V3_PSAF_R1_N3_2019SEP

HL7 Version 3 Standard:
Privacy and Security Architecture Framework
Release 1
Volume 4: Audit Conceptual Model
September 2019

HL7 Normative Ballot

Sponsored by:
Security Work Group

Community Based Care and Privacy Work Group

IMPORTANT NOTES:

HL7 licenses its standards and select IP free of charge. **If you did not acquire a free license from HL7 for this document,** you are not authorized to access or make any use of it. To obtain a free license, please visit:

http://www.HL7.org/implement/standards/index.cfm.

If you are the individual that obtained the license for this HL7 Standard, specification or other freely licensed work (in each and every instance "Specified Material"), the following describes the permitted uses of the Material.

A. HL7 INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS, who register and agree to the terms of HL7's license, are authorized, without additional charge, to read, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part without paying license fees to HL7.

INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS wishing to incorporate additional items of Special Material in whole or part, into products and services, or to enjoy additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS as noted below, must become ORGANIZATIONAL MEMBERS of HL7.

B. HL7 ORGANIZATION MEMBERS, who register and agree to the terms of HL7's License, are authorized, without additional charge, on a perpetual (except as provided for in the full license terms governing the Material), non-exclusive and worldwide basis, the right to (a) download, copy (for internal purposes only) and share this Material with your employees and consultants for study purposes, and (b) **utilize** the Material for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, Compliant Products, in all cases subject to the conditions set forth in this Agreement and any relevant patent and other intellectual property rights of third parties (which may include members of HL7). No other license, sublicense, or other rights of any kind are granted under this Agreement.

C. NON-MEMBERS, who register and agree to the terms of HL7's IP policy for Specified Material, are authorized, without additional charge, to read and use the Specified Material for evaluating whether to implement, or in implementing, the Specified Material, and to use **Specified** Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part.

NON-MEMBERS wishing to incorporate additional items of Specified Material in whole or part, into products and services, or to enjoy the additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS, as noted above, must become ORGANIZATIONAL MEMBERS of HL7.

Please see http://www.HL7.org/legal/ippolicy.cfm for the full license terms governing the Material.

Ownership. Licensee agrees and acknowledges that HL7 owns all right, title, and interest, in and to the Materials. Licensee shall take no action contrary to, or inconsistent with, the foregoing.

Licensee agrees and acknowledges that HL7 may not own all right, title, and interest, in and to the Materials and that the Materials may contain and/or reference intellectual property owned by third parties ("Third Party IP"). Acceptance of these License Terms does not grant Licensee any rights with respect to Third Party IP. Licensee alone is responsible for identifying and obtaining any necessary licenses or authorizations to utilize Third Party IP in connection with the Materials or otherwise. Any actions, claims or suits brought by a third party resulting from a breach of any Third-Party IP right by the Licensee remains the Licensee's liability.

Following is a non-exhaustive list of third-party terminologies that may require a separate license:

Terminology	Owner/Contact
Current Procedures Terminology (CPT) code set	American Medical Association https://www.ama-assn.org/practice-management/cpt-licensing
SNOMED CT	SNOMED International http://www.snomed.org/snomed-ct/get-snomed-ct or info@ihtsdo.org
Logical Observation Identifiers Names & Codes (LOINC)	Regenstrief Institute
International Classification of Diseases (ICD) codes	World Health Organization (WHO)
NUCC Health Care Provider Taxonomy code set	American Medical Association. Please see www.nucc.org. AMA licensing contact: 312-464-5022 (AMA IP services)

Important Note to September 2019 Ballot Voters

The September 2019 Privacy and Security Framework (PSAF) ballot is a package containing all of the Volumes developed to date under the PSAF Project Scope Statement 914. See the September Ballot Announcement:

https://confluence.hl7.org/display/HL7/2019SEP+Announcement+of+Formation+of+Consensus+Groups

The Privacy and Security Architecture Framework (PSAF) is comprised of:

- Volumes 1 and 2, and the Informative Guidance document for Trust Framework for Federated Authorization conceptual and behavioral models (TF4FA), which passed normative ballot in May 2018. Being normative, it is not in scope for September 2019 ballot comments.
- Volume 3 Provenance, a conceptual model addressing topics needed for trustworthy information exchange, passed normative ballot in January 2019. It has been significantly restructured as a Domain Analysis Model (DAM) for the September 2019 ballot based on input from commenters and stakeholders. Volume 3 Provenance is in scope for September 2019 ballot comments.
- Volume 4 Audit, a conceptual model for the audit service interfaces. This document was approved as normative in January 2017 under the title HL7 Version 3 Standard: Privacy, Access and Security Services (PASS) - Healthcare Audit Services Conceptual Model, Release 1 (PI ID: 1264). However, the Security Work Group missed the publication deadline, so this volume was re-balloted and past normative during the May 2019 cycle. Being normative, it is not in scope for September 2019 ballot comments.
- The Security Work Group decided to combine all volumes into one ballot package to keep them moving in tandem through balloting, publication and potential reaffirmation.

As stated, only Volume 3 Provenance, is in scope for comments for September.

Inclusion of Volumes 1, 2, and the TF4FA Guide, and Volume 4 in the September PSAF ballot package also affords voters an opportunity to review the wider privacy and security context in which the Provenance DAM was developed, and to which it contributes a significant component.

Editor	Diana Proud-Madruga (VHA) | diana.proud-madruga@va.gov
Authors	John "Mike" Davis (Veterans Health Administration) | Mike.Davis@va.gov
	Diana Proud-Madruga (Veterans Health Administration) | diana.proud-madruga@va.gov
	David Pyke | david.pyke@readycomputing.com

Other contributors
Bill Braithwaite (Anakam) | bbraithwaite@anakam.com
Laura Bright (Nexj) | laura.bright@nexj.com
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
Mark Underwood | mark.underwood@kryptonbrothers.com

PREFACE

This document is part of a series of interrelated privacy and security architecture framework documents that address core security, policy, and traceability topics needed to enable trustworthy interoperability for information exchange. The series of documents are:

- *Volume 1, Trust Framework for Federated Authorization (TF4FA), Conceptual Model*: presents a general architecture for creating a trusted relationship with a healthcare partner supporting policy derivation for security and privacy. This document provides a general conceptual overview of what defines interoperable authorized exchange and what is needed to achieve it.
- *Volume2, Trust Framework for Federated Authorization (TF4FA), Behavioral Model*: presents a more technical behavioral model describing logical interaction among Federated Authorization components.
- *TF4FA Guide*: presents an informative supplement that amplifies information contained in Volumes 1 and 2.
- *Volume 3, Provenance*: presents a general conceptual overview of what defines resource lifecycle events and associated provenance events, and what is needed to process and leverage that provenance data for resource trustworthiness decisions (i.e., "fitness for use" decisions by resource recipients).
- *Volume 4, Audit Conceptual Model:* presents a general conceptual overview of security audit and audit services in a healthcare environment.

Figure 1 illustrates the document series larger context of establishing trustworthy interoperability for information exchange.

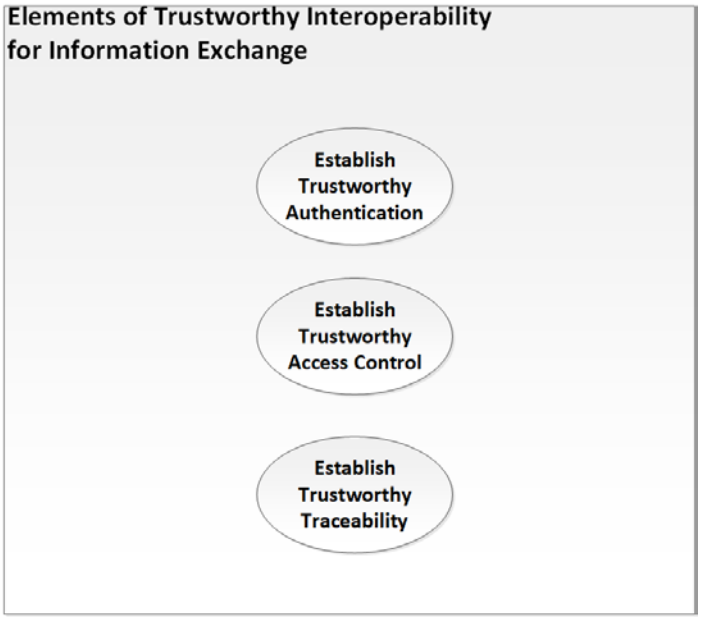

Figure 1: Elements of Trustworthy Interoperability

Table of Contents

List of Figures

List of Tables

List of Appendices

1 INTRODUCTION

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

"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 the privacy of subjects of care 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. Health records should be created, processed and managed in ways that guarantee the integrity and confidentiality of their contents and that support legitimate control by subjects of care in how the records are created, used and maintained.

Trust in electronic health records requires physical and technical security elements along with data integrity elements. Among the most important of all security requirements to protect personal health information and the integrity of records are those relating to audit and logging. These help to ensure accountability for subjects of care who entrust their information to electronic health record (EHR) systems. They also help to protect record integrity, as they provide a strong incentive to users of such systems to conform to organizational policies on the use of these systems."[1]

This document defines the requirements that are necessary to make up a Healthcare Audit Control Service. 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.

Technical mechanisms for providing healthcare audit record collection are and have been addressed by other standards bodies and serve to guide this specification. Accordingly, key elements of ISO TS 12052 (DICOM Part 15 Section A.5),[2] ISO 27789, IHE ATNA, The Open Group's Distributed Audit System (XDAS) preliminary specification, ASTM E2147, and work from the International Security, Trust, and Privacy Alliance have all been incorporated into this specification.[3]

1.1 Definition

"The Audit Service handles the recording and maintenance of auditable 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:

- The principle of accountability – that is holding users of a system accountable for their actions within the system, and

[1] ISO 27789 Health Informatics – Audit trails for electronic health records
[2] http://dicom.nema.org/medical/dicom/current/output/html/part15.html#sect_A.5.
[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

- 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.

1.2 Scope

This document includes 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.

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.

Development of this specification is planned as a series of incremental releases, each building upon the previous, with each release balloted sequentially (in turn) and independently. Accordingly, the following items are included in the scope of this version (Release 1):

- Semantics and behavior required to support audit record collection,
- Semantics and behavior required to support downstream processing of audit event information, including support for privacy accounting (i.e., accounting for collection, access, use, or disclosure of Personal Health Information (PHI)),
- Healthcare-specific requirements to support security Incident management, and
- Surveillance and/or monitoring services.

Out of scope for this specification in this release are:

- The capture and persistence of an audit trail of changes to clinical information, and
- Information and functional support for forensic auditing.
- HL7 FHIR specific references. A FHIR platform specific section may be added in future releases.

2 BUSINESS VIEWPOINT (CONCEPTUAL)

2.1 Overview

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

2.2 Business Model

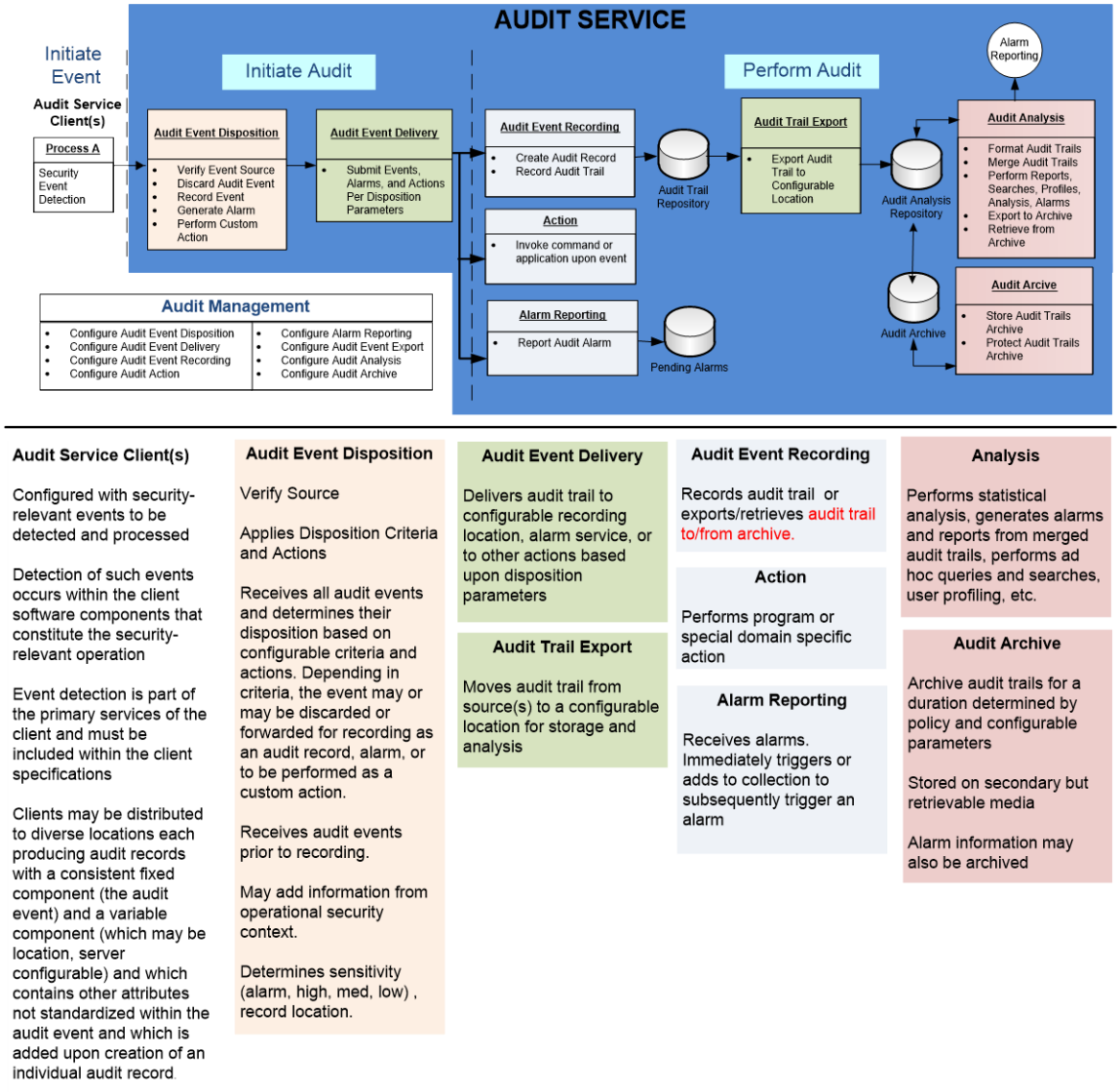

Figure 2: Audit Service Capabilities[5]

[5] This model is derived from ISO/IEC 10181-7 and work done by The Open Group on security audit. The ISO/IEC 10181-7 model calls out audit trail monitoring (Audit Analyzer) and audit trail analysis (Audit Provider and Audit Trail Examiner) capabilities separately. Those capabilities are all part of the Analysis Service in this simplified conceptual model, with no mandates on how they should be implemented. Likewise, the ISO/IEC 10181-7 model shows all alarms going through one Alarm Processor. Our model allows for alarms to be processed at two points: right after audit event disposition and delivery, and during analysis. Again, how this is implemented, as well as the

Figure 2: provides a high-level view of the overall security audit and alarm capabilities of an Audit Service. These capabilities are described in greater detail in the *Audit Service Functional Framework* section.

