
          <xs:documentation>Other</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<xs:attribute name="AlternativeUserID"/>
<xs:attribute name="UserName"/>
<xs:attribute name="UserIsRequestor" type="xs:boolean"/>
<xs:attribute name="NetworkAccessPointID" type="xs:token"/>
<xs:attribute name="NetworkAccessPointTypeCode">
  <xs:simpleType>
    <xs:restriction base="xs:token">
      <xs:enumeration value="1">
        <xs:annotation>
          <xs:documentation>Machine Name, including DNS name</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="2">
        <xs:annotation>
          <xs:documentation>IP Address</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="3">
        <xs:annotation>
          <xs:documentation>Telephone Number</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="4">
        <xs:annotation>
          <xs:documentation>Email address</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="5">
        <xs:annotation>
          <xs:documentation>URI (user directory, HTTP-PUT, ftp,
etc.)</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>

```

```

    </xs:simpleType>
  </xs:attribute>
</xs:complexType>
<xs:element name="RoleIDCode">
  <xs:complexType>
    <xs:attributeGroup ref="CodedValueType"/>
  </xs:complexType>
</xs:element>
<xs:element name="MediaIdentifier">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="MediaType"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="MediaType">
  <xs:complexType>
    <xs:attributeGroup ref="CodedValueType"/>
  </xs:complexType>
</xs:element>
<!--
  The BinaryValuePair is used in ParticipantObject descriptions to capture
  parameters.
  All values (even those that are normally plain text) are encoded as
  xsd:base64Binary. This
  is to preserve details of encoding (e.g., nulls) and to protect against text
  contents that contain
  XML fragments. These are known attack points against applications, so security
  logs
  can be expected to need to capture them without modification by the audit encoding
  process.
-->
<xs:attributeGroup name="ValuePair">
  <xs:annotation>
    <xs:documentation>URI (user directory, HTTP-PUT, ftp, etc.)</xs:documentation>
  </xs:annotation>
  <xs:attribute name="type" use="required" type="xs:token"/>
  <xs:attribute name="value" use="required" type="xs:base64Binary"/>
</xs:attributeGroup>
<!-- used to encode potentially binary, mal-formed XML text, etc. -->
<!-- Define ParticipantObjectIdentification, used later -->
<!-- Participant Object Description, used later -->
<xs:group name="DICOMObjectDescriptionContents">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="unbounded" ref="MPPS"/>
    <xs:element minOccurs="0" maxOccurs="unbounded" ref="Accession"/>
    <xs:element ref="SOPClass"/>
    <xs:element ref="ParticipantObjectContainsStudy"/>
    <xs:element minOccurs="0" ref="Encrypted"/>
    <xs:element minOccurs="0" ref="Anonymized"/>
  </xs:sequence>
</xs:group>
<xs:element name="MPPS">
  <xs:complexType>
    <xs:attribute name="UID" use="required" type="xs:token"/>
  </xs:complexType>
</xs:element>
<xs:element name="Accession">
  <xs:complexType>
    <xs:attribute name="Number" use="required" type="xs:token"/>
  </xs:complexType>
</xs:element>
<xs:element name="SOPClass">
  <xs:complexType>
    <xs:sequence>

```

```

    <xs:element minOccurs="0" maxOccurs="unbounded" ref="Instance"/>
  </xs:sequence>
  <xs:attribute name="UID" type="xs:token"/>
  <xs:attribute name="NumberOfInstances" use="required" type="xs:integer"/>
</xs:complexType>
</xs:element>
<xs:element name="Instance">
  <xs:complexType>
    <xs:attribute name="UID" use="required" type="xs:token"/>
  </xs:complexType>
</xs:element>
<xs:element name="ParticipantObjectContainsStudy">
  <xs:complexType>
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="unbounded" ref="StudyIDs"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="StudyIDs">
  <xs:complexType>
    <xs:attribute name="UID" use="required" type="xs:token"/>
  </xs:complexType>
</xs:element>
<xs:element name="Encrypted" type="xs:boolean"/>
<xs:element name="Anonymized" type="xs:boolean"/>
<xs:complexType name="ParticipantObjectIdentificationContents">
  <xs:sequence>
    <xs:element ref="ParticipantObjectTypeCode"/>
    <xs:choice>
      <xs:element ref="ParticipantObjectName"/>
      <xs:element ref="ParticipantObjectQuery"/>
    </xs:choice>
    <xs:element minOccurs="0" maxOccurs="unbounded" ref="ParticipantObjectDetail"/>
    <xs:element minOccurs="0" maxOccurs="unbounded"
ref="ParticipantObjectDescription"/>
    <xs:group ref="DICOMObjectDescriptionContents"/>
  </xs:sequence>
  <xs:attribute name="ParticipantObjectID" use="required" type="xs:token"/>
  <xs:attribute name="ParticipantObjectTypeCode">
    <xs:simpleType>
      <xs:restriction base="xs:token">
        <xs:enumeration value="1">
          <xs:annotation>
            <xs:documentation>Person</xs:documentation>
          </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="2">
          <xs:annotation>
            <xs:documentation>System object</xs:documentation>
          </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="3">
          <xs:annotation>
            <xs:documentation>Organization</xs:documentation>
          </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="4">
          <xs:annotation>
            <xs:documentation>Other</xs:documentation>
          </xs:annotation>
        </xs:enumeration>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
  <xs:attribute name="ParticipantObjectTypeCodeRole">

```

