INTERNATIONAL STANDARD

ISO 27789

Second edition
2021-10

Health informatics — Audit trails for electronic health records

Informatique de santé — Historique d'expertise des dossiers de santé informatisés

Reference number
ISO 27789:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics,* in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 251, *Health informatics,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO 27789: 2013), which has been technically revised.

The main changes are as follows:

— harmonization between audit record format and DICOM format;

— review of the content in Annex A;

— review of the chart in Annex B;

— bibliography update.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 General

Personal health information is regarded by many as among the most confidential of all types of personal information and protecting its confidentiality is essential to maintain the privacy of subjects of care. 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.

Effective audit and logging can help to uncover misuse of EHR systems or EHR data and can help organisations and subjects of care obtain redress against users abusing their access privileges. For auditing to be effective, it is necessary that audit trails contain sufficient information to address a wide variety of circumstances (see Annex A).

Audit logs are complementary to access controls. The audit logs provide a means to assess conformity with organizational access policy and can contribute to improving and refining the policy itself. But as such a policy needs to anticipate the occurrence of unforeseen or emergency cases, analysis of the audit logs becomes the primary means of ensuring access control for those cases.

This document is strictly limited in scope to logging of events. Changes to data values in fields of an EHR are presumed to be recorded in the EHR database system itself and not in the audit log. It is presumed that the EHR system itself contains both the previous and updated values of every field. This is consistent with contemporary point-in-time database architectures. The audit log itself is presumed to contain no personal health information other than identifiers and links to the record.

Electronic health records on an individual person can reside in many different information systems within and across organisational or even jurisdictional boundaries. To keep track of all actions that involve records on a particular subject of care, a common framework is a prerequisite. This document provides such a framework. To support audit trails across distinct domains, it is essential to include references in this framework to the policies that specify the requirements within the domain, such as access control rules and retention periods. Domain policies may be referenced implicitly by identification of the audit log source.

0.2 Benefits of using this document

Standardization of audit trails on access to electronic health records aims at two goals:

— ensuring that information captured in an audit log is sufficient to clearly reconstruct a detailed chronology of the events that have shaped the content of an electronic health record;

— ensuring that an audit trail of actions relating to a subject of care's record can be reliably followed, even across organizational domains.

This document is intended for those responsible for overseeing health information security or privacy and for healthcare organizations and other custodians of health information seeking guidance on audit trails, together with their security advisors, consultants, auditors, vendors and third-party service providers.

0.3 Related standards on electronic health record audit trails

This document builds upon, and is consistent with, the work begun in RFC 3881 with respect to access to the EHR. This document also builds upon and is consistent with the content in ISO/TS 21089:2018.

Health informatics — Audit trails for electronic health records

1 Scope

This document specifies a common framework for audit trails for electronic health records (EHR), in terms of audit trigger events and audit data, to keep the complete set of personal health information auditable across information systems and domains.

It is applicable to systems processing personal health information that create a secure audit record each time a user reads, creates, updates, or archives personal health information via the system.

NOTE Such audit records at a minimum uniquely identify the user, uniquely identify the subject of care, identify the function performed by the user (record creation, read, update, etc.), and record the date and time at which the function was performed.

This document covers only actions performed on the EHR, which are governed by the access policy for the domain where the electronic health record resides. It does not deal with any personal health information from the electronic health record, other than identifiers, the audit record only containing links to EHR segments as defined by the governing access policy.

It does not cover the specification and use of audit logs for system management and system security purposes, such as the detection of performance problems, application flaw, or support for a reconstruction of data, which are dealt with by general computer security standards such as ISO/IEC 15408 (all parts)[9].

Annex A gives examples of audit scenarios. Annex B gives an overview of audit log services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 27799:2016, *Health informatics — Information security management in health using ISO/IEC 27002*

ISO 8601-1, *Date and time — Representations for information interchange — Part 1: Basic rules*

ISO/TS 21089:2018, *Health informatics — Trusted end-to-end information flows*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/TS 21089:2018 and the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
access control
means to ensure that access to assets is authorized and restricted based on business and security requirements

[SOURCE: ISO/IEC 27000:2018, 3.1]

3.2
access policy
definition of the obligations for authorizing access to a resource

3.3
accountability
obligation of an individual or organization to account for its activities, for completion of a deliverable or task, accept responsibility for those activities, deliverables or tasks, and to disclose the results in a transparent manner