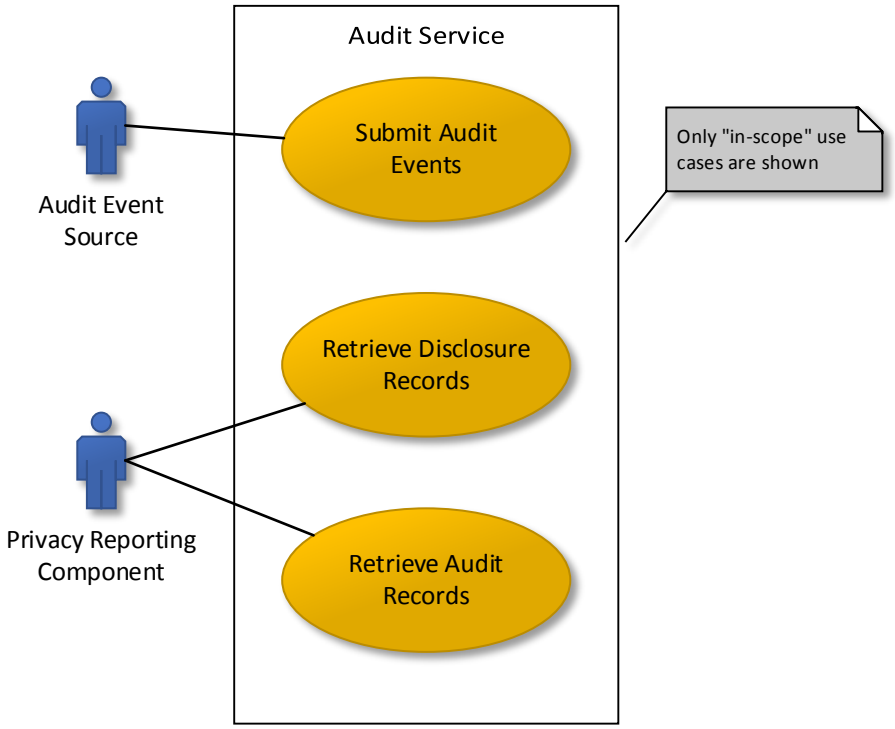

Figure 3: Audit Service Boundary Diagram

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:

- Submit Audit Events – a capability to accept audit events from one or more Audit Event Sources (including the Audit Service itself),
- 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. The audit function in Figure 2: Audit Service Capabilities that would be responsible for this capability would be found in the Audit Analysis Service, and
- 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. The audit function in Figure 2: that would be responsible for this capability would be found in the Audit Analysis Service.

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 part

---

destination and result of the alarm(s), is left open to the implementers.

dealing with scenarios which expose disclosure requirements; the second part dealing with scenarios which expose behavioral requirements.

Note: 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 Scenario 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.
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.

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 record an audit event.

2.3.2.1 DS 1 – Disclosure by Faxed Referral

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 (Doctors Inc.).

2.3.2.2 DS 2 – Disclosure to Patient (Download from EHR)

Adam Everyman arrives at Dr. Heart's clinic and is given a battery of tests. Dr. Heart evaluates the results of Adam's tests in combination with Heart's 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.

2.3.2.3 DS 3 – Disclosure to PCP (Upload into EHR)

Eve Everywoman visits Dr. Primary and delivers a CD of test results to Nurse Nightingale, who loads the information into Doctors, Inc. EHR system.

2.3.2.4 DS 4 – Electronic Disclosure Between Organizations

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.

2.3.2.5 DS 6 – Disclosure via Patient Portal

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.

2.3.2.6 DS 7 – Disclosure by Couriered Referral

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.

2.3.2.7 DS 8 – Disclosure via Consultation

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 in-person with Dr. Heart.

2.3.2.8 DS 9 – Disclosure via Inheritance

Dr. Eric Younger purchases the clinical practice of retiring Dr. Oldman. This is a bulk version of Disclosure via Consultation.

2.3.2.9 DS 10 – Inter-device Electronic Disclosure

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.

2.3.2.10 DS 11 – Emergency Third-Party Disclosure

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 Ace Ambulance, a local ambulance company, providing them with the information obtained from Eve.

2.3.2.11 DS 12 – Emergency Disclosure

Ernest Emt is dispatched from Ace Ambulance. He picks up Eve and transports her to GHH, 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 in route to Nurse Nightingale.

2.3.2.12 DS 13 – Secondary Disclosure of Familial Medical History

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.

2.3.2.13 DS 14 – Public Health Disclosure

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 cases. They are not exhaustive.

2.3.3.1 BhS 1 - 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.

2.3.3.2 BhS 2 - A request for privacy accounting information occurs

Eve requests from GHH an accounting of disclosures.

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

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 Client:	Any appropriately authorized source of healthcare audit records. The Audit Event Source can be a component of the Audit Service itself. Audit clients may be distributed to diverse locations and are configured with security audit always on.
Reporting Component:	Any appropriately authorized requestor of information relating to the collection, access, use, and/or disclosure of personal information or personal health information.

2.4.2 Use Case AU-1: Submit Audit Events[6]

2.4.2.1 Description

Invoke a function to submit one or more audit events to the audit service.

2.4.2.2 Assumptions

- In order for an audit trail to effectively support one or more distributed Audit Clients, those Clients and all Audit Service components, must maintain consistent time from a

[6] An instance of the refinement of this use case into specifications at the Platform Specific level has been completed as DICOM Part 15, Section A.5 (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.

designated authoritative time service. The accuracy requirement of the coordinated timekeeping is a policy decision.

- Appropriate security controls are in place to ensure adequate protection of the audit event information both in transit and at rest.

2.4.2.3 Actors

Audit Client

2.4.2.4 Trigger Event

The use case is triggered when one or more audit events are ready to be transmitted.[7]

2.4.2.5 Pre-conditions

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

2.4.2.6 Post-conditions

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

2.4.3 Use Case AU-2: Retrieve Audit Records

2.4.3.1 Description

Provide a mechanism to extract information from the Audit Service to support use via pre-configured or ad hoc rules. Assumptions.

- The information in the audit trail is sufficient to meet the reporting requirements.
- Formatting and other processing of the data in order to create the report is outside the scope of this use case.

2.4.3.2 Actors

Reporting Component

2.4.3.3 Trigger Event

The use case is triggered by a request for audit information.

2.4.3.4 Pre-conditions

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

2.4.3.5 Post-conditions

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

[7] 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.

2.4.4 Use Case AU-3: Retrieve Disclosure Records[8]

2.4.4.1 Description

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

2.4.4.2 Assumptions

- 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.
- We expect that the data provided by this capability will be supplemented by mechanisms that will allow identities in the record to be resolved. There is no expectation that the audit log can or should be the sole source of information required for a complete patient-consumable accounting of disclosures.

2.4.4.3 Actors

Privacy Reporting Component

2.4.4.4 Trigger Event

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

2.4.4.5 Pre-conditions

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

2.4.4.6 Post-conditions

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

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.

Requirements for use case AU-1 have not been identified here, as those requirements have been identified and satisfied in other standards.[9] The focus of this work is on use cases AU-2 and AU-3, which deal with retrieving information to support healthcare audit and disclosure accounting processes.

Note 1: Where the requirements in Table 3 identify healthcare-specific functionality or semantic content, those requirements are reflected in the Conformance Section of this document.

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

[9] ISO TS 12052/DICOM Part 15 Section A.5, and IHE Record Audit Event Section of the IHE ATNA specifications.

Table 4: Healthcare Audit Requirements

ID	Requirement	Functional / Interop.	Healthcare Specific? Y/N
AU-R1	The Audit Service must be able to request and retrieve information obtained from audit event information that would support disclosure accounting. 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: • Date 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, and • Verification method of the requesting party's identification. Source: ASTM E 2147-01 (Reapproved 2013) Section 8	F	Y[10]
AU-R2	The Audit Service 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
AU-R3	The Audit Service must have the ability to establish mutually-authenticated communication channels.	I	N
AU-R4	The Audit Service must have the ability to validate that any request has been appropriately authorized, based upon implementation policy.	F	N
AU-R5	The Audit Service must have the ability to deny a request where validation of the authorization credentials associated with that request fail.	F	N
AU-R6	The Audit Service shall support the protection of audit event information in transit across networks as required by organizational policy.	I	N
AU-R7	Where the information elements described in Requirement AU-R1 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.	F	N

[10] 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
AU-R8	The Audit Service must be able to request and retrieve audit event information that supports healthcare security audit. Specifically, audit logs must contain the following minimum data elements: • Date and Time of Event • Patient Identification (PII) • User Identification • Access Device (when available) • Type of Action (additions, deletions, changes, queries, print, copy) • Identification of the Patient Data that is Accessed (PHI)* • Source of Access (optional unless the log is combined from multiple systems or can be indisputably inferred) • Reason for Access (Purpose of Use)* Source: ASTM E 2147-01 (Reapproved 2013) Section 7	F	Y[11]

2.6 Platform Independent Model Level

2.6.1 Audit Service Functional Framework

2.6.1.1 Audit Service Overview

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.0	***Audit Service***	Description: Security Audit Service consists of the detection, collection and recording of various security-related auditable events as security audit events, audit records and audit trails as well as the disposition and analysis of those events.	• ISO 10181-7 (ITU X.16) • Open Group: Security Audit • ASTM E2147

The Audit Service Functional Framework is a comprehensive listing of elements to be considered for a Healthcare Security Audit solution. These elements handle the detection, recording, maintenance, and reporting of healthcare auditable events.

Figure 4: Healthcare Audit Service Security and Privacy Functional Model (SPFM), shows a detailed functional model which provides a logical view that encapsulates related requirements into capabilities. It is not an implementation design. In fact, functional models are, by definition, implementation and technology agnostic. Instead, the functional model informs business requirements development.

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

The Audit SPFM is based on published standards and recommendations from organizations such as International Organization for Standardization (ISO), ASTM International, Health Level Seven (HL7), and The Open Group.

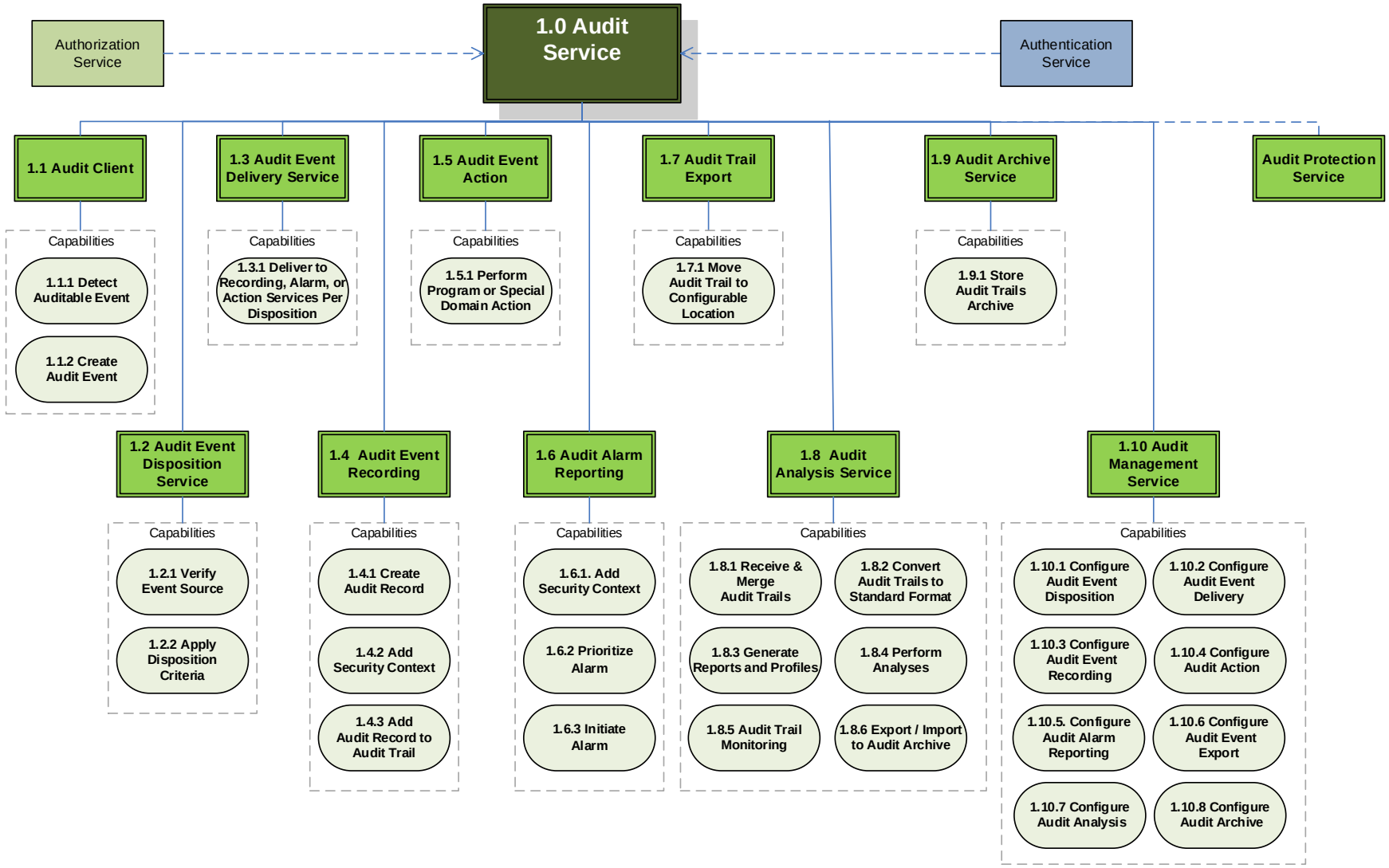

Figure 4: Healthcare Audit Service Security and Privacy Functional Model (SPFM)

2.6.1.2 Services Description and Purpose

The following sections describe each function within the Healthcare Audit Service SPFM. They also describe each function's set of capabilities. A capability is a specific feature of a function that can be reflected in a business requirements document (BRD) and subsequently implemented by a project team.