```

<xs:annotation>
  <xs:documentation>optional role</xs:documentation>
</xs:annotation>
<xs:simpleType>
  <xs:restriction base="xs:token">
    <xs:enumeration value="1">
      <xs:annotation>
        <xs:documentation>Patient</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="2">
      <xs:annotation>
        <xs:documentation>Location</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="3">
      <xs:annotation>
        <xs:documentation>Report</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="4">
      <xs:annotation>
        <xs:documentation>Resource</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="5">
      <xs:annotation>
        <xs:documentation>Master File</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="6">
      <xs:annotation>
        <xs:documentation>User</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="7">
      <xs:annotation>
        <xs:documentation>List</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="8">
      <xs:annotation>
        <xs:documentation>Doctor</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="9">
      <xs:annotation>
        <xs:documentation>Subscriber</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="10">
      <xs:annotation>
        <xs:documentation>guarantor</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="11">
      <xs:annotation>
        <xs:documentation>Security User Entity</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="12">
      <xs:annotation>
        <xs:documentation>Security User Group</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
</xs:simpleType>

```

```

<xs:enumeration value="13">
  <xs:annotation>
    <xs:documentation>Security Resource</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="14">
  <xs:annotation>
    <xs:documentation>Security Granulativity Definition</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="15">
  <xs:annotation>
    <xs:documentation>Provider</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="16">
  <xs:annotation>
    <xs:documentation>Report Destination</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="17">
  <xs:annotation>
    <xs:documentation>Report Library</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="18">
  <xs:annotation>
    <xs:documentation>Schedule</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="19">
  <xs:annotation>
    <xs:documentation>Customer</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="20">
  <xs:annotation>
    <xs:documentation>Job</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="21">
  <xs:annotation>
    <xs:documentation>Job Stream</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="22">
  <xs:annotation>
    <xs:documentation>Table</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="23">
  <xs:annotation>
    <xs:documentation>Routing Criteria</xs:documentation>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="24">
  <xs:annotation>
    <xs:documentation>Query</xs:documentation>
  </xs:annotation>
</xs:enumeration>
</xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="ParticipantObjectDataLifeCycle">
  <xs:annotation>

```

```

    <xs:documentation>optional life cycle stage</xs:documentation>
  </xs:annotation>
</xs:simpleType>
<xs:restriction base="xs:token">
  <xs:enumeration value="1">
    <xs:annotation>
      <xs:documentation>Origination, Creation</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="2">
    <xs:annotation>
      <xs:documentation>Import/ Copy</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="3">
    <xs:annotation>
      <xs:documentation>Amendment</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="4">
    <xs:annotation>
      <xs:documentation>Verification</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="5">
    <xs:annotation>
      <xs:documentation>Translation</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="6">
    <xs:annotation>
      <xs:documentation>Access/Use</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="7">
    <xs:annotation>
      <xs:documentation>De-identification</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="8">
    <xs:annotation>
      <xs:documentation>Aggregation, summarization,
derivation</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="9">
    <xs:annotation>
      <xs:documentation>Report</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="10">
    <xs:annotation>
      <xs:documentation>Export</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="11">
    <xs:annotation>
      <xs:documentation>Disclosure</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
  <xs:enumeration value="12">
    <xs:annotation>
      <xs:documentation>Receipt of Disclosure</xs:documentation>
    </xs:annotation>
  </xs:enumeration>
</xs:restriction>

```

```

    <xs:enumeration value="13">
      <xs:annotation>
        <xs:documentation>Archiving</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="14">
      <xs:annotation>
        <xs:documentation>Logical deletion</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="15">
      <xs:annotation>
        <xs:documentation>Permanent erasure, physical
destruction</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="ParticipantObjectSensistity" type="xs:token"/>
</xs:complexType>
<xs:element name="ParticipantObjectTypeCode">
  <xs:complexType>
    <xs:attributeGroup ref="CodedValueType"/>
  </xs:complexType>
</xs:element>
<xs:element name="ParticipantObjectName" type="xs:token"/>
<xs:element name="ParticipantObjectQuery" type="xs:base64Binary"/>
<xs:element name="ParticipantObjectDetail">
  <xs:complexType>
    <xs:attributeGroup ref="ValuePair"/>
  </xs:complexType>
</xs:element>
<xs:element name="ParticipantObjectDescription" type="xs:token"/>
</xs:schema>

```

RetrieveAuditRecords

- 570 <CONF-8> Any Audit Service implementation that claims conformance to the HL7 Audit Reporter Profile shall provide the ability for a client to invoke the RetrieveAuditRecords operation with the schema as identified in Figure 12 PSM – HL7 Audit Reporter Profile - RetrieveAuditRecords Schema, below.

Figure 12 PSM – HL7 Audit Reporter Profile - RetrieveAuditRecords Schema

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:h17-org:v3"
  targetNamespace="urn:h17-org:v3"
  elementFormDefault="qualified">

  <xs:include schemaLocation="./V3_PASS_AuditMessage.xsd"/>
  <xs:include schemaLocation="../coreschemas/datatypes.xsd"/>

  <xs:element name="RetrieveAuditRecords.request"
type="RetrieveAuditRecords.requestType"/>
  <xs:element name="RetrieveAuditRecords.response"
type="RetrieveAuditRecords.responseType"/>

  <!-- retrieveAuditRecords Request Semantic Signifier -->
  <xs:complexType name="RetrieveAuditRecords.requestType">
    <xs:sequence>