[SOURCE: ISO/TS 21089:2018, 3.3.1]

3.4
agent
entity that takes programmed actions, such as software or a device

[SOURCE: ISO/TS 21089:2018, 3.6.4]

3.5
alert
what is sent when the monitor service notices that a series of events matches a pattern

3.6
audit
independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures

[SOURCE: ISO/TS 21089:2018, 3.20]

3.7
audit archive
archival collection of one or more audit logs

3.8
audit data
data obtained from one or more audit records

3.9
audit log
chronological sequence of audit records, each of which contains data about a specific event

3.10
audit record
record of a single specific event in the life cycle of an electronic health record

3.11
audit system
information processing system that maintains one or more audit logs

3.12
audit trail
chronological record of system activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results

[SOURCE: GCST]

3.13
authentication
provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2018, 3.5]

3.14
authorization
granting of rights, which includes the granting of access based on access rights

[SOURCE: ISO/IEC 2382:2015, 2126256, modified — Notes to entry deleted.]

3.15
availability
property of being accessible and useable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.16
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.17
coordinated universal time
UTC
time scale which forms the basis of a coordinated radio dissemination of standard frequencies and time signals

Note 1 to entry: UTC corresponds exactly in rate with international atomic time, but differs from it by an integral number of seconds.

[SOURCE: IEC 60050-713:1998, 05-20]

3.18
data integrity
property of data whose accuracy and consistency are preserved regardless of changes made

[SOURCE: ISO 2382:2015, 2126247, modified — Notes to entry deleted.]

3.19
electronic health record
EHR
repository of (organized sets of) information regarding the health status of a subject of care, in computer processable form

[SOURCE: ISO/TR 20514:2005, 2.11, modified — Text in parenthesis added.]

3.20
electronic health record segment
EHR segment
part of an electronic health record that constitutes a distinct resource for the access policy

3.21
identification
process of recognizing the attributes that identify the object

[SOURCE: ISO 16678:2014, 2.1.7]

3.22
identifier
one or more characters used to identify or name a data element and possibly to indicate certain properties of that data element

[SOURCE: ISO/IEC 2382:2015, 2121623]

3.23
information security
preservation of confidentiality, integrity and availability of information

[SOURCE: ISO/IEC 27000:2018, 3.28]

3.24
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.25
object identifier
OID
globally unique identifier for an information object

Note 1 to entry: The object identifiers used in this document refer to code systems. These code systems can be defined in a standard or locally defined per implementation. The object identifier is specified using the Abstract Syntax Notation One (ASN.1) defined in ISO/IEC 8824-1 and ISO/IEC 8824-2.

3.26
policy
set of rules related to a particular purpose

Note 1 to entry: A rule can be expressed as an obligation, an authorization, a permission or a prohibition.

[SOURCE: ISO 19101-2:2018, modified — Note 1 to entry added]

3.27
privilege
capacity assigned to an entity by an authority

3.28
records management
field of management responsible for control of creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records

[SOURCE: ISO 15489-1:2016, 3.15, modified]

3.29
role
set of competences and/or performances associated with a task

3.30
security policy
plan or course of action adopted for providing computer security

[SOURCE: ISO/IEC 2382:2015, 2126246, modified — Notes to entry deleted.]

3.31
sensitivity
measure of the potential or perceived potential to abuse or misuse data about subjects or to harm them

3.32
subject of care
person or defined groups of persons receiving or registered as eligible to receive healthcare services or having received healthcare services

Note 1 to entry: For example, a patient, client, customer, or health plan member.

[SOURCE: ISO/TS 17975:2015, modified — Note to entry added.]

3.33
user
person or other entity authorized by a provider to use some or all of the services provided by the provider

Note 1 to entry: Also, human being using the system to issue requests to objects in order to get them to perform functions in the system on his/her behalf.

[SOURCE: COACH; OMG]

4 Abbreviated terms

HL7 ® Health Level Seven

EV Enumerated Value

5 Requirements and uses of audit data

5.1 Ethical and formal requirements

5.1.1 General

Healthcare providers have their professional ethical responsibilities to meet. Among these are protecting the privacy of subjects of care and documenting the findings and activities of care. Restricting access to health records and ensuring their appropriate use are both essential requirements in healthcare and in many jurisdictions, these requirements are set down in law.