2.6.1.2.1 Audit Client

The audit client is the application or process software configured with security-relevant auditable events to be detected and processed. Event detection is part of the primary services of the client and must be included within the client specifications.

Audit clients may be distributed to diverse locations and are configured with security audit always on. Each audit client produces audit records where the audit event is a consistent fixed component and event attributes, such as location, are variable components configurable by the Audit Management Service located on the server side. The variable component is added upon creation of an individual audit record.

The Audit Client has two capabilities:

1. *"Detect Auditable Event" Capability* – This is a capability which detects security-relevant events. Security-relevant auditable events are established by policy and integrated into the client design so that the auditable events are intrinsic to the client programmatic workflow.
2. *"Create Audit Event" Capability* - Audit Events are generated at the occurrence of each instance of a security-relevant auditable event. This capability cannot be modified, turned off or disabled. When a security-relevant auditable event occurs, the client creates a corresponding "audit event". Creation of audit events must include the identity of the audit client and relative attributes of the client, such as client location. Additional information may need to be added to the client audit event to complete the generation of individual "audit records" which are then incorporated into an "audit trail" (see 2.6.1.2.4 Audit Recording).

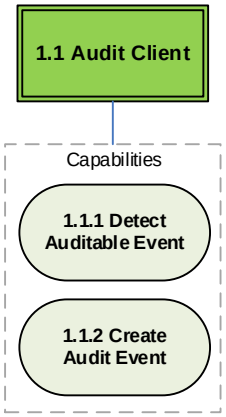

Figure 5: Audit Client

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.1	***Audit Client***	Description: The audit client is the application or process software configured to detect and process security-relevant auditable events. Event detection is part of the primary services of the client and must be included within the client specifications. Audit clients may be distributed to diverse locations each producing audit records where the audit event is a consistent fixed component and event attributes, such as location, are variable components configurable by the Audit Management Service located on the server side. The variable component is added upon creation of an individual audit record.	• ISO 10181-7 • Open Group: Security Audit

ID #	Requirement Title	Requirement Text	Guidance[12]	Source
1.1.1	Detect Auditable Events	Provide the capability to detect security-relevant auditable events.	The detection of security-relevant auditable events. Security-relevant auditable events are established by policy and integrated into the client design.	• ISO 10181-7 • Open Group: Security Audit
1.1.2	Create Audit Event	Provide the capability to create audit events.	An audit event is created upon detection of an auditable event. Information to be collected as part of the audit event is specified via audit configuration in the Audit Management Service. Creation of the audit event cannot be modified, turned off or disabled as this function is intrinsic to the client programmatic workflow. Creation of audit events must include the identity of the presenter of the audit event. Additional information may need to be added by the audit service to the client audit event to complete the generation of individual "audit records" which are then incorporated into an "audit trail."	• ISO 10181-7 • Open Group: Security Audit • ASTM E2147

2.6.1.2.2 Audit Event Disposition Service

The Audit Event Disposition Service determines if an audit event captured by the Audit

[12] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

Client is retained and passed on to other services through the Audit Delivery Service or ignored as a "no action." Dispositions and consequential actions for retained audit events are based on criteria determined by policy and configured in the Audit Management Service.

The Audit Event Disposition Service has two capabilities:

1. *"Verify Audit Event Source" Capability* - To prevent attacks (e.g., denial of service), the source of every audit event received is verified to ensure they are valid.
2. *"Apply Disposition Criteria" Capability* – Dispositions are applied to each received audit event, based on configurable criteria.
    - Principal requesting the operations
    - Sensitivity of the operations
    - Attributes of the information being processed
    - Context of the operation, for example, location and time of day (to detect unusual behavior or behavior that is inconsistent with the user profile).

Examples of consequential actions include:

- Ignore audit event (No action),
- Generate alarm,
- Record audit event, or
- Record audit event and generate alarm.

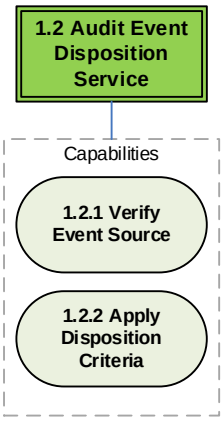

Figure 6: Audit Event Disposition Service

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.2	***Audit Event Disposition Service***	Description: The Audit Event Disposition Service determines if an audit event captured by the Audit Client is retained and passed on to other services through the Audit Delivery Service or ignored as "no action." Dispositions and consequential actions for retained audit events are based on criteria determined by policy and configured in the Audit Management Service.	• ISO 10181-7 • Open Group: Security Audit

ID #	Requirement Title	Requirement Text	Guidance[13]	Source
1.2.1	Verify Audit Event Source	Provide the capability to verify the source of the Audit Events.	This is an important security step to prevent attacks (e.g., denial of service). This capability ensures an authorized/trusted client is submitting the Audit Event. One approach to verification is the use of an appropriate authentication mechanism.	• Open Group: Security Audit • ISO/IEC 10181-7
1.2.2	Apply Disposition Criteria	Provide the capability to filter all submitted Audit Events to determine whether the Audit Events should be processed or ignored.	This is an audit event reduction capability. Determine the disposition of each submitted audit event and its associated information based on configurable criteria and actions. Depending on the criteria and filtering, the audit event may be ignored or forwarded for further processing. This filtering eliminates unneeded alarms, actions, logging, and analysis thereby improving efficiencies and performance. The configured criteria for dispositioning audit records is applied to each received audit event. Criteria may include: • Principal requesting the operations. • Sensitivity of the operations. • Attributes of the information being processed. • Context of the operation, for example, location and time of day (to detect unusual behavior). Examples of consequential actions	• Open Group: Security Audit • ISO/IEC 10181-7

[13] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

ID #	Requirement Title	Requirement Text	Guidance[13]	Source
			include: • Ignore Audit Event (No action), • Generate alarm, • Record audit event, or • Record audit event and generate alarm.	

2.6.1.2.3 Audit Event Delivery Service

This component delivers audit events as determined by the Disposition Service.

1. *"Deliver to Recording, Alarm, or Action Services Per Disposition" Capability* - Deliver audit events to a recording service, alarm service, and/or to the action service based upon disposition parameters

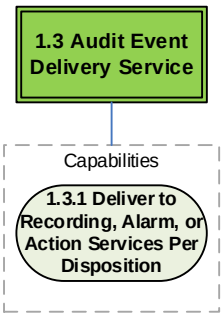

Figure 7: Audit Event Delivery Service

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.3	***Audit Event Delivery Service***	Description: Upon determination that an audit event requires an alarm, action, and/or recording, the Audit Delivery Service sends an alarm request, action request, and/or recording request to the applicable service as determined by the Disposition Service.	• ISO 10181-7 • Open Group: Security Audit • ASTM E2147

ID #	Requirement Title	Requirement Text	Guidance[14]	Source
1.3.1	Deliver to Recording, Alarm, or Action Services Per Disposition	Provide the capability to deliver an Audit Event to the Recording, Alarm, and/or Action service.	Deliver audit events to a configurable recording location, alarm service, or to other action services based upon disposition parameters. Delivery can be to any combination of the Recording, Alarm, and Action services.	• ISO/IEC 10181-7 • Open Group: Security Audit

2.6.1.2.4 Audit Recording

An audit event that requires recording must be appended to an audit trail in a manner such that it cannot be subsequently modified or deleted. For each audit event the identity of the initiating principal or performing principal or both together with other relevant information, such as date and time, are recorded.

1. "*Create Audit Record" Capability* - A standard audit record is created from the information provided in the audit event received.
2. *"Add Security Context" Capability* - Other information may be added to the audit record as directed by any audit and security policies in effect. This includes the operational security context of the audit event together with security domain management information that allows the record to be interpreted (for example, mappings of internal security attribute values to text strings). This may include the recording of cryptographic keys for encrypting audit record data. For efficiency, the security domain management information may be recorded periodically (for example, once per day) and the security management state applicable to any individual audit event regenerated by tracing all other changes to the information since the last record of the state.
3. *"Add Audit Record to Audit Trail" Capability* - The completed audit record is added to the appropriate audit trail at a configurable destination. This supports search, retrieval, and reporting capabilities.

[14] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

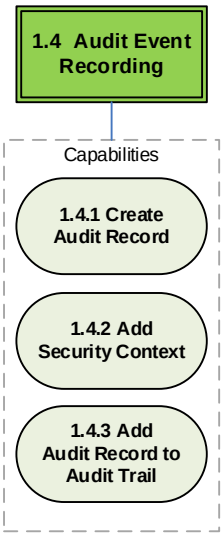

Figure 8: Audit Event Recording

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.4	***Audit Event Recording***	Description: An audit event that requires recording must be appended to an audit trail in a manner such that it cannot be subsequently modified or deleted. For each audit event the identity of the initiating principal or performing principal or both, together with other relevant information, such as date and time, are recorded.	• ISO 10181-7 • Open Group: Security Audit • ASTM E2147

ID #	Requirement Title	Requirement Text	Guidance[15]	Source
1.4.1	Create Audit Record	Provide the capability to create a complete audit record.	A standard audit record is created from the information provided in the audit event received.	• ISO/IEC 10181-7 • Open Group: Security Audit • ISO 27789 • ASTM E2147
1.4.2	Add Security Context	Provide the capability to add additional information to the audit record as necessary from operational security context.	Other information may be added to the audit record as directed by any audit and security policies in effect. This includes the operational security context of the audit event together with security domain management information that allows the record to be interpreted	• Open Group: Security Audit • ISO/IEC 10181-7

[15] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

ID #	Requirement Title	Requirement Text	Guidance[15]	Source
			(for example, mappings of internal security attribute values to text strings). This may include the recording of cryptographic keys for encrypting audit record data. For efficiency, the security domain management information may be recorded periodically (for example, once per day) and the security management state applicable to any individual audit event regenerated by tracing all other changes to the information since the last record of the state.	
1.4.3	Add Audit Record to Audit Trail	Provide the capability to store audit records in an audit trail.	Complete records of the type of access and all actions performed on the data should be maintained at a configurable location. This supports search, retrieval, and reporting capabilities. Logging should be executed in accordance with audit operational parameter configurations, security policies, and audit policies published by the Audit Management Service. An audit event that requires recording must be appended to an audit trail in a manner such that it cannot be subsequently modified or deleted. The identity of the initiating principal or performing principal or both, together with other relevant information, such as date and time, are recorded.	• ASTM E2147 • ISO/IEC 10181-7 • ISO 27001 • Open Group: Security Audit

2.6.1.2.5 Audit Event Action

An action (invoking commands or application upon trigger event) may need to be initiated to protect the system from further threat. For example, an action may be initiated to inhibit the operation that caused the (or is causing additional) audit events. Actions may be initiated in addition to alarms in order to expedite response to the detected audit events.

1. *"Perform Program or Special Domain Action" Capability* - The specified program or special domain-specific actions are performed. Examples of actions are invoking commands or applications in response to specific events. Actions should be executed in accordance with audit operational parameter configurations, security policies, and audit policies published by the Audit Management Service.

Audit data should support flags to distinguish levels of criticality, which specify when actions should be processed. For example:

- Actions requiring immediate priority processing.
- Actions that must be processed within 8 hrs.
- Actions that must be processed with 24 hours.
- Actions that must be processed greater than 24 hours.

Actions marked to be processed in the future could be added to a separate, dedicated Pending Alarms log. Logging should be executed in accordance with audit operational parameter configurations, security policies, and audit policies published by the Audit Management Service.

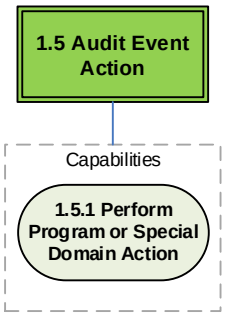

Figure 9: Audit Event Action

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.5	***Audit Event Action***	Description: An action (invoking commands or application upon trigger event) may need to be initiated to protect the system from further threat. For example, an action may be initiated to inhibit the operation that caused (or is causing additional) audit events. Actions may be initiated in addition to alarms in order to expedite response to the detected audit events.	• ISO 10181-7 • Open Group: Security Audit

ID #	Requirement Title	Requirement Text	Guidance[16]	Source
1.5.1	Perform Program or Special Domain Action	Provide the capability to take pre-defined actions on the occurrence of specific events.	The specified program or special domain-specific actions are performed. Examples of actions are invoking commands or applications in response to specific events. Actions should be executed in accordance with audit operational parameter configurations, security policies, and audit policies published	• Open Group: Security Audit • ISO/IEC 10181-7 • ASTM E2147

[16] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

ID #	Requirement Title	Requirement Text	Guidance[16]	Source
			by the Audit Management Service. Audit data should support flags to distinguish levels of criticality, which specify when action should be processed. For example: • Actions requiring immediate priority processing. • Actions that must be processed within 8 hrs. • Actions that must be processed with 24 hours. • Actions that must be processed greater than 24 hours. Actions marked to be processed in the future could be added to a separate, dedicated Pending Alarms log. Logging should be executed in accordance with audit operational parameter configurations, security policies, and audit policies published by the Audit Management Service.	

2.6.1.2.6 Audit Alarm Reporting

This component receives security alarm notifications generated by audit events in the Audit Disposition Service. Audit alarms must either be immediately initiated or be added to a collection of alarm notifications which subsequently trigger a response when a configured threshold is reached. The alarm reporting service may add information from the operational security context as it generates an alarm. When triggered, an alarm is sent to a pre-configured destination.

The triggering of an alarm may also initiate additional alarm-related actions to protect the system from further threat. For example: inhibiting the operation causing the generation of further audit events responsible for triggering the alarm.

This service has three capabilities:

1. *"Add Security Context" Capability* - Information from the operational security context may be added to the alarm content as directed by any audit and security policies in effect. Additional information is intended to assist those who receive and respond to the alarms.
2. *"Prioritize Alarm" Capability* - An event that is configured to generate an alarm must either immediately initiate an alarm or be added to a collection of similar events subsequently to trigger an alarm when a configured threshold is reached. The speed at which the alarm is raised is determined by the severity of the event. Ideally, the reporting of the alarm should give as much time as possible to those responsible for responding.