```

```

        <xs:element name="dateRange" type="IVL_TS"/>
        <xs:element name="processingMode" type="CS" minOccurs="0" maxOccurs="1"/>
        <xs:element name="EventID" type="CV" minOccurs="0"
maxOccurs="unbounded">
            <xs:annotation>
                <xs:documentation>(HL7 PIM)AuditRecordRequest.eventType =>
(ATNA) EventIdentification.EventId </xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="EventTypeCode" type="CV" minOccurs="0"
maxOccurs="unbounded">
            <xs:annotation>
                <xs:documentation>(HL7 PIM)AuditRecordRequest.eventCategory
=> (ATNA) EventIdentification.EventTypeCode </xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="purposeOfUse" type="CV" minOccurs="0"
maxOccurs="unbounded"/>
        <xs:element name="participants"
type="RetrieveAuditRecords.participantCriteriaType" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<!-- retrieveDisclosureRecords Response Semantic Signifier -->
<xs:complexType name="RetrieveAuditRecords.responseType">
    <xs:sequence>
        <xs:element name="auditMessage" type="AuditMessageType" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="RetrieveAuditRecords.participantCriteriaType">
    <xs:sequence>
        <xs:element name="id" type="ST" minOccurs="0" maxOccurs="1">
            <xs:annotation>
                <xs:documentation>
                    (HL7 PIM)DisclosureRecordRequest.ParticipantCriteria.id =>
any of:
                    1. (ATNA) ActiveParticipantEventIdentification.UserID,
or
                    2. (ATNA) ActiveParticipantEventIdentification.UserID, or
                    3. (ATNA) AuditSourceIdentification.AuditSourceID, or
                    4. (ATNA) AuditSourceIdentification.EnterpriseSourceID,
or
                    5. (ATNA)
ParticipantObjectIdentification.ParticipantObjectID
                </xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="role" type="CV" minOccurs="0" maxOccurs="1">
            <xs:annotation>
                <xs:documentation>
                    (HL7 PIM)DisclosureRecordRequest.role => any of:
                    1. (ATNA)
ActiveParticipantEventIdentification.RoleIDCode, or
                    2. (ATNA)
ParticipantObjectIdentification.ParticipantObjectTypeCodeRole
                </xs:documentation>
            </xs:annotation>
        </xs:element>
    </xs:sequence>
</xs:complexType>
</xs:schema>

```

RetrieveDisclosureRecords

<CONF-9> Any Audit Service implementation that claims conformance to the HL7 Audit Reporter Profile shall provide the ability for a client to invoke the retrieveDisclosureRecords operation with the schema as identified in **Error! Reference source not found.**

Figure 13 PSM - HL7 Audit Reporter Profile - RetrieveDisclosureRecords Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:h17-org:v3"
  targetNamespace="urn:h17-org:v3"
  elementFormDefault="qualified">

  <xs:include schemaLocation="./V3_PASS_AuditMessage.xsd"/>
  <xs:include schemaLocation="..coreschemas/datatypes.xsd"/>

  <xs:element name="RetrieveDisclosureRecords.request"
    type="RetrieveDisclosureRecords.requestType"/>
  <xs:element name="RetrieveDisclosureRecords.response"
    type="RetrieveDisclosureRecords.responseType"/>

  <!-- retrieveDisclosureRecords Request Semantic Signifier -->
  <xs:complexType name="RetrieveDisclosureRecords.requestType">
    <xs:sequence>
      <xs:element name="dateRange" type="IVL_TS" minOccurs="1" maxOccurs="1"/>
      <xs:element name="processingMode" type="CS" maxOccurs="1"/>
      <xs:element name="purposeOfUse" type="CV" minOccurs="0"
maxOccurs="unbounded"/>
      <xs:element name="participants"
type="RetrieveDisclosureRecords.participantCriteriaType" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <!-- retrieveDisclosureRecords Response Semantic Signifier -->
  <xs:complexType name="RetrieveDisclosureRecords.responseType">
    <xs:sequence>
      <xs:element name="auditMessage" type="AuditMessageType" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="RetrieveDisclosureRecords.participantCriteriaType">
    <xs:sequence>
      <xs:element name="id" type="ST" minOccurs="0" maxOccurs="1">
        <xs:annotation>
          <xs:documentation>
            (HL7 PIM)DisclosureRecordRequest.ParticipantCriteria.id =>
any of:
          1. (ATNA) ActiveParticipantEventIdentification.UserID,
or
          2. (ATNA) ActiveParticipantEventIdentification.UserID, or
          3. (ATNA) AuditSourceIdentification.AuditSourceID, or
          4. (ATNA) AuditSourceIdentification.EnterpriseSourceID,
or
          5. (ATNA)
ParticipantObjectIdentification.ParticipantObjectID
        </xs:documentation>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
```

```

        </xs:annotation>
    </xs:element>
    <xs:element name="role" type="CV" minOccurs="0" maxOccurs="1">
        <xs:annotation>
            <xs:documentation>
                (HL7 PIM)DisclosureRecordRequest.role => any of:
                1. (ATNA)
                ActiveParticipantEventIdentification.RoleIDCode, or
                2. (ATNA)
                ParticipantObjectIdentification.ParticipantObjectTypeCodeRole
            </xs:documentation>
        </xs:annotation>
    </xs:element>
</xs:sequence>
</xs:complexType>
</xs:schema>

```

Computational Viewpoint

4.1 Overview

585 A computational viewpoint on a SAIF/RM-ODP¹⁸ system and its environment is a specification that enables distribution of the functional behavior of the system into service components that interact at interfaces. In the computational viewpoint, applications and business process realizations consist of configurations of interacting service components reflecting business roles participating in service collaborations.

590 4.2 Conceptual Level

4.2.1 Capabilities

This section describes the behavior that has been identified from the requirements. The attributes of Accountability Type, Role, and Dependencies act to provide input to determining what collaborations may be required to ensure that any contract associated with the capability is fulfilled.

595 *Submit Audit Record*

Name	Submit Audit Record
Description	Receive an Audit Message and process it in accordance with implementation policy.
Accountability Type	Event record receipt
Role	Audit Event Handler
Obligations	To accept audit messages and process them in accordance with implementation policy.
Community	All Audit Event Sources
Prohibitions	None
Dependencies	None
Precondition	A consistent time source is available
Constraints	None
Postconditions	The audit event information has been treated in accordance with implementation policy.
Exception Conditions	None

¹⁸ RM-ODP – ITU-T X.911 ISO/IEC 15414 – Open Distributed Processing – Reference Model

Retrieve Audit Records

Name	Retrieve Audit Records
Description	Accepts a request to receive audit information.
Accountability Type	Audit Event Post-Processing
Role	Audit Information Source
Obligations	To provide audit event information to authorized commissioners.
Community	Healthcare Audit components, related systems, and users.
Prohibitions	
Dependencies	
Precondition	The service must have the capability to provide security controls that will assist in minimizing the risk of unauthorized disclosure of this information while in transit from the Audit Service to the requesting component.
Constraints	
Postconditions	All audit event information that meets the request criteria and the requesting party has authorization to access has been returned.
Exception Conditions	Invalid input was received

Retrieve Disclosure Records

Name	Retrieve Disclosure Records
Description	Accepts a request to receive information that directly indicates that a disclosure of personal information has occurred.
Accountability Type	Privacy Accounting
Role	Disclosure Accounting Information Source
Obligations	To provide audit event information that identifies confirmed disclosures of personal information.
Community	Privacy Accounting components and users.
Prohibitions	
Dependencies	
Precondition	The service must have the capability to provide security controls that will assist in minimizing the risk of unauthorized disclosure of this information while in transit from the Audit Service to the requesting component.
Constraints	
Postconditions	All audit event information that directly identifies confirmed disclosures of personal information has been sent to the invoking party.

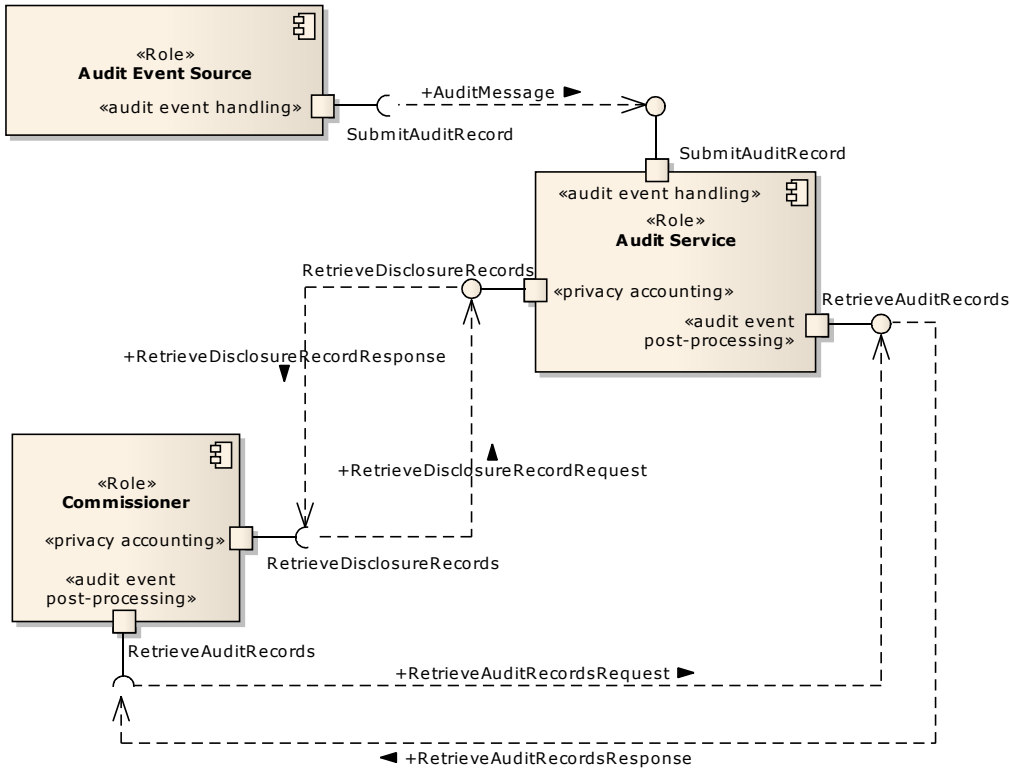
Exception Conditions	Invalid input was received
-----------------------------	----------------------------

600 **4.2.2 Collaboration Analysis**

This section discusses the interactions between capabilities classified by roles. It also identifies the obligations associated with those roles as well as the interdependencies of the capabilities.

The diagram below illustrates these interactions.

Figure 14 Audit Service Capabilities



605

Submit Audit Record

The capability is invoked by any Audit Event Source. No application response is expected and there is no expectation by the client with respect to the impact that the invocation has.

Retrieve Disclosure Records

610 The capability is invoked by an authorized component, identified in the diagram as a Commissioner. The Audit Service will return event information that relates to confirmed disclosures, scoped by the criteria provided in the request.

Retrieve Audit Records

615 The capability is invoked by an authorized component, identified in the diagram as a Commissioner. The expectation is that the invocation will return all audit events that match the criteria outlined in the request.

4.2.3 Conformance

This section identifies those contracts and profiles that will be necessary for working interoperability.

620 Conceptual-level conformance statements will only occur in standards which are intended to constrain some feature of a real implementation, so testing is possible. Testing is performed at prescribed accessible interfaces, known as reference points. A conformance statement is a statement that identifies the expected observable events and the functional behavior which must be satisfied at these points.

The following contract specifications and conformance profiles constitute conceptual conformance statements.

Contracts

625 This section identifies those contracts and profiles that will be necessary for working interoperability. Contracts tie capabilities to the semantic content required to execute the behavior associated with those capabilities.

630 The tables below identify the specific healthcare requirements that are satisfied by the contract. The rows entitled Inputs and Outputs identify the specific Semantic Signifiers that are bound to the capability to make the contract normative.

Submit Audit Record

Capability Name	Submit Audit Record
Description	Accepts a request to receive an audit event record and process in accordance with implementation policy.
Inputs	Audit Message
Outputs	None
Healthcare-specific Requirements satisfied	[DICOM95-2010], [IHE-ITI-2A], [IHE-ITI-2B], [IHE-ITI-3], and ASTM E2147-01

Retrieve Disclosure Records

Capability Name	Retrieve Disclosure Records
Description	Accepts a request to receive information from Audit Event Records that directly indicate disclosure of personal information
Inputs	Disclosure Information Request
Outputs	Disclosure Information Response