Prioritization is for all alarms regardless of whether the alarm is for immediate or future processing. Benefits of logging include audit and analysis of alarms over time.

Audit data should support flags to distinguish levels of criticality, which specify when alarms should be processed. For example:

- Alarms/alerts requiring immediate priority processing.
- Alarms/alerts requiring processing when a threshold is reached.

Alarms marked to be processed in the future could be added to a separate, dedicated Pending Alarms log.

Logging should be executed in accordance with audit operational parameter configurations, security policies, and audit policies published by the Audit Management Service.

3. *"Initiate Alarm" Capability* - The alarm is initiated and sent to a configurable destination. The triggering of an alarm may also initiate action to protect the system from further threat, for example, by inhibiting the operation causing the generation of the audit events triggering the alarm. An example could be the application of blocks on certain addresses or disabling of a principal identity or I/O device in the case of failed or duplicated authentication operations.

   The alarm should identify the cause of the alarm, the source of the detection of the security-related event, the appropriate end users, and of the perceived severity of the event, attack, or breach of security.

   Processing should be performed in accordance with audit operational parameter configurations, any audit policies published by the Audit Management Service, and security policies.

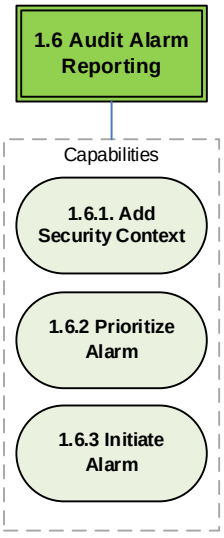

Figure 10: Audit Alarm Reporting

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.6	***Audit Alarm Reporting***	Description: This component receives security alarm notifications generated by audit events in the Audit Disposition Service. Audit alarms must either be immediately initiated or be added to a collection of alarm notifications which subsequently trigger a response when a configured threshold is reached. The alarm reporting service may add information from the operational security context as it generates an alarm. When triggered, an alarm is sent to a pre-configured destination. The triggering of an alarm may also initiate additional alarm-related actions to protect the system from further threat. For example: inhibiting the operation causing the generation of further audit events responsible for triggering the alarm.	• ISO 10181-7 • Open Group: Security Audit

ID #	Requirement Title	Requirement Text	Guidance[17]	Source
1.6.1	Add Security Context	Provide the capability to add additional information to the alarm as necessary from operational security context.	Information from the operational security context may be added to the alarm content as directed by any audit and security policies in effect. Additional information is intended assist those who receive and respond to the alarms.	• Open Group: Security Audit • ISO/IEC 10181-7
1.6.2	Prioritize Alarm	Provide the capability to prioritize initiation of alarms.	An event that is configured to generate an alarm must either immediately initiate an alarm or be added to a collection of similar events subsequently to trigger an alarm when a configured threshold is reached. The speed at which the alarm is raised is determined by the severity of the event. Ideally, the reporting of the alarm should give as much time as possible to those responsible for responding. Prioritization is for all alarms regardless of whether the alarm is for immediate or future processing. Benefits of logging include audit and analysis of alarms over time. Audit data should support flags to	• Open Group: Security Audit • ISO/IEC 10181-7 • ASTM E2147

[17] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

ID #	Requirement Title	Requirement Text	Guidance[17]	Source
			distinguish levels of criticality, which specify when alarms should be processed. For example: • Alarms/alerts requiring immediate priority processing. • Alarms/alerts requiring processing when a threshold is reached. Alarms marked to be processed in the future could be added to a separate, dedicated Pending Alarms log. Logging should be executed in accordance with audit operational parameter configurations, security policies, and audit policies published by the Audit Management Service.	
1.6.3	Initiate Alarm	Provide the capability to initiate additional actions and/or messages as necessary in response to the triggering of an alarm.	The alarm is initiated and sent to a configurable destination. The triggering of an alarm may also initiate action to protect the system from further threat, for example, by inhibiting the operation causing the generation of the audit events triggering the alarm. An example could be the application of blocks on certain addresses or disabling of a principal identity or I/O device in the case of failed or duplicated authentication operations. The alarm should identify the cause of the alarm, the source of the detection of the security-related event, the appropriate end users, and of the perceived severity of the event, attack, or breach of security. Processing should be performed in accordance with audit operational parameter configurations, any audit policies published by the Audit Management Service, and security policies.	• ISO/IEC 10181-7 • NIST SP 800-12 • ISO 10164-7 • Open Group: Security Audit

2.6.1.2.7 Audit Trail Export

The Audit Trail Export facilitates enterprise-wide analysis of audit information via a centralized analysis service. This service provides one capability:

1. *"Move Audit Trail to Configurable Location" Capability* - Move an audit trail to a configurable location.

   Securely export (transport) audit trails located throughout the enterprise to a (possibly centralized) audit analysis service based upon criticality criteria such as:

- Alarms and alerts
- Audit events that must be delivered within configurable time limits for analysis and processing
- Audit events that have routine criticality for analysis and processing

This capability is sometimes referred to as audit trail aggregation.

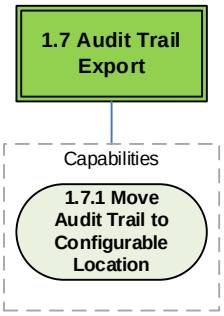

Figure 11: Audit Trail Export

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.7	***Audit Trail Export***	Description: Move an audit trail to a configurable location. Audit trail export facilitates enterprise-wide analysis of audit information since it can export audit trails throughout the enterprise to a centralized analysis service.	• ISO 10181-7 • Open Group: Security Audit

ID #	Requirement Title	Requirement Text	Guidance[18]	Source
1.7.1	Move Audit Trail To Configurable Location	Provide the capability to move an audit trail to a configurable location.	Securely export (transport) audit trails located throughout the enterprise to a (possibly centralized) audit analysis service based upon criticality criteria such as: • Alarms and alerts • Audit events that must be delivered within configurable time limits for analysis and processing • Audit events that have routine criticality for analysis and processing This capability is sometimes referred to as audit trail aggregation.	• Open Group: Security Audit • ISO/IEC 10181-7

[18] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

2.6.1.2.8 Audit Analysis Service

This component gathers, merges, formats, and processes audit trail information to facilitate analysis of security-relevant usage and operation. Analysis can help detect security issues that need attention. The user can initiate prepared and ad hoc queries and searches to generate useful reports and user profiles. Leveraging the reports and profiles, various types of analysis can be performed such as statistical or trend analysis. Analysis can be performed at any suitable level – from high-level (abstract) analysis to very detailed analysis. Security reports may indicate that an attempt has been made to breach the security of a system, in which case, security recovery actions may need to be undertaken. Analysis of the security audit trail can be used to assess the extent of an attack and to determine appropriate damage control procedures.

1. *"Receive and Merge Audit Trails"* Capability - Receives and merges audit trails from the audit trail and Archive for further analysis and reporting, possibly after identification of a potential security event months or even years later. Merging different audit trails provides the added benefit of being able to fully trace chains of events across the entire enterprise.
2. *"Convert Audit Trails to Standard Format"* Capability - Convert any local representation of an audit trail to a common interchange analysis format. This capability is essential to supporting centralized archiving and analysis of audit trails in a distributed heterogeneous environment. Required standard formats include XML, XLS, TXT, Comma Delimited (CSV), and DBF. Other formats may be implemented as necessary in addition to the required set.
3. *"Generate Reports and Profiles"* Capability - Produces formatted and ad hoc reports and searches, and profiles.

   Reporting should include using predetermined flags to generate audit summary reports by designated schedule.

   Profiles are based upon a record of historical user activities. This includes profiling user activities and access patterns. Such profiles can be used in searches and reporting. For example, searching for activities inconsistent with stored user profiles or identifying misuse.

   Query/Search is essential to report and profile generation. This is an audit event reduction capability. Query/Search should be efficient to operate and provide easy, on demand, menu-driven reporting within a reasonable time frame. Search/queries should provide logical controls, menu-driven sort capability based upon record content, logical operators (AND, OR, NEAR, NOT, etc.). This facilitates precise selection of the needed sub-set of audit records from the complete population of audit records.

   Searching should include the capability of an authorized requester to query the application to generate a report on an unscheduled basis. This feature is called for so that prompt response can be provided for incidents that are identified as a potential security breach. Managers should be able to specify queries that arise from patient, provider, or employee complaints, or a combination thereof.
4. *"Perform Analyses"* Capability - Perform various analysis using reports and profiles. Types of analysis include but are not limited to trending analysis and statistical analysis.

   The statistical analysis should be able to be performed on any set of information retrieved by Audit Provider. Use of a graphical presentation should be considered.

5. *"Audit Trail Monitoring"* Capability - Checks audit trails and, if appropriate, produces security alarms, actions, and security audit messages. The objective is to proactively identify and investigate specific events (e.g., failed access attempts) and unusual or suspicious patterns.

   Monitoring also includes searching audit trails for any new alarms or actions that need to be initiated (e.g., due to revised audit or security configurations), searching alarm logs for any alarms that have come due, and searching action logs for any actions that have come due.

   Monitoring and identification should be performed in accordance with audit operational parameter configurations and any audit policies published by the Audit Management Service.

6. *"Export/Import into Audit Archive"* Capability - Periodically export audit trail to Audit Archive Service based upon program parameters, policy and storage capabilities. Importing from the Audit Archive Service is done as needed to support audit analysis activities.

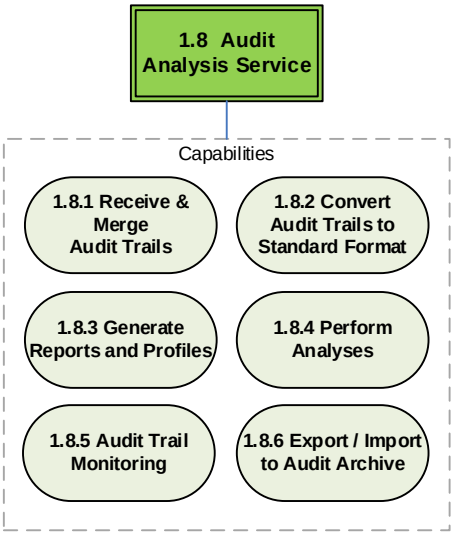

Figure 12: Audit Analysis Service

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.8	***Audit Analysis Service***	Description: Audit Analysis Service gathers, merges, formats, and processes audit trail information to facilitate analysis of security-relevant usage and operation. Analysis can help detect security issues that need attention. The user can initiate prepared and ad hoc queries and searches to generate useful reports and user profiles. Leveraging the reports and profiles, various types of analysis can be performed such as statistical or trend analysis. Analysis can be performed at any suitable level – from high-level (abstract) analysis to very detailed analysis. Security reports may indicate that an attempt has been made to breach the security of a system, in which case, security recovery actions may need to be undertaken. Analysis of the security audit trail can be used to assess the extent of an attack and to determine appropriate damage control procedures.	• ISO 10181-7 • Open Group: Security Audit • ASTM E2147

ID #	Requirement Title	Requirement Text	Guidance[19]	Source
1.8.1	Receive & Merge Audit Trails	Provide the capability to receive and merge audit trails.	Receive and merge audit trails from Audit Archives for further analysis and reporting, possibly after identification of a potential security events months or even years later. Merging different audit trails provides the added benefit of being able to fully trace chains of events across the entire enterprise.	• Open Group: Security Audit • ISO/IEC 10181-7 • ASTM E2147
1.8.2	Convert Audit Trails to Standard Format	Provide the capability to convert standard audit records to standard formats.	Convert any local representation of an audit trail to a common interchange analysis format. This capability is essential to supporting centralized archiving and analysis of audit trails in a distributed heterogeneous environment. Required standard formats include XML, XLS, TXT, CSV, and DBF. Other formats may be implemented as necessary in addition to the required set.	• HIA • Open Group: Security Audit • ISO/IEC 10181-7
1.8.3	Generate Reports and Profiles	Provide the capability to produce reports and profiles against retrieved audit information	Produces formatted and ad hoc reports and searches, and profiling. Reporting should include using predetermined flags to generate audit summary reports by designated schedule. Profiles are based upon a record of	• Open Group: Security Audit • ISO/IEC 10181-7 • ISO

[19] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

ID #	Requirement Title	Requirement Text	Guidance[19]	Source
			historical user activities. This includes profiling user activities and access patterns. Such profiles can be used in searches and reporting. For example, searching for activities inconsistent with stored user profiles or identifying misuse. Query/Search is essential to report and profile generation. This is an audit event reduction capability. Query/Search should be efficient to operate and provide easy, on demand, menu-driven reporting within a reasonable time frame. Search/queries should provide logical controls, menu-driven sort capability based upon record content, logical operators (AND, OR, NEAR, NOT, etc.). This facilitates precise selection of the needed sub-set of audit records from the complete population of audit records. Searching should include the capability of an authorized requester to query the application to generate a report on an unscheduled basis. This feature is called for so that prompt response can be provided for incidents that are identified as a potential security breach. Managers should be able to specify queries that arise from patient, provider, or employee complaints, or a combination thereof.	27001 • ASTM E2147 • NIST SP 800-92
1.8.4	Perform Analysis	Provide the capability to perform analysis on retrieved audit information and user profiles.	Perform various analysis using reports and profiles. Types of analysis include but are not limited to trending analysis and statistical analysis. The statistical analysis should be able to be performed on any set of information retrieved by Audit Provider. Use of a graphical presentation should be considered.	• Open Group: Security Audit • ISO/IEC 10181-7 • NIST SP 800-92
1.8.5	Audit Trail Monitoring	Provide the capability to perform ongoing, real time monitoring of audit trails.	This checks audit trails and, if appropriate, produces security alarms, actions, and security audit messages. The objective is to proactively identify and investigate specific events (e.g., failed access attempts) and unusual or suspicious patterns.	• ISO 27789 • ISO/IEC 10181-7 • ISO 27001 • NIST SP

ID #	Requirement Title	Requirement Text	Guidance[19]	Source
			Monitoring also includes searching audit trails for any new alarms or actions that need to be initiated (e.g., due to revised audit or security configurations), searching alarm logs for any alarms that have come due, and searching action logs for any actions that have come due. Monitoring and identification should be performed in accordance with audit operational parameter configurations and any audit policies published by the Audit Management Service.	800-92
1.8.6	Export / Import to Audit Archive	Provide the capability to export and import audit records to and from audit archives.	Periodically export audit trail to Audit Archive Service based upon program parameters, policy and storage capabilities. Importing from the Audit Archive Service is done as needed to support audit analysis activities.	• Open Group: Security Audit • ISO/IEC 10181-7

2.6.1.2.9 Audit Archive Service

This component allows audit trails to be securely archived to allow for long-term retention, restoral, and subsequent analysis, possibly after a long-elapsed period of time.