Healthcare-specific Requirements satisfied	1, 2

635 Retrieve Audit Records

Capability Name	Retrieve Audit Records
Description	Accepts a request to receive information from Audit Event Records.
Inputs	Audit Record Request
Outputs	Audit Record Response
Healthcare-specific Requirements satisfied	1, 2

Open Issues

1. In the Retrieve Audit Records contract, we have only modeled the capability to return audit records that may provide insight into potential disclosures or partial disclosure information. Further modeling of the filter criteria may be necessary to effectively select any set of audit records.

640

Conformance Profiles

A Conformance Profile in the context of this document consists of a set of contracts which, taken together, provide complete, coherent behavior against which conformance can be claimed at both Platform Independent, and Platform Dependent levels of specificity. Conformance profiles at this level provide the foundation for working operability. These profiles may optionally include additional constraints where relevant.

645

Audit Recorder

This conformance profile includes the following contracts:

- Submit Audit Record

650 **Audit Reporter**

This conformance profile includes the following contracts:

- Request Audit Record
- Request Disclosure Record

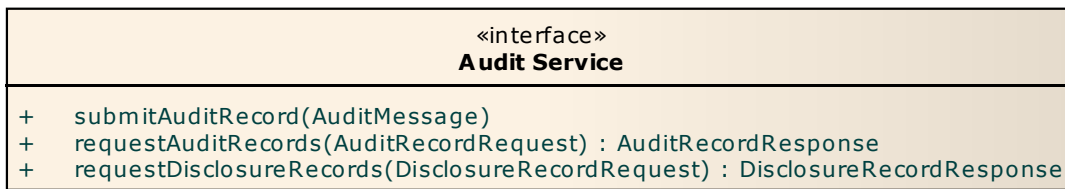
4.3 Platform Independent Model

655 **4.3.1 Operations**

This section describes the mechanisms used to fulfill the capabilities identified at the platform independent level. Each operation represents an entry to some defined behavior.

The UML diagram below illustrates the platform independent operations specified for the Audit Service

Figure 15 PIM - Audit Service Operations



660

4.3.2 submitAuditRecord

submitAuditRecord is an operation that receives an audit event message and records it based upon implementation policy. No application-level response is expected.

Operation	Parameter	Direction	Description
submitAuditRecord	AuditMessage	In	An audit event message as described in the PIM-Level section entitled AuditMessage on page 34.

Expected Behavior

- 665
- <CONF-3> The service shall receive both well-formed and malformed AuditMessages.
 - <CONF-4> The service shall have the capability to persist received messages.

Error Responses

- <CONF-5> There shall no application-level error responses provided by the operation.

4.3.3 requestDisclosureRecords

670 The requestDisclosureRecords operation provides a standard service interface to retrieve audit event records that may be used to support downstream creation of disclosure accounting reports for patient

consumption.

Operation	Parameter	Direction	Description
requestDisclosureRecords	DisclosureRecordRequest	In	As defined in Disclosure Record Request on page 31
	DisclosureRecordResponse	Out	As defined in Disclosure Record Response on page 32

Expected Behavior

- 675 <CONF-6> The operation shall successfully receive both well-formed and malformed DisclosureRecordRequests.
- <CONF-7> Any optional DisclosureRecordRequest attribute that is null, shall not be used as a selection criteria for that invocation.
- <CONF-8> The criteria for populating the DisclosureRecordResponse shall be as follows:

Select all records where:
 DisclosureRecordRequest.dateRange.lowValue >= EventIdentification.dateTime AND
 DisclosureRecordRequest.dateRange.highValue <= EventIdentification.dateTime AND
 (EventIdentification.purposeOfUse IN DisclosureRecordRequest.purposeOfUse) AND
 ((AuditSource.sourceId IN DisclosureRecordRequest.parties.id[]) OR
 (ActiveParticipant.id IN DisclosureRecordRequest.parties.id[]) OR
 (ParticipantObject.id IN DisclosureRecordRequest.parties.id[])) OR
 ((ActiveParticipant.roleIdCode IN DisclosureRecordRequest.parties.roleCode []) OR
 (ParticipantObject.typeCodeRole IN DisclosureRecordRequest.parties.roleCode []))

680

Error Responses

- <CONF-9> The operation shall support the following application error responses:

Error Response	Description
Malformed Request	The operation request was not formed correctly.

4.3.4 requestAuditRecords

- 685 The requestAuditRecords operation provides a standard service interface to retrieve audit event records that may be used to support downstream creation of disclosure accounting reports for patient consumption.

Operation	Parameter	Direction	Description
requestAuditRecords	AuditRecordRequest	In	As defined in Audit Record Request on page 31
	AuditRecordResponse	Out	As defined in Audit Record Response on page 33

Expected Behavior

- 690 <CONF-10> The operation shall successfully receive both well-formed and malformed AuditRecordRequests.
- <CONF-11> Any optional AuditRecordRequest attribute that is null, shall not be used as a selection criteria for that invocation.
- <CONF-12> The criteria for output record selection shall be applied as follows:

Select all records where:
 AuditRecordRequest.dateRange.lowValue >= EventIdentification.dateTime AND
 AuditRecordRequest.dateRange.highValue <= EventIdentification.dateTime AND
 (EventIdentification.eventId IN AuditRecordRequest.eventId) AND
 (ANY EventIdentification.eventTypeCode IN AuditRecordRequest.eventTypeCode) AND
 (EventIdentification.purposeOfUse IN AuditRecordRequest.purposeOfUse) AND
 ((AuditSource.sourceId IN AuditRecordRequest.parties.id[]) OR
 (ActiveParticipant.id IN AuditRecordRequest.parties.id[]) OR
 (ParticipantObject.id IN AuditRecordRequest.parties.id[])) OR
 ((ActiveParticipant.roleIdCode IN AuditRecordRequest.parties.roleCode []) OR
 (ParticipantObject.typeCodeRole IN AuditRecordRequest.parties.roleCode []))

695

Error Responses

- <CONF-13> The operation shall support the following application error responses:

Error Response	Description
Malformed Request	The operation request was not formed correctly.

4.4 Platform Specific Model

700 4.4.1 Audit Recorder Profile

- <CONF-14> An Audit Service claiming behavioral conformance to this profile shall demonstrate conformance with the IHE ITI-20 Transaction specification [IHE-ITI-2A] using the Audit Recorder Profile - Audit Message as defined on page 53.

4.4.2 Audit Reporter Profile

705 Two operations are defined that make up this profile. Figure 16, below contains the W3C Web Services Definition Language (WSDL) definition of the two query operations described in Figure 15 PIM - Audit Service Operations.

Note: The WSDL definition in Figure 16 contains URL's that will need to be changed for each implementation, based on machine identification and security requirements (see Engineering Viewpoint, Platform Specific Level).

710

Figure 16 HL7 Audit Reporter Profile WSDL

```
<?xml version="1.0" encoding="utf-8"?>
<definitions name="V3PASS_Audit"
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
  xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  xmlns:wsa="http://www.w3.org/2005/08/addressing"
  targetNamespace="urn:h17-org:v3"
  xmlns:h17="urn:h17-org:v3">

  <documentation>
    HL7 PASS - Audit and Disclosure record retrieval service
  </documentation>
  <types>
    <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns="urn:h17-org:v3"
      targetNamespace="urn:h17-org:v3">

      <xs:include schemaLocation="../xsd/retrieveAuditRecord.xsd"/>
      <xs:include schemaLocation="../xsd/retrieveDisclosureRecord.xsd"/>

      <xs:element name="malformedRequest" type="xsd:string" default="A malformed
request was received"/>
    </xs:schema>
  </types>
  <message name="retrieveAuditRecord.Request_Message">
    <part name="Body" element="h17:RetrieveAuditRecords.request"/>
  </message>
  <message name="retrieveAuditRecord.Response_Message">
    <part name="Body" element="h17:RetrieveAuditRecords.response" />
  </message>
  <message name="retrieveDisclosureRecord.Request_Message">
    <part name="Body" element="h17:RetrieveDisclosureRecords.request" />
  </message>
  <message name="retrieveDisclosureRecord.Response_Message">
    <part name="Body" element="h17:RetrieveDisclosureRecords.response" />
  </message>
  <message name="V3PASS_Audit_malformedRequestFault">
    <part name="Body" element="h17:malformedRequest"/>
  </message>
  <portType name="V3PASS_Audit_PortType">
    <operation name="V3PASS_Audit_retrieveAuditRecords">
      <input message="h17:retrieveAuditRecord.Request_Message" wsa:Action="urn:h17-
org:v3:V3PASS_Audit_01010010"/>
      <output message="h17:retrieveAuditRecord.Response_Message" wsa:Action="urn:h17-
org:v3:V3PASS_Audit_01010015"/>
      <fault name="malformedRequest"
message="h17:V3PASS_Audit_malformedRequestFault"/>
    </operation>
    <operation name="V3PASS_Audit_retrieveDisclosureRecords">
```