1. "*Store Audit Trails Archive" Capability* - The audit trail is archived in accordance with archive policy and configurable parameters.

   Audit logs must be archived to a secondary but retrievable medium (separate from where files and data are being processed.). Audit logs should be retained, at a minimum, according to the statute governing medical records in the geographic area. Guidance on long-term archiving while assuring data integrity guidance is also given in the documents IETF RFC 4810 and IETF RFC 4998.

   Retention of the audit records should follow legal requirements and relevant audit and security policies. Retention of the audit records should support the corresponding life of the health records, data and documents. At a minimum, the Audit Service shall be able to store at least one year of audit online for analysis and reporting. Necessary security to protect the archives and the integrity of the audit records (e.g., digital signatures) should be implemented as necessary.

   If stored separately, internal Audit Service alarm and action information may also be archived.

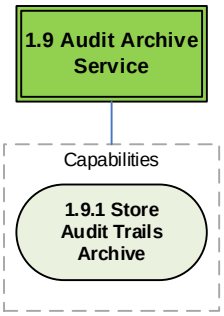

Figure 13: Audit Archive Service

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.9	***Audit Archive Service***	Description: This component allows audit trails to be securely archived to allow for long-term retention, restoral, and subsequent analysis, possibly after a long-elapsed period of time.	• ISO 10181-7 • Open Group: Security Audit

ID #	Requirement Title	Requirement Text	Guidance[20]	Source
1.9.1	Store Audit Trails Archive	Provide the capability to archive all audit trails for a duration determined by policy.	The audit trail is archived in accordance with archive policy and configurable parameters. Audit logs must be archived to a secondary but retrievable medium (separate from where files and data are being processed.). Audit logs should be retained, at a minimum, according to the statute governing medical records in the geographic area. Guidance on long-term archiving while assuring data integrity guidance is also given in the documents IETF RFC 4810 and IETF RFC 4998. Retention of the audit records should follow legal requirements and relevant audit and security policies. Retention of the audit records should support the corresponding life of the health records, data and documents. At a minimum, the Audit Service shall be able to store at least one year of audit online for analysis and reporting. Necessary security to protect the	• ISO 27789 • ISO 27001 • ASTM E2147 • NIST SP 800-92

[20] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

ID #	Requirement Title	Requirement Text	Guidance[20]	Source
			archives and the integrity of the audit records (e.g., digital signatures) should be implemented as necessary. If stored separately, alarm information may also be archived.	

2.6.1.2.10 Audit Management Service

This component provides a centralized way to define and manage operational parameters and criteria used by the various audit services. Audit management services fall into three groups: configure audit event disposition, configure audit alarm reporting, and configure audit analysis and archive.

1. "*Configure Audit Event Disposition" Capability* - Install, modify, and de-install the criteria used to control which audit events are generated and the consequential actions applied by the Audit Event Disposition Service. Some examples of criteria that may be managed include principal requesting the operations, sensitivities of the operations, attributes of the information being processed, and context of the operation.
2. *"Configure Audit Event Delivery" Capability* -
3. *"Configure Audit Event Recording" Capability* – Includes the ability to: a) Install or reinstall an audit trail. Install initializes an audit trail and designates it as the destination for recorded audit events and b) Temporarily disable or enable an audit trail. Disable/enable provides the ability to turn off and restart the addition of audit events to the specified audit trail."
4. *"Configure Audit Action" Capability* - Install, modify, uninstall the instructions that determine what happens when actions are received. This requires the specification of information such as destinations of actions messages, contents of action messages, and tasks to be performed upon receipt of actions (e.g., disable user account and terminal). Instructions also include specifying the location of the action repository, action priority levels, rules for assigning priorities to actions, and priority threshold values,
   This capability also includes disabling and enabling to temporarily turn off and restart action reporting for a specified alarm.
5. *"Configure Audit Alarm Reporting" Capability* - Install, modify, and de-install the instructions that determine actions triggered upon receipt. This requires the specification of information such as threshold values, destinations of alarm messages, contents of alarms message, and actions to be taken in addition to sending alarm (e.g., disable user account and terminal). This capability also includes the ability to turn off and restart alarm reporting for a specified alarm.
6. *"Configure Audit Event Export" Capability* – Install, modify, uninstall the instructions that specify information such as the location of the centralized (enterprise) audit trail, and the rules for moving local audit records to the central audit trail.
   This capability also includes disabling and enabling to temporarily turn off and restart export.

7. *"Configure Audit Analysis" Capability* – Install, modify, uninstall the instructions that specify information such as the location of audit trails to use, location of User Profile stores, content of User Profiles, and the location of pre-defined report templates.
8. *"Configure Audit Archive" Capability* - Install, modify, uninstall the instructions that specify information such as the location of audit trail archives, archive storage capacity/limits, and archive retention periods.
   Archive capacity/limits and retention periods should be consistent with regulatory and organizational information retention requirements.

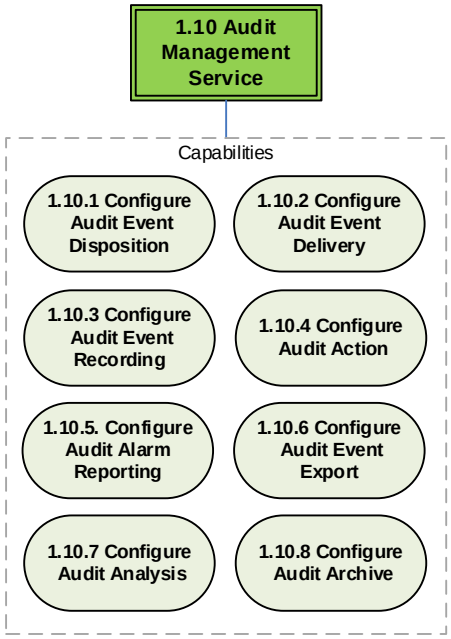

Figure 14: Audit Management Service

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.10	***Audit Management Service***	Description: This component provides a centralized way to define and manage operational parameters and criteria used by the various audit services. Audit management services fall into three groups: configure audit event discrimination, configure audit alarm reporting, and configure audit analysis and archive.	

ID #	Requirement Title	Requirement Text	Guidance[21]	Source

[21] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

ID #	Requirement Title	Requirement Text	Guidance[21]	Source
1.10.1	Configure Audit Event Disposition	Provide the capability to configure event dispositions.	Install, modify, and de-install the criteria used to control which audit events are generated and the consequential actions applied by the Audit Event Disposition Service. Some examples of criteria that may be managed include principal requesting the operations, sensitivities of the operations, attributes of the information being processed, and context of the operation.	• Open Group: Security Audit • ISO 10181-1 (ITU X.816) • NIST SP 800-92
1.10.2	Configure Audit Event Delivery	Provide the capability to configure the delivery of events to the proper services.	Install, modify, uninstall the instructions that specify the location of services to which events may be delivered (i.e., location of recording service, alarm service, and action service).	• Open Group XDAS • ISO 10181-1 (ITU X.816) • NIST SP 800-92
1.10.3	Configure Audit Event Recording	Provide the capability to configure event recording.	Includes the ability to: • Install or reinstall an audit trail. Install initializes an audit trail and designates it as the destination for recorded audit events. • Temporarily disable or enable an audit trail. o Disable/enable provides the ability to turn off and restart the addition of audit events to the specified audit trail.	• Open Group: Security Audit • ISO 10181-1 (ITU X.816) • NIST SP 800-92 • ASTM E2147

ID #	Requirement Title	Requirement Text	Guidance[21]	Source
1.10.4	Configure Audit Action	Provide the capability to configure event actions.	Install, modify, uninstall the instructions that determine what happens when actions are received. This requires the specification of information such as destinations of actions messages, contents of action messages, and tasks to be performed upon receipt of actions (e.g., disable user account and terminal). Instructions also include specifying the location of the action repository, action priority levels, rules for assigning priorities to actions, and priority threshold values, This capability also includes disabling and enabling to temporarily turn off and restart action reporting for a specified alarm.	• Open Group XDAS • ISO 10181-1 (ITU X.816) • NIST SP 800-92
1.10.5	Configure Audit Alarm Reporting	Provide the capability to configure alarm reporting.	Install, modify, uninstall the instructions that determine what happens when alarms are received. This requires the specification of information such as threshold values, destinations of alarm messages, contents of alarms message, and actions to be taken in addition to sending alarm (e.g., disable user account and terminal). This capability also includes disabling and enabling to temporarily turn off and restart alarm reporting for a specified alarm.	• Open Group: Security Audit • ISO 10181-1 (ITU X.816) • NIST SP 800-92
1.10.6	Configure Audit Event Export	Provide the capability to configure the exporting of events.	Install, modify, uninstall the instructions that specify information such as the location of the centralized (enterprise) audit trail, and the rules for moving local audit records to the central audit trail. This capability also includes disabling and enabling to temporarily turn off and restart export.	• Open Group XDAS • ISO 10181-1 (ITU X.816) • NIST SP 800-92

ID #	Requirement Title	Requirement Text	Guidance[21]	Source
1.10.7	Configure Audit Analysis	Provide the capability to configure audit analysis.	Install, modify, uninstall the instructions that specify information such as the location of audit trails to use, location of User Profile stores, content of User Profiles, and the location of pre-defined report templates.	• Open Group XDAS • ISO 10181-1 (ITU X.816) • NIST SP 800-92
1.10.8	Configure Audit Archive	Provide the capability to configure audit archiving.	Install, modify, uninstall the instructions that specify information such as the location of audit trail archives, archive storage capacity/limits, and archive retention periods. Archive capacity/limits and retention periods should be consistent with regulatory and organizational information retention requirements.	• Open Group XDAS • ISO 10181-1 (ITU X.816) • NIST SP 800-92

2.6.1.2.11 Audit Protection Service

The audit solution protects audit information and audit tools from unauthorized access, modification, and deletion. Audit information includes all information (e.g., audit records, audit trails, audit archives, audit settings, and audit reports) needed to successfully audit information system activity. Audit Protection focuses on technical protection of audit information. Physical protection of audit information is addressed by separate media protection mechanisms and physical and environmental protection mechanisms.

Figure 15: Audit Protection Service

ID #	Service/Sub-service Title	Service/ Sub-service Description	Source
1.11	***Audit Protection Service***	Description: The audit solution protects audit information and audit tools from unauthorized access, modification, and deletion. Audit information includes all information (e.g., audit records, audit trails, audit archives, audit settings, and audit reports) needed to successfully audit information system activity. Audit Protection focuses on technical protection of audit information. Physical protection of audit information is addressed by separate media protection mechanisms and physical and environmental protection mechanisms.	• NIST SP 800-53

3 INFORMATIONAL VIEWPOINT

3.1 Conceptual Information Model Level

3.1.1 Business Rules / Constraints

Business rules and constraints are identified in both DICOM Part 15 Section A.5 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

3.1.2.1 Generalized Audit Event

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 Part 15 Section A.5 healthcare audit event schema, ASTM E2147 Section 8 Disclosure Log Content, as well as the Open Group XDAS work specification and is referenced by the IHE ATNA profile.

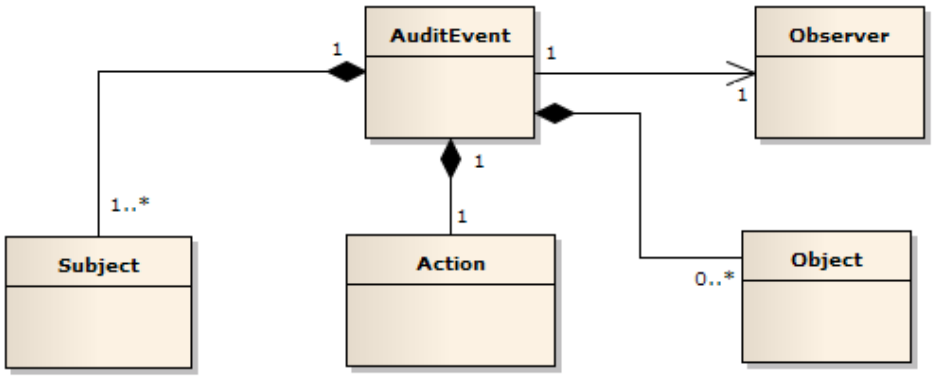

Figure 16: Generalized Audit Record Model

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 Observer – usually the active component that observes and records the activity;
- Action – the event Information that describes the activity that occurred;
- Zero or more Objects – entities that were acted upon or were involved in some passive way in the activity.

3.1.2.2 Generalized Disclosure Event

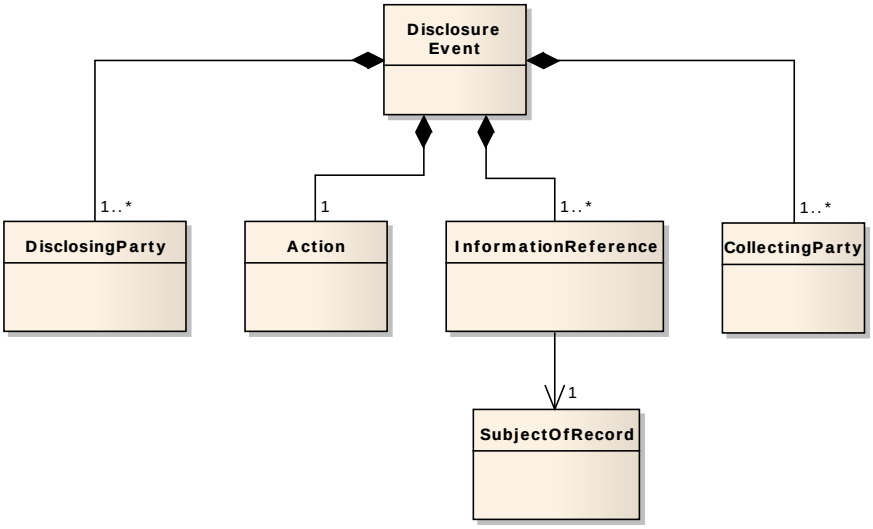

Figure 17: Generalized Disclosure Event Model

A disclosure event can be characterized as illustrated in Figure 16 above. The general properties of a disclosure event are:

- The Action that describes the disclosure 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.
- The information reference to one or more Information Object(s) that were disclosed.
- The subject of record is 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.