```

    <input message="h17:retrieveDisclosureRecord.Request_Message"
wsa:Action="urn:h17-org:v3:V3PASS_Audit_01010020" />
    <output message="h17:retrieveDisclosureRecord.Response_Message"
wsa:Action="urn:h17-org:v3:V3PASS_Audit_01010025" />
    <fault name="malformedRequest"
message="h17:V3PASS_Audit_malformedRequestFault" />
  </operation>
</portType>
<binding name="V3PASS_Audit_Binding" type="h17:V3PASS_Audit_PortType">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <operation name="V3PASS_Audit_retrieveDisclosureRecords">
    <soap:operation
soapAction="http://service/audit/RetrieveDisclosureRecords"/>
    <input>
      <soap:body use="literal"/>
    </input>
    <output>
      <soap:body use="literal"/>
    </output>
  </operation>
  <operation name="V3PASS_Audit_retrieveAuditRecords">
    <soap:operation
soapAction="http://service/audit/RetrieveAuditRecords"/>
    <input>
      <soap:body use="literal"/>
    </input>
    <output>
      <soap:body use="literal"/>
    </output>
  </operation>
</binding>
<binding name="V3PASS_Audit_Binding_Soap12" type="h17:V3PASS_Audit_PortType">
  <soap12:binding style="document"
transport="http://schemas.xmlsoap.org/soap/http"/>
  <operation name="V3PASS_Audit_retrieveDisclosureRecords">
    <soap12:operation soapAction="urn:h17-
org:v3:V3PASS_Audit_retrieveDisclosureRecords" soapActionRequired="true"/>
    <input>
      <soap12:body use="literal"/>
    </input>
    <output>
      <soap12:body use="literal"/>
    </output>
  </operation>
  <operation name="V3PASS_Audit_retrieveAuditRecords">
    <soap12:operation soapAction="urn:h17-
org:v3:V3PASS_Audit_retrieveAuditRecords"/>
    <input>
      <soap12:body use="literal"/>
    </input>
    <output>
      <soap12:body use="literal"/>
    </output>
  </operation>
</binding>
<service name="V3PASS_Audit_Service">
  <port name="V3PASS_Audit_Port" binding="h17:V3PASS_Audit_Binding">
    <soap:address location="http://service/location/V3PASS_Audit" />
  </port>
  <port name="V3PASS_Audit_PortSoap12" binding="h17:V3PASS_Audit_Binding_Soap12">
    <soap12:address location="http://service/location/V3PASS_Audit"/>
  </port>
</service>
</definitions>

```

5 Engineering Viewpoint

This section identifies the infrastructure that is required to support functional distribution of an ODP system¹⁹.

715 5.1 *Conceptual Level*

5.1.1 ODP Functions

The ODP Functions are specified by the Reference Model and are intended to provide broad categories of functions to be considered. At the conceptual level, the majority of these functions would not necessarily be filled.

720 *Physical Distribution Functions*

N/A

Communication Functions

N/A

Processing Functions

725 N/A

Storage Functions

N/A

Security Functions

N/A

730 5.1.2 Engineering Roles

None identified.

5.2 *Platform Independent Level*

5.2.1 ODP Functions

Physical Distribution Functions

735 N/A

¹⁹ ISO/IEC 10746-3 Open Distributed Processing – Reference Model Architecture

Communication Functions

Submit Audit Record - IHE-ATNA Profile

- There shall be a means of acknowledging receipt of messages that can be available should an implementation require it.

740 **Processing Functions**

N/A

Storage Functions

N/A

Security Functions

745 N/A

5.2.2 Engineering Roles

None identified.

5.3 Platform Specific Level

5.3.1 ODP Functions

750 **Physical Distribution Functions**

N/A

Communication Functions

Audit Recorder – Syslog Profile

755 The Submit Audit Record operation is mapped to the IHE-ITI-20 Record Audit Event transaction. There is no expectation that the Submit Audit Record operation will actually record the event. The behavior is expected to be implementation policy dependent.

760 Both the IHE-ITI-20 transaction [IHE-ITI-2A] and DICOM Supplement 95 [DICOM95] specify the use of either of two transport mechanisms for the communication of audit event messages from Audit Event Sources to an Audit Service. They are Syslog-UDP (IETF RFC 5426), and Syslog-TLS (IETF RFC 5425). Further references are made to WS-I Basic Security Profile v1.1, however only insofar as it's conformance to the TLS requirements.

<CONF-16> Implementations of the Submit Audit Record capability that claim conformance to the Submit Audit Record profile, shall be fully conformant with the IHE-ITI-20 transaction transport specification as described in [IHE-ITI-2A].

765 **Audit Reporter – SOAP Profile**

The retrieveDisclosureRecords and retrieveAuditRecords operations have identical requirements from an

engineering perspective.

770 <CONF-17> Implementations of the Retrieve Disclosure Records capability that wish to claim conformance to the Web Services Profile, shall be conformant to the HL7 Version 3 Standard: Transport Specification - Web Services Profile, Release 2 [HL7-WSS-R2].

<CONF-18> Implementations of the Retrieve Audit Records capability that wish to claim conformance to the Web Services Profile, shall be conformant to the HL7 Version 3 Standard: Transport Specification - Web Services Profile, Release 2 [HL7-WSS-R2].

775 <CONF-19> Query operations shall use a “Request-Response” message exchange pattern, as described in [HL7-WSS-R2].

<CONF-20> Implementations of the Audit Reporter Profile shall support both HTTP/SOAP and HTTPS/SOAP transport bindings.

<CONF-21> Implementations of the Audit Reporter Profile shall only one of HTTP/SOAP or HTTPS/SOAP transport bindings to be active.

780 Whether an implementation requires HTTP or HTTPS will be dependent on the evaluation of security risks for each implementation and is solely at the discretion of the implementation.

Processing Functions

N/A

Storage Functions

785 N/A

Security Considerations

This section details both the security control measures that this specification directly supports as well as identified risks where no mitigation is available via the specification.

790 The following two tables identify those security control measures that are supported by this specification and are recommended as mitigation of the risks identified. It must be pointed out that regardless of the mitigations recommended herein, each implementation is strongly encouraged to perform an independent risk assessment to identify risks and develop mitigation strategies that are appropriate for that implementation.

Audit Recorder – Syslog Profile

795 *Table 36 Security Control Measures – Audit Recorder – Syslog Profile*

Measure	Targeted Risk(s)
Syslog-TLS (Server authentication)	<ul style="list-style-type: none">- Server masquerade- Audit clients unaware of service unavailability
Syslog-TLS (Mutual authentication)	<ul style="list-style-type: none">- As above- Non-repudiation of audit source- Masquerading audit source

Audit Reporter – SOAP Profile

Table 37 Security Control Measures – Audit Reporter – SOAP Profile

Measure	Targeted Risk(s)
HTTPS (Server authentication)	<ul style="list-style-type: none">- Eavesdropping- Server masquerade
HTTPS (Mutual authentication)	<ul style="list-style-type: none">- As above- Non-repudiation of query client- Masquerading query client

Implementation Security Considerations

800 While there will continue to be disclosures that can only be identified by combining multiple audit events with external information sources, the capability to create a single disclosure record as described in the Idealized Disclosure Record section of this document, on page 37, has the potential to reduce the occurrences of reporting errors as a result of correlation issues.