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.

3.1.3 Semantic Signifiers (Normative)

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.

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

The following semantic signifier elements are referenced directly from the S&P DAM[22]:

- InformationReference
- SubjectOfReference
- Patient

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.

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 have not been modeled in the S&P DAM.

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

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 January 2017, modeled these relationships.

3.1.3.2 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.

[22] HL7 Security and Privacy Domain Analysis Model – DSTU Ballot – May 2010

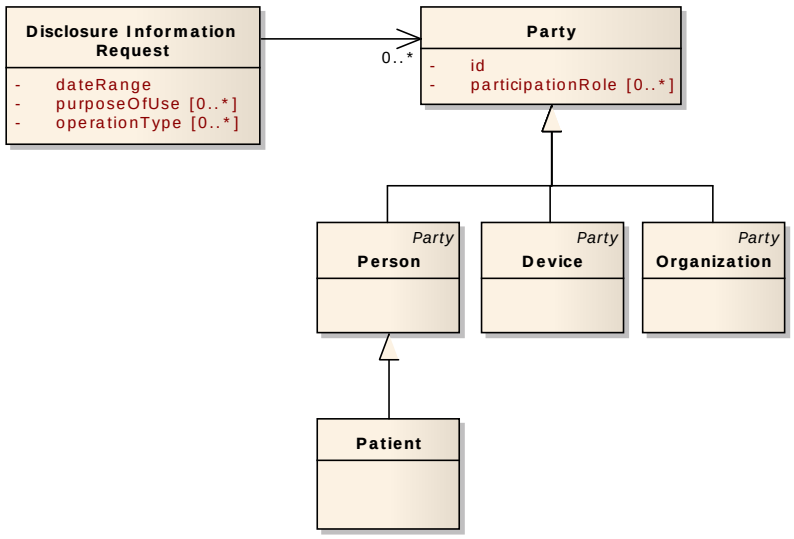

Figure 18: CIM - Disclosure Information Request Semantic Signifier

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 5: CIM - Disclosure Information Request Semantic Signifier

Element	Attribute	Description
DisclosureInformationRequest		The container for the request semantic signifier.
	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 represents 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).

3.1.3.3 Disclosure Information Response

Figure 19 below illustrates the conceptual semantic signifier associated with the response to a request for Disclosure Information 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 and used by the Audit Service in fulfilling the request.

The semantic signifier recognizes that Disclosing and Collecting 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.

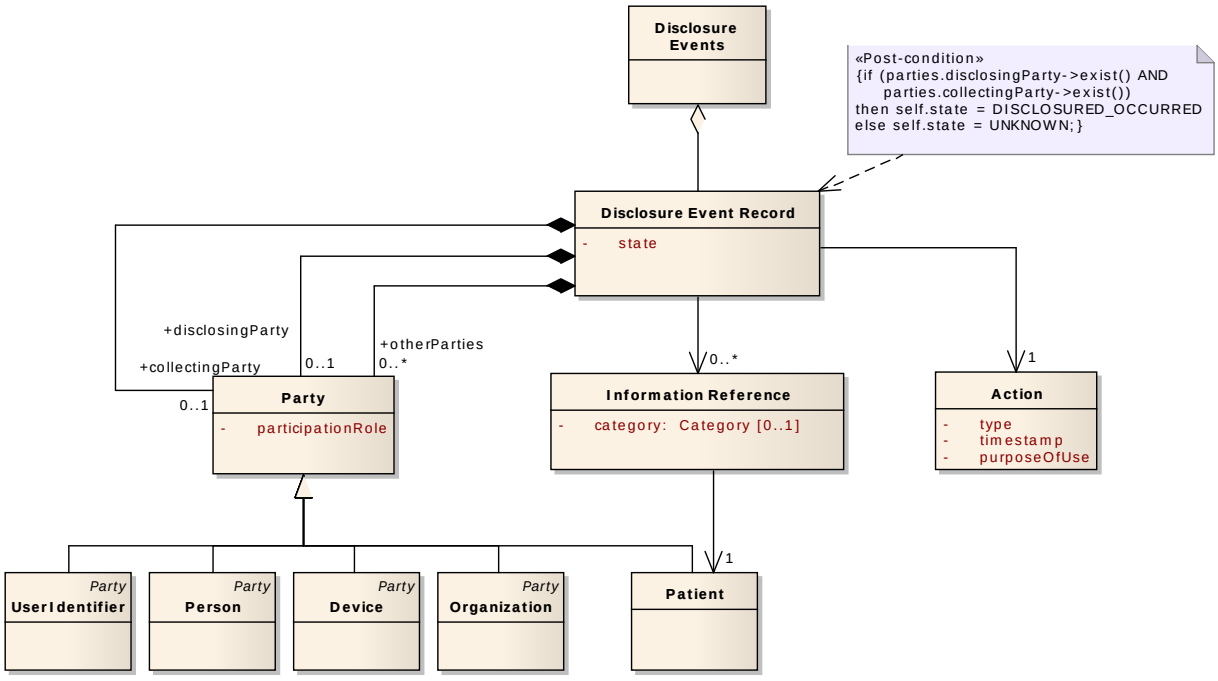

Figure 19: CIM - Disclosure Information Response Semantic Signifier

3.1.3.3.1 Disclosure Events

This class acts as the container of the audit event records that contain information that may be useful for disclosure reporting. Additional information may be needed in order to make a final determination if the audit event indicates an actual disclosure.

3.1.3.3.2 Disclosure Event Record

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 individually identifiable health information (IIHI) onto portable media may or may not 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.

3.1.3.3.3 Action

The Action class specifies the details of the event.

Table 6: 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.

3.1.3.3.4 Party

Party identifies the entities that were involved in the event.

Table 7: 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).

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 46

3.1.3.3.5 InformationReference

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

Table 8: CIM - InformationReference Element Details

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

3.1.3.3.6 Patient

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

Table 9: 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 Model Level

3.2.1 Business Rules / Constraints

Business rules and constraints are identified in both DICOM Part 15 Section A.5 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

DICOM Part 15 Section A.5 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.

3.2.2.1 Vocabulary

Table 10, 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 10: PIM - Disclosure Audit Vocabulary

Structure Name	Concept	Description
Participant.role | ParticipantCriteria.role	Authorization	The entity on whose authority the Personal Information was released.
	Destination	Ref: [DICOM]
	Information Reference	Metadata which describes the Personal Information which was the subject of this audit event. Ref: [HL7 Composite Security and Privacy Domain Analysis Model]
	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 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: [DICOM]

Structure Name	Concept	Description
	Audit Source	The entity (person, system, or device) that observed and recorded the event.
EventIdentification.purposeOfUse[23] | DisclosureRecordRequest.purposeOfUse	Reason for performing one or more operations on information, which may be permitted by source system's security policy in accordance with one or more privacy policies and consent directives.	The rationale or purpose for an act relating to the management of personal health information, such as collecting personal health information for research or public health purposes.
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 determined	No attempt has been made by the Audit Source to determine whether the event represents a disclosure.
	Disclosure unknown	No information is available regarding the disclosure status of this audit event.
	DICOM Part 15 Section A.5 table ccc2 values	See [DICOM]
	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 Part 15 Section A.5 table ccc1 values	See [DICOM]
	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

[23] Definition and description come from HL7 Healthcare Privacy and Security Classification System (HCS), Release 1, August 2014: Security Label Vocabulary, http://www.hl7.org/implement/standards/product_brief.cfm?product_id=345 . Refer to this document for an extensive list of healthcare purpose of use codes and descriptions.

Structure Name	Concept	Description
		performed.
Participant.type	DICOM Part 15 Section A.5	See [DICOM]

3.2.3 Semantic Signifiers (Normative)

3.2.3.1 AuditRecordRequest

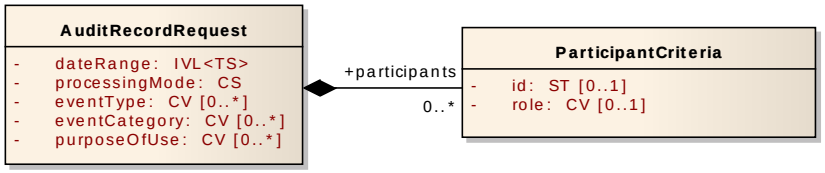

Figure 20: PIM - AuditRecordRequest Semantic Signifier

The AuditRecordRequest 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.

Table 11: 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: • 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 Part 15 Section A.5 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.

3.2.3.2 ParticipantCriteria

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

Table 12: 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)

3.2.3.3 DisclosureRecordRequest

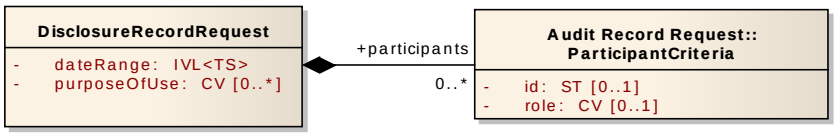

Figure 21: PIM - DisclosureRecordRequest Semantic Signifier

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

Table 13: 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.

3.2.3.4 ParticipantCriteria

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

Table 14: 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)

3.2.3.5 AuditRecordResponse

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

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

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.

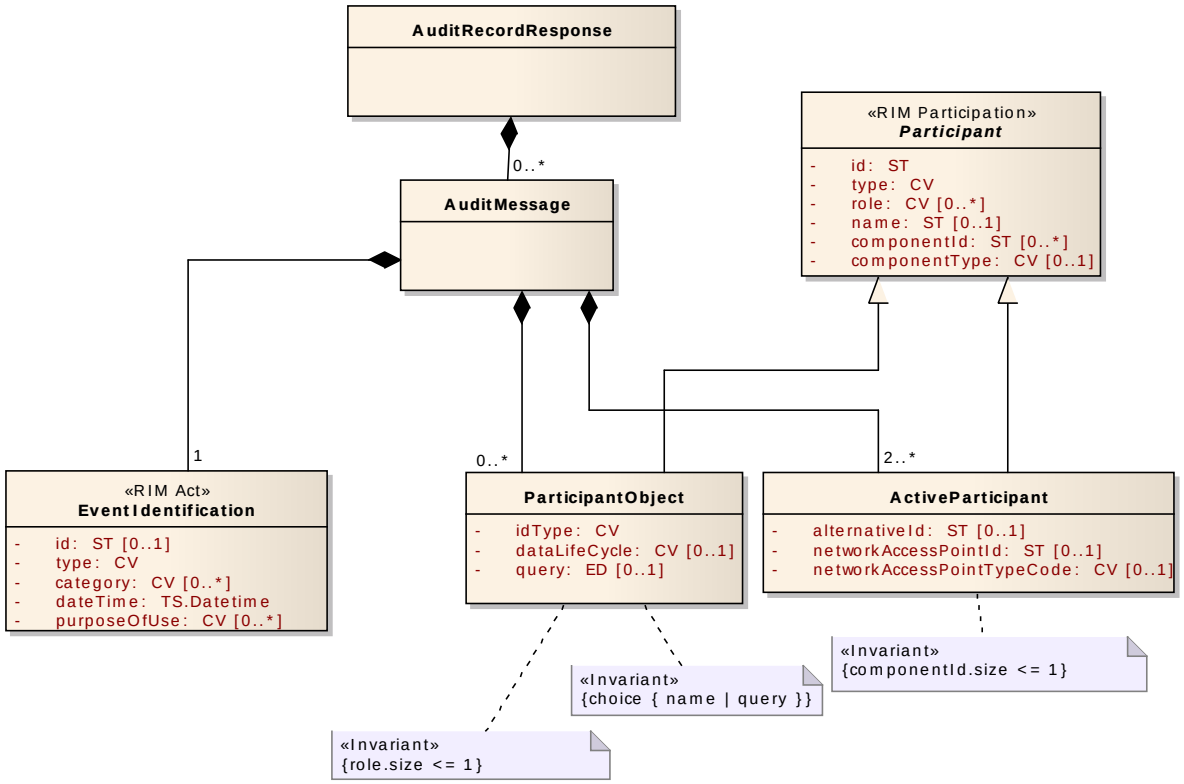

Figure 22: PIM - Audit Record Response Semantic Signifier

3.2.3.6 AuditMessage

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.

3.2.3.7 EventIdentification

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

Table 15: 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 Part 15 Section A.5 (ISO TS 12052).
purposeOfUse	An optional value indicating the legitimate purpose for which the information referenced in this audit event can be subsequently used.

3.2.3.8 Participant

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 16: PIM - DisclosureRecordResponse - 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. Note: While there may be multiple componentIds, they will all be of the same componentType for each instance of participant.

3.2.3.9 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 17: PIM - DisclosureRecordResponse - 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.

3.2.3.10 ParticipantObject

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 18: PIM - DisclosureRecordResponse - 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.

3.2.3.11 DisclosureRecordResponse

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

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.

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

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

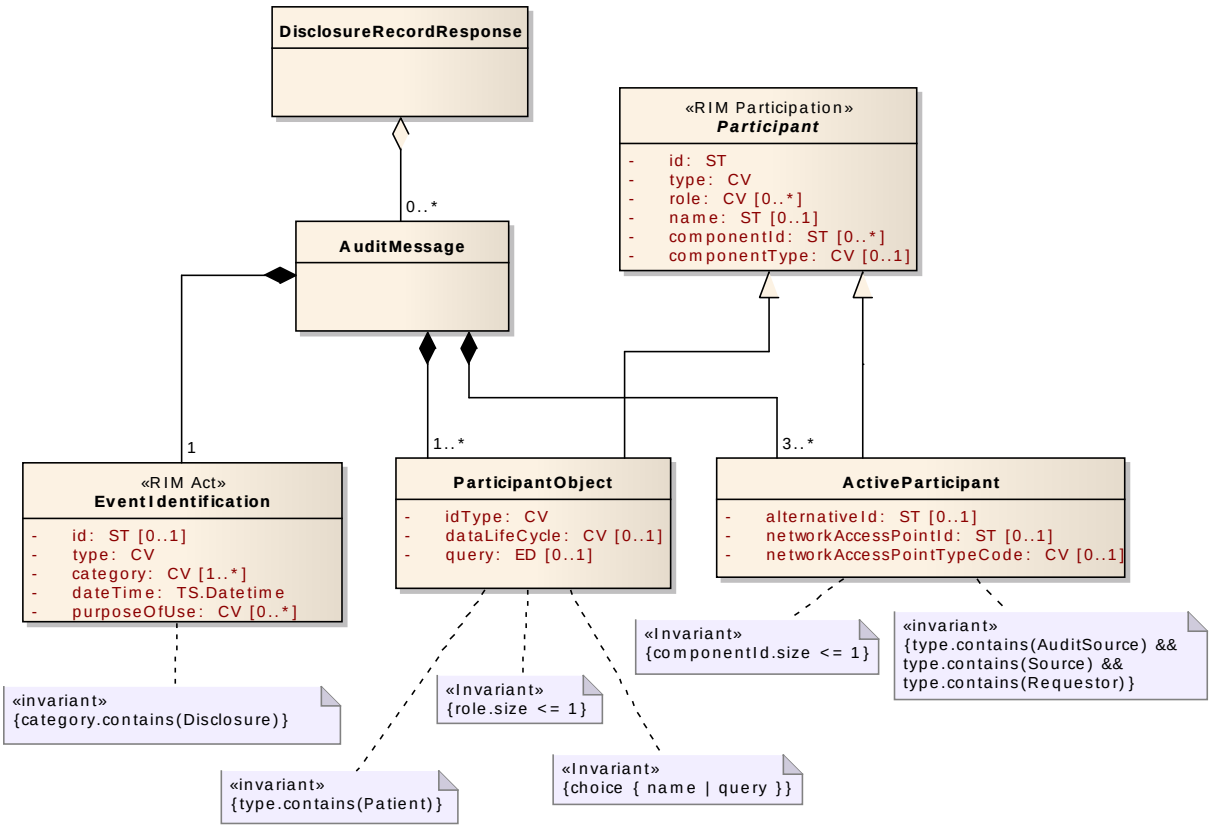

Figure 23: PIM - Disclosure Record Response Semantic Signifier

3.2.3.12 Idealized Disclosure Record

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 Part 15 Section A.5 specification. The scenarios described in the Business Viewpoint have identified the participating roles that would be relevant in a privacy context.

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

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

M – Mandatory – the attribute must be supplied,

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

U – (User) Optional – the attribute is optional and may be conditional, and

N/A – the attribute is not applicable in this context.

Table 19: Idealized Disclosure Event Record – Audit Object

Audit Object
Event (Disclosure)
Active Participants24
Source (Releasing Object/Node) (1..n)
Releasing Agent (0..1)
Receiving Agent (0..1)
Destination (Receiving Object/Node) (0..n)
Requestor (1) – Distinct Active Participant only required if no other Active Participant is identified specifically as a Requestor.
Audit Source (1) – Distinct Audit Source only required if no other Active Participant is identified specifically as an Audit Source.
Participant Objects
Patient (1)
Releasing Custodian/Controller (0..1)
Receiving Custodian/Controller (0..1)
Information Reference (0..n)
Authorization (0..1)

Where:

Table 20: 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. **Note:** Where purposeOfUse is populated, and no Authorization Participant Object exists, the purposeOfUse has been assumed.

[24] At least one ActiveParticipant must have the element UserIsRequestor set.

Table 21: 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. This is the entity that is sending. 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*
	userIsRequestor	M	*not specialized* - 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*	*not specialized*
	componentType	*U*	*not specialized*

Table 22: 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*	*not specialized*
	alternativeId	*U*	*not specialized*
	Name	*U*	*not specialized*
	networkAccessPointTypeCode	*N/A*	
	networkAccessPointId	*N/A*	
	componentId	*N/A*	
	componentType	*N/A*	

Table 23: Idealized Disclosure Event Record - Receiving Agent Participation

	Field Name	Opt	Value Constraints
Receiving Agent (if known) AuditMessage/ ActiveParticipant	Id	MC	Identity of the human that was responsible for the receipt of information. Note: Conditional on "if known."
	Role	MC	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. Note: Conditional on "if known."
	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 - 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 25: Idealized Disclosure Event Record - Destination Participation

	Field Name	Opt	Value Constraints
Destination AuditMessage/ ActiveParticipant	Id	*M*	*not specialized*
	Role	M	Destination. This is the entity that is receiving. 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*

Table 26: Idealized Disclosure Event Record - Audit Source Participation

	Field Name	Opt	Value Constraints
Audit Source AuditMessage/ AuditSource	Id	*U*	*not specialized*
	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*	*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*

Table 27: 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	*not specialized*
	idType	M	The type of Patient identifier
	Name	U	*not specialized*
	Query	U	*not specialized*
	componentId	U	*not specialized*
	componentType	U	*not specialized*

Table 28 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
	dataLifeCycle	N/A	
	idType	M	The type of Organization identifier
	Name	U	*not specialized*
	Query	U	*not specialized*
	componentId	U	*not specialized*
	componentType	U	*not specialized*

Table 29: 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
	dataLifeCycle	N/A	
	idType	M	The type of Organization identifier
	Name	U	*not specialized*
	Query	U	*not specialized*
	componentId	U	*not specialized*
	componentType	U	*not specialized*

Table 30: Idealized Disclosure Event Record - Information Reference Participation

	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	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	M	System Object
	dataLifeCycle	U	*not specialized*
	idType	M	*not specialized*
	Name	U	*not specialized*
	Query	U	*not specialized*
	componentId	MC	*If the information bundle contains known and identifiable sub-components, this attribute must contain the list of the identifiers of those sub-components.*
	componentType	MC	*If componentId contains information, this attribute must contain the type of sub-components identified.*

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

Table 31: 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	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	M	*not specialized*.
	dataLifeCycle	N/A	
	idType	M	The type of entity identifier contained in the “id” attribute
	Name	U	*not specialized*
	Query	N/A	
	componentId	N/A	
	componentType	N/A	

3.2.4 Dynamic Model

The records describing auditable events are static, and in fact most healthcare audit standards specify that the audit record log should be made immutable. However, audit needs to support capabilities including intrusion detection that necessitate requesting clients report on their status and possibly requesting additional auditing as triggers fire. For instance, if a disclosure is recorded yet there are no indications the source party was actually logged in, the requisite audit client could be requested to provide additional information.

3.3 Platform Specific Level

3.3.1 Semantic Signifiers

3.3.1.1 Submit Audit Record

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 Part 15 Section A.5. 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.

3.3.1.2 Transformations

- 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 32: Submit Audit Record - PIM to PSM Transformation - AuditRecordRequest

Semantic 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 33: 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		dateRange	As is
		purposeOfUse		purposeOfUse	As is
	ParticipantCriteria		ParticipantCriteria		As is
		id		id	As is
		role		role	As is

Table 34: 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 35: 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

Table 36: 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
AuditMessage (cont.)	ParticipantObject (cont.)	componentId		Accession.Number	Rename attribute if componentType == Accession

Signifier	PIM Classifier	PIM Attribute	HL7/ATNA Classifier	HL7/ATNA Attribute	PIM -> PSM Transformation
AuditMessage (cont.)		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
	ActiveParticipantOb Ject (cont.)	componentId		MediaIdentifier	Rename attribute
		componentType		MediaType	Rename attribute
			AuditSourceIdentification		Rename classifier if role contains Audit Source

Signifier	PIM Classifier	PIM Attribute	HL7/ATNA Classifier	HL7/ATNA Attribute	PIM -> PSM Transformation
		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

3.3.1.3 Audit Recorder Profile - Audit Message

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 24: HL7 Audit Recorder Profile - Audit Message Schema**, below.

```
datatypes xsd = "http://www.w3.org/2001/XMLSchema-datatypes"

# This defines the coded value type. The comment shows a pattern that can be used to further
# constrain the token to limit it to the format of an OID. Not all schema software
# implementations support the pattern option for tokens.
other-csd-attributes =
  (attribute codeSystemName { token } |     # OID pattern="[0-2](\.0)|(\.[1-9][0-9]*))*"
    attribute codeSystemName { token }),    # This makes clear that codeSystemName is either an OID or String
  attribute displayName { token }?,
  attribute originalText { token }              # Note: this also corresponds to DICOM "Code Meaning"
CodedValueType =
  attribute csd-code { token },
  other-csd-attributes

# Define the event identification, used later

EventIdentificationContents =
  element EventID { CodedValueType },
  element EventTypeCode { CodedValueType }*, # Note: DICOM/IHE defines and uses this
                                             # differently than RFC-3881
  attribute EventActionCode {                # Optional action code
    "C" |           ## Create
    "R" |           ## Read
    "U" |           ## Update
    "D" |           ## Delete
    "E"             ## Execute
  }?,

  attribute EventDateTime { xsd:dateTime },
  attribute EventOutcomeIndicator {
    "0" |         ## Nominal Success (use if status otherwise unknown or ambiguous)
    "4" |         ## Minor failure (per reporting application definition)
    "8" |         ## Serious failure (per reporting application definition)
    "12"          ## Major failure, (reporting application now unavailable)
  },

  element EventOutcomeDescription { text }?

# Define AuditSourceIdentification, used later
```

```
AuditSourceIdentificationContents =
  attribute AuditEnterpriseSiteID { token }?,
  attribute AuditSourceID { token },
  element AuditSourceTypeCode { AuditSourceTypeCodeContent }*

# Define AuditSourceTypeCodeContent so that an isolated single digit
# value is acceptable, or a token with other csd attributes so that
# any controlled terminology can also be used.

AuditSourceTypeCodeContent =
  attribute csd-code {
    "1" |             ## End-user display device, diagnostic device
    "2" |             ## Data acquisition device or instrument
    "3" |             ## Web Server process or thread
    "4" |             ## Application Server process or thread
    "5" |             ## Database Server process or thread
    "6" |             ## Security server, e.g., a domain controller
    "7" |             ## ISO level 1-3 network component
    "8" |             ## ISO level 4-6 operating software
    "9" |             ## other
    token },          ## other values are allowed if a codeSystemName is present
  other-csd-attributes?  ## If these are present, they define the meaning of code

# Define ActiveParticipantType, used later

ActiveParticipantContents =
  element RoleIDCode { CodedValueType }*,
  element MediaIdentifier {
    element MediaType { CodedValueType }
  }?,
  attribute UserID { text },
  attribute AlternativeUserID { text }?,
  attribute UserName { text }?,
  attribute UserIsRequestor { xsd:boolean },
  attribute NetworkAccessPointID { token }?,
  attribute NetworkAccessPointTypeCode {
    "1" |           ## Machine Name, including DNS name
    "2" |           ## IP Address
    "3" |           ## Telephone Number
    "4" |           ## Email address
    "5" }?          ## URI (user directory, HTTP-PUT, ftp, etc.)

# 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.
```



```
ValuePair =
  # clarify the name
  attribute type { token },
  attribute value { xsd:base64Binary } # used to encode potentially binary, malformed XML text, etc.

# Define ParticipantObjectIdentification, used later

# Participant Object Description, used later

DICOMObjectDescriptionContents =
  element MPPS {
    attribute UID { token }      # OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"
  }*,
  element Accession {
    attribute Number { token }
  }*,
  element SOPClass {            # SOP class for one study
    element Instance {
      attribute UID { token }    # OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"
    }*,
    attribute UID { token }?,    # OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"
    attribute NumberOfInstances { xsd:integer }
  }*,
  element ParticipantObjectContainsStudy {
    element StudyIDs {
      attribute UID { token }
    }*
  }?,
  element Encrypted { xsd:boolean }?,
  element Anonymized { xsd:boolean }?

ParticipantObjectIdentificationContents =
  element ParticipantObjectIDTypeCode { CodedValueType },
  (element ParticipantObjectName { token } |                  # either a name or
  element ParticipantObjectQuery { xsd:base64Binary }),  # a query ID field,
  element ParticipantObjectDetail { ValuePair }*,             # optional details, these can be extensive
                                  # and large
  element ParticipantObjectDescription { DICOMObjectDescriptionContents }*,
  attribute ParticipantObjectID { token },        # mandatory ID
  attribute ParticipantObjectTypeCode {        # optional type
    "1" | ## Person
    "2" | ## System object
    "3" | ## Organization
    "4"   ## Other
  }?,

  attribute ParticipantObjectTypeCodeRole {        ## optional role
```



```
  "1" |       ## Patient
  "2" |       ## Location
  "3" |       ## Report
  "4" |       ## Resource
  "5" |       ## Master File
  "6" |       ## User
  "7" |       ## List
  "8" |       ## Doctor
  "9" |       ## Subscriber
  "10" |      ## Guarantor
  "11" |      ## Security User Entity
  "12" |      ## Security User Group
  "13" |      ## Security Resource
  "14" |      ## Security Granularity Definition
  "15" |      ## Provider
  "16" |      ## Data Destination
  "17" |      ## Data Archive
  "18" |      ## Schedule
  "19" |      ## Customer
  "20" |      ## Job
  "21" |      ## Job Stream
  "22" |      ## Table
  "23" |      ## Routing Criteria
  "24" |      ## Query
  "25" |      ## Data Source
  "26"        ## Processing Element
  }?,

 attribute ParticipantObjectDataLifeCycle {        # optional life cycle stage
  "1" |       ## Origination, Creation
  "2" |       ## Import/ Copy
  "3" |       ## Amendment
  "4" |       ## Verification
  "5" |       ## Translation
  "6" |       ## Access/Use
  "7" |       ## De-identification
  "8" |       ## Aggregation, summarization, derivation
  "9" |       ## Report
  "10" |      ## Export
  "11" |      ## Disclosure
  "12" |      ## Receipt of Disclosure
  "13" |      ## Archiving
  "14" |      ## Logical deletion
  "15" }?,    ## Permanent erasure, physical destruction

 attribute ParticipantObjectSensitivity { token }?

# The basic message
```



```
message =
 element AuditMessage {
  (element EventIdentification { EventIdentificationContents }, # The event must be identified
   element ActiveParticipant { ActiveParticipantContents }+, # It has one or more active participants
   element AuditSourceIdentification {                # It is reported by one source
    AuditSourceIdentificationContents
   },
   element ParticipantObjectIdentification {            # It may have other objects involved
    ParticipantObjectIdentificationContents
   }*)
 }

# And finally the magic statement that message is the root of everything.
start = message
```

Figure 24: HL7 Audit Recorder Profile - Audit Message Schema

3.3.1.4 RetrieveAuditRecords

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 25: PSM – HL7 Audit Reporter Profile - RetrieveAuditRecords Schema**, below.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns="urn:hl7-org:v3"
           targetNamespace="urn:hl7-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>
```

Figure 25: PSM – HL7 Audit Reporter Profile - RetrieveAuditRecords Schema

3.3.1.5 RetrieveDisclosureRecords

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 **Figure 26: 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:hl7-org:v3"
           targetNamespace="urn:hl7-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: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>
```

Figure 26: PSM - HL7 Audit Reporter Profile - RetrieveDisclosureRecords Schema

4 COMPUTATIONAL VIEWPOINT

4.1 Overview

A computational viewpoint on a SAIF/RM-ODP[25] 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.