805 Implementers of this specification should take into consideration that all audit sources may not submit compliant audit records, and are encouraged to ensure that the implementation can accept different schema versions, as well as formatting errors as gracefully, losing as little information as possible. Approaching an implementation in this manner reduces the risk of reduced service availability in addition to providing a more complete audit trail.

810 In order to reduce the risk of unauthorized disclosure of Personal Information (PI), the contents of submitted audit records should be reviewed to ensure that the absolute minimum amount of PI is contained within the audit record itself. Identifiers should be used rather than descriptive names, and the identifiers themselves could be made opaque using a number of techniques.

815 It is assumed that appropriate access controls are in place to ensure that only authorized entities can invoke the services specified herein. To enhance accountability around the use of audit information, two audit records should be added to the audit trail whenever either of the operations of the Audit Reporter profile is invoked. One of the records should have an Audit Event ID conformant to the “Audit Log Used” event described in [DICOM95]. The second record should be conformant to the “Query” event described in [DICOM95].

Finally, implementers should ensure that all schema dereferencing is performed using a trusted schema source.

820 5.3.2 Engineering Roles

None identified.

825

Appendix A - Glossary of Terms

The following table identifies terms used in this document that are specific to the subject domain.

Term	Description
Access control	Access control is principally concerned with the three components of: privacy policies, security policies, and enforcement of the resulting merged set of policies that are used to determine if access to system resources and functions are to be authorized. Access control includes privacy rules as well as security rules [HITSP TP20]
Alarm	Notification that a condition has been reached
Alert	What is sent when the monitor service notices that a series of events matches a pattern
Analysis application	Application program with ability to analyze and report based on audit data
Archiving	Moving of records from active to inactive state
Audit event	Occurrence of a condition specified in the audit policy
Audit log	Place where audit records are collected
Audit message	Structured collection of audit data items
Audit record	Data structure used to record audit events
Audit Service Artifact	An object that helps determine the behavior and function of the Audit service
Audit trail	Place where audit records are collected
Audit trail synchronization	Adjusting audit trails from disparate sources to a common time standard
Behavior	Manner in which activity is exhibited
Break glass	Condition where access restrictions are knowingly avoided
Business context	Enterprise requirements
Business purpose	Enterprise requirements
Capability, functional	Capacity to exhibit a relevant behavior
Composable	Capable of being combined with other like components to form a new capability
Consent, patient	Authorization from a patient to access an object
Consistent time	Synchronized chronographic sequence
Constraint	A limitation on an access control rule
Dependency	Requirement to consult another entity
Directive, patient consent	An artifact embodying patient consent
Domain	Bounded environment
Emergency access	Access permitted by policy when an emergency condition exists

Term	Description
Environment	Surrounding space
Event	Occurrence of a condition
Event, auditable	Event that can be recorded in an audit log.
Event, security relevant	Event that is included in security policy
Filter	Select attributes based on specified criteria
Granularity	Level of detail
Interaction	Participation in joint activity
Interface	Point where interchange of data takes place
Interoperability	Ability to coordinate operations in a meaningful way
Maintenance	Administration to ensure acceptable operation
Management interface	Point where interchange of data takes place for purposes of system management
Management services	Functions needed to conduct establishment, review, and maintenance
Object	Any system resource subject to access control, such as a file, printer, terminal, database record
Permission	An operation on an object [INCITS 359-2004]
Policy	Rules to govern operations and behavior
Profile	A named set of cohesive capabilities
Profile, conformance	Profile that specifies compliance with a specification
Profile, functional	Named list of a subset of the operations defined within this specification which must be supported in order to claim conformance to the profile.
Provisioning	Supplying of items to a membership class
Purpose of use	Stated intent for access to privacy data
Reduction	Ability to reduce incoming audit records based on the content of the audit record, i.e., dump unneeded records
Reliable time	Dependable time source
Repository, audit	Organized collection of audit logs
Role	Named set of permissions controlling accesses
Schema	Format specification with meaningful components
Service consumer	A component that uses a service
Service provider	A component that provides a service
Targeted	Selected for communication
Vocabulary	Language terms pertaining to a domain of discourse

830 **Appendix B – Reference Documents**

The following works are referenced and provide foundational components for this work:

Normative

- ISO/IEC 10181-7/ITU-T Rec. X.816(1995 E) – Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Security Audit and Alarms Framework
- 835 ▪ IHE Audit Trails and Node Authentication
 - [IHE-ITI-1] - IHE IT Infrastructure Technical Framework, Volume 1, Revision 6.0
 - [IHE-ITI-2A] - IHE IT Infrastructure Technical Framework, Volume 2a, Revision 6.0
 - [IHE-ITI-2B] - IHE IT Infrastructure Technical Framework, Volume 2a, Revision 6.0
 - [IHE-ITI-3] - IHE IT Infrastructure Technical Framework, Volume 2a, Revision 6.0
- 840 ▪ [DICOM95] - Digital Imaging and Communications in Medicine (DICOM) Supplement 95: Audit Trail Messages – Letter Ballot – 26 March 2010
- HL7 Security and Privacy Domain Analysis Model – Draft Standard for Trial Use – May 2010
- Internet Engineering Task Force (IETF) RFC 5424 – March 2009 - The Syslog Protocol
- 845 ▪ Internet Engineering Task Force (IETF) RFC 5425 – March 2009 - Transport Layer Security (TLS) Transport Mapping for Syslog
- Internet Engineering Task Force (IETF) RFC 5426 – March 2009 - Transmission of Syslog Messages over UDP
- E2147-01 Standard Specification for Audit and Disclosure Logs in Use in Health Information Systems, ASTM International, June 2002.

850

Informative

- Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications (IETF RFC 3881).
- ISO CD 27789 - Health informatics — Audit trails for electronic health records – 2008-06-26
- 855 ▪ ISO DTS 14265 - Health Informatics — Classification of purposes for processing personal health information
- The Open Group – Distributed Audit Service (XDAS), Preliminary Specification, January 1998
- International Security, Trust & Privacy Alliance (ISTPA) – Privacy Management Reference Model, Version 2.0
- 860 ▪ Health Level Seven™, Inc. - HL7 V3 TRANS WS R2
HL7 Version 3 Standard: Transport Specification - Web Services Profile, Release 2
January 2010 (Withdrawn Ballot)