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.

4.2.1.1 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

4.2.1.2 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.

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

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

4.2.1.3 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

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.

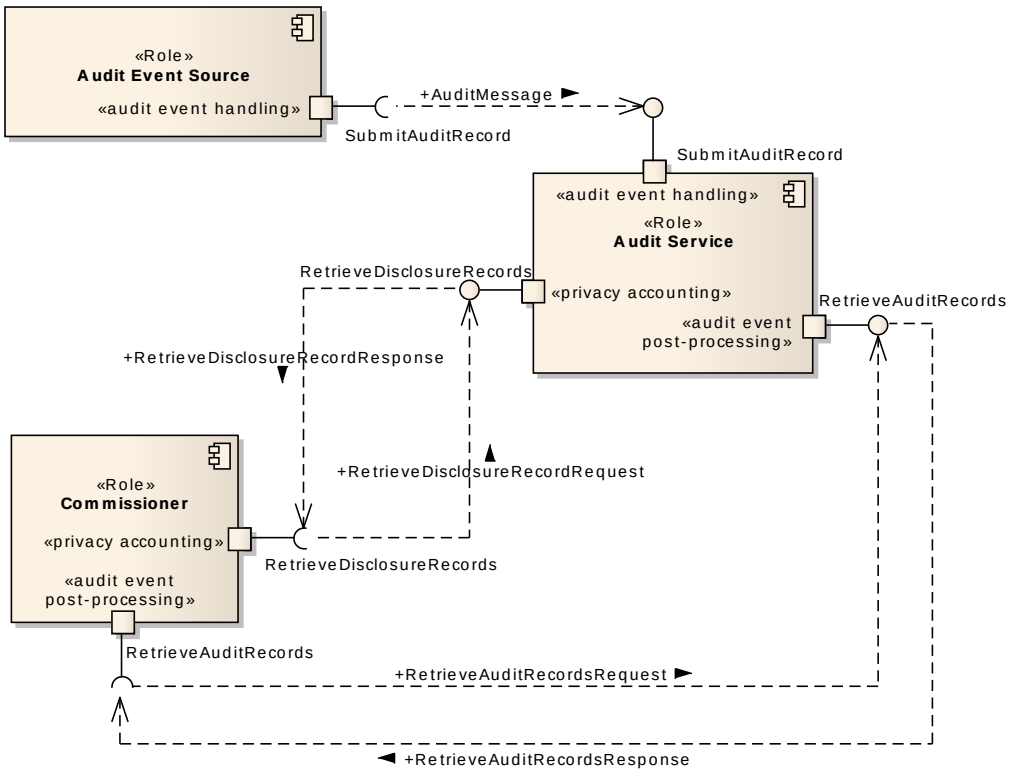

Figure 27: Audit Service Capabilities

4.2.2.1 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.

4.2.2.2 Retrieve Disclosure Records

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.

4.2.2.3 Retrieve Audit Records

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.

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.

4.2.3.1 Contracts

Contracts tie capabilities to the semantic content required to execute the behavior associated with those capabilities.

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.

4.2.3.1.1 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	[DICOM], [IHE-ITI-2A], [IHE-ITI-2B], [IHE-ITI-3], and ASTM E2147-01

4.2.3.1.2 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	AU-R1, AU-R2

4.2.3.1.3 Retrieve Audit Records

Capability Name	Retrieve Audit Records
Description	Accepts a request to receive information from Audit Event Records.
Inputs	AuditRecordRequest
Outputs	AuditRecordResponse
Healthcare-specific Requirements satisfied	AU-R1, AU-R2

4.2.3.2 Open Issues

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.

4.2.3.3 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.

4.2.3.3.1 Audit Recorder

This conformance profile includes the following contracts:

- Submit Audit Record

4.2.3.3.2 Audit Reporter

This conformance profile includes the following contracts:

- Request Audit Record
- Request Disclosure Record

4.3 Platform Independent Model

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 28: PIM - Audit Service Operations

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 3.2.3.6, AuditMessage.

4.3.2.1 Expected Behavior

- The service shall receive both well-formed and malformed AuditMessages.
- The service shall have the capability to persist received messages.

4.3.2.2 Error Responses

- There shall be no application-level error responses provided by the operation.

4.3.3 requestDisclosureRecords

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 DisclosureRecordRequest on Page 48
	DisclosureRecordResponse	Out	As defined in DisclosureRecordResponse on Page 49

4.3.3.1 Expected Behavior

- The operation shall successfully receive both well-formed and malformed DisclosureRecordRequests.
- Any optional DisclosureRecordRequest attribute that is null, shall not be used as a selection criterion for that invocation.
- 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 []))

4.3.3.2 Error Responses

- 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

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

Operation	Parameter	Direction	Description
requestAuditRecords	AuditRecordRequest	In	As defined in AuditRecordRequest on Page 48
	AuditRecordResponse	Out	As defined in AuditRecordResponse on Page 50

4.3.4.1 Expected Behavior

- The operation shall successfully receive both well-formed and malformed AuditRecordRequests.
- Any optional AuditRecordRequest attribute that is null, shall not be used as a selection criterion for that invocation.
- 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 []))

4.3.4.2 Error Responses

- 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

4.4.1 Audit Recorder Profile

- 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 66.

4.4.2 Audit Reporter Profile

Two operations are defined that make up this profile. **Figure 29: HL7 Audit Reporter Profile WSDL**, below contains the W3C Web Services Definition Language (WSDL) definition of the two query operations described in **Figure 28: PIM - Audit Service Operations**.

Note: The WSDL definition in **Figure 28** 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).

```
<?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:hl7-org:v3"
   xmlns:hl7="urn:hl7-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:hl7-org:v3"
                 targetNamespace="urn:hl7-org:v3">

            <xs:include schemaLocation="../xsd/retreiveAuditRecord.xsd"/>
            <xs:include schemaLocation="../xsd/retreiveDisclosureRecord.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="hl7:RetrieveAuditRecords.request"/>
```



```
      </message>
      <message name="retrieveAuditRecord.Response_Message">
        <part name="Body" element="hl7:RetrieveAuditRecords.response" />
      </message>
      <message name="retrieveDisclosureRecord.Request_Message">
        <part name="Body" element="hl7:RetrieveDisclosureRecords.request" />
      </message>
      <message name="retrieveDisclosureRecord.Response_Message">
        <part name="Body" element="hl7:RetrieveDisclosureRecords.response" />
      </message>
      <message name="V3PASS_Audit_malformedRequestFault">
        <part name="Body" element="hl7:malformedRequest"/>
      </message>
  <portType name="V3PASS_Audit_PortType">
    <operation name="V3PASS_Audit_retrieveAuditRecords">
      <input    message="hl7:retrieveAuditRecord.Request_Message"  wsa:Action="urn:hl7-
org:v3:V3PASS_Audit_01010010"/>
      <output  message="hl7:retrieveAuditRecord.Response_Message"  wsa:Action="urn:hl7-
org:v3:V3PASS_Audit_01010015"/>
      <fault                                                    name="malformedRequest"
message="hl7:V3PASS_Audit_malformedRequestFault"/>
    </operation>
    <operation name="V3PASS_Audit_retrieveDisclosureRecords">
      <input                      message="hl7:retrieveDisclosureRecord.Request_Message"
wsa:Action="urn:hl7-org:v3:V3PASS_Audit_01010020" />
      <output                   message="hl7:retrieveDisclosureRecord.Response_Message"
wsa:Action="urn:hl7-org:v3:V3PASS_Audit_01010025"/>
      <fault                                                    name="malformedRequest"
message="hl7:V3PASS_Audit_malformedRequestFault"/>
    </operation>
  </portType>
  <binding name="V3PASS_Audit_Binding" type="hl7:V3PASS_Audit_PortType">
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="V3PASS_Audit_retrieveDisclosureRecords">
        <soap:operation
soapAction="http://servicelocation/audit/RetrieveDisclosureRecords"/>
        <input>
              <soap:body use="literal"/>
        </input>
        <output>
            <soap:body use="literal"/>
        </output>
    </operation>
    <operation name="V3PASS_Audit_retrieveAuditRecords">
        <soap:operation
soapAction="http://servicelocation/audit/RetrieveAuditRecords"/>
```



```
        <input>
               <soap:body use="literal"/>
        </input>
        <output>
            <soap:body use="literal"/>
        </output>
    </operation>
  </binding>
  <binding name="V3PASS_Audit_Binding_Soap12" type="hl7:V3PASS_Audit_PortType">
    <soap12:binding                                                    style="document"
transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="V3PASS_Audit_retrieveDisclosureRecords">
        <soap12:operation                                          soapAction="urn:hl7-
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:hl7-
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="hl7:V3PASS_Audit_Binding">
      <soap:address location="http://servicelocation/V3PASS_Audit" />
    </port>
    <port name="V3PASS_Audit_PortSoap12" binding="hl7:V3PASS_Audit_Binding_Soap12">
    <soap12:address location="http://servicelocation/V3PASS_Audit"/>
   </port>
  </service>
</definitions>
```

Figure 29: HL7 Audit Reporter Profile WSDL

5 ENGINEERING VIEWPOINT

This section identifies the infrastructure that is required to support functional distribution of an ODP system.[26]

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.

5.1.1.1 Physical Distribution Functions

N/A

5.1.1.2 Communication Functions

N/A

5.1.1.3 Processing Functions

N/A

5.1.1.4 Storage Functions

N/A

5.1.1.5 Security Functions

N/A

5.1.2 Engineering Roles

None identified.

5.2 Platform Independent Level

5.2.1 ODP Functions

5.2.1.1 Physical Distribution Functions

N/A

5.2.1.2 Communication Functions

5.2.1.3 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.

5.2.1.4 Processing Functions

N/A

5.2.1.5 Storage Functions

N/A

[26] ISO/IEC 10746-3 Open Distributed Processing – Reference Model Architecture

5.2.1.6 Security Functions

N/A

5.2.2 Engineering Roles

None identified.

5.3 Platform Specific Level

5.3.1 ODP Functions

5.3.1.1 Physical Distribution Functions

N/A

5.3.1.2 Communication Functions

5.3.1.3 Audit Recorder – Syslog Profile

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.

Both the IHE-ITI-20 transaction [IHE-ITI-2A] and DICOM Part 15 Section A.5 [DICOM] 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 its conformance to the TLS requirements.

- 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].

5.3.1.4 Audit Reporter – SOAP Profile

The retrieveDisclosureRecords and retrieveAuditRecords operations have identical requirements from an engineering perspective.

- 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].
- 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].
- Query operations shall use a “Request-Response” message exchange pattern, as described in [HL7-WSS-R2].
- Implementations of the Audit Reporter Profile shall support both HTTP/SOAP and HTTPS/SOAP transport bindings.
- Implementations of the Audit Reporter Profile shall permit only one of HTTP/SOAP or HTTPS/SOAP transport bindings to be active.

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.

5.3.1.5 Processing Functions

N/A

5.3.1.6 Storage Functions

N/A

5.3.1.7 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.

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.

5.3.1.8 Audit Recorder – Syslog Profile

Table 37: Security Control Measures – Audit Recorder – Syslog Profile

Measure	Targeted Risk(s)
Syslog-TLS (Server authentication)	- Server masquerade - Audit clients unaware of service unavailability
Syslog-TLS (Mutual authentication)	- As above - Non-repudiation of audit source - Masquerading audit source

5.3.1.9 Audit Reporter – SOAP Profile

Table 38: Security Control Measures – Audit Reporter – SOAP Profile

Measure	Targeted Risk(s)
HTTPS (Server authentication)	- Eavesdropping - Server masquerade
HTTPS (Mutual authentication)	- As above - Non-repudiation of query client - Masquerading query client

5.3.1.10 Implementation Security Considerations

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 53, has the potential to reduce the occurrences of reporting errors as a result of correlation issues.

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.

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.

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 [DICOM]. The second record should be conformant to the “Query” event described in [DICOM].

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

5.3.2 Engineering Roles

None identified.

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	See Security Audit
Audit Analysis	The *analysis* of audit data comprises manual or automated processes which scrutinize the audit data to identify in them real or potential security threats or to track system activity for the purpose of assigning accountability. Several approaches are possible including: • to compare activity with a profile based on *normal* behavior; • to seek out unacceptable or suspicious events by establishing a rules base for inappropriate system activity. Analysis can generate filtering requirements which can be fed back into the discrimination process and provide strong reporting utilities. [Open Group XDAS]
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

Term	Description
Consistent time	Synchronized chronographic sequence
Constraint (authorization)	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
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

Term	Description
Security Audit	An independent review and examination of system records and operations in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security and to recommend any indicated changes in control, policy and procedures [ISO/IEC 7498-2].
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

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
- IHE Audit Trails and Node Authentication: http://ihe.net/Technical_Frameworks/#IT
    - [IHE-ITI-1] - IHE IT Infrastructure Technical Framework, Volume 1
    - [IHE-ITI-2A] - IHE IT Infrastructure Technical Framework, Volume 2a
    - [IHE-ITI-2B] - IHE IT Infrastructure Technical Framework, Volume 2b
    - [IHE-ITI-3] - IHE IT Infrastructure Technical Framework, Volume 3
- [DICOM] – ISO 12052 Digital Imaging and Communications in Medicine (DICOM) Part 15 Section A.5: Audit Trail Message Format Profile, 2018, http://dicom.nema.org/medical/dicom/current/output/html/part15.html#sect_A.5
- 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
- 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
- ASTM E2147-01 Standard Specification for Audit and Disclosure Logs in Use in Health Information Systems, ASTM International, June 2002.

Informative

- Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications (IETF RFC 3881).
- ISO 27789:2013 - Health informatics — Audit trails for electronic health records
- ISO TS 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
- Health Level Seven™, Inc. - HL7 V3 TRANS WS R2
  HL7 Version 3 Standard: Transport Specification - Web Services Profile, Release 2
  January 2010 (Withdrawn Ballot)