Secure audit trails of access to electronic health records can support conformity with professional ethics, organizational policies and legislation, but they are not sufficient in themselves to assess completeness of an electronic health record.

5.1.2 Access policy

Access to the audit trail shall be governed by an access policy. This policy should be determined by the organization responsible for maintaining the audit log.

The access policy shall be in accordance with ISO 27799:2016, 9.1.1.

NOTE 1 The access policy is presumed to define an EHR segment structure.

NOTE 2 In the audit record the access policy is identified by the audit log source.

Guidance on specifying and implementing access policies can be found in ISO 22600 (all parts).[6] A field "Participant object Permission PolicySet" is defined in 7.6.6 to support referencing the actual policies in the audit record.

5.1.3 Unambiguous identification of information system users

The audit trails shall provide sufficient data to unambiguously identify all authorized health information system users. Users of the information system can be persons, but also other entities.

The audit trails shall provide sufficient data to determine which authorized users and external systems have accessed or been sent health record data from the system.

5.1.4 User roles

The audit trail shall show the role of the user while performing the recorded action on personal health information.

Information systems processing personal health information should support role-based access control capable of mapping each user to one or more roles, and each role to one or more system functions, as recommended in ISO 27799:2016, 9.2.3.

Functional and structural roles are documented in ISO 21298.[4] Additional guidance on privilege management in health is given by ISO 22600 (all parts)[6].

5.1.5 Secure audit records

Secure audit records, in accordance with ISO 27799:2016, 12.4.1, shall be created each time personal health information is read, created, updated, or archived. The audit records shall be maintained by secure records management.

5.2 Uses of audit data

5.2.1 Governance and supervision

The audit trails shall provide data to enable responsible authorities to assess conformity with the organization's policy and to evaluate its effectiveness.

This implies

— detecting unauthorized access to health records,

— evaluating emergency access, and

— detecting abuse of privileges.

and support for:

— documenting access across domains, and

— evaluation of access policies.

NOTE Full assessment of conformity with the organization's policy can require additional data that is not contained in the audit record, such as user information, permission tables or records on physical entry to secured rooms. See Annex B for audit log services.

The audit trails shall provide sufficient data to determine all access within a defined time period to the records of subjects of care, by a specified user.

The audit trails shall provide sufficient data to determine all access within a defined time period to the records of subjects of care, that are marked to be at elevated risk of privacy breaches.

5.2.2 Subjects of care exercising their rights

The audit trails shall provide sufficient data to subjects of care to enable

— assessing which authorized user(s) have accessed his/her health record and when,

— assessing accountability for the content of the record,

— determination of conformity with the subject of care's consent directives on access to or disclosure of the subject of care's data, and

— determination of emergency access (if any) granted by a user to the subject of care's record, including the identification of the user, time of access and location where accessed from.

5.2.3 Evidence and retention requirements

The audit trails shall hold data [(that care providers can use as documentary evidence)] to determine which actions were taken (create, look-up, read, correct, update, extract, output, archive, etc.) in relation to the information as well as when and by whom.

Audit records shall be retained in accordance with the retention policy as specified in 9.3.

The following documents provides guidance and further information:

— ISO/TS 21089;

— ISO/HL7 10781. [20]

6 Trigger events

6.1 General

The audit events (trigger events) that cause the audit system to generate audit records are defined according to each health information system's scale, purpose, and the contents of privacy and security policies. As the scope of this document is limited to personal health information, only trigger events relating to access and query of such information are specified here.

In order to generate the audit records that satisfy the requirement derived from Clause 5, i.e. "when", "who", "whose", audit records shall be generated for the following two events:

— Access events to personal health information;

— Query events about personal health information.

Examples of out-of-scope events are:

a) Start and stop events of the application program;

b) Authentication events involving authentication of users;

c) Input and output events from/to the external environment;

d) Access events to information other than personal health information;

e) Security alert events related to the application programs;

f) Access events to the audit log preserved in the application programs;

g) Events generated by the operating system, middleware and so on;

h) Access events generated by using system utilities;

i) Physical connection/disconnection events of equipment to the network;

j) Start/stop events of the protection systems such as anti-virus protection systems;

k) Software update events involving software modification or patch programs.

6.2 Details of the event types and their contents

6.2.1 Access events to the personal health information

In this document, the access to the personal health information is regarded as an audit event. Here "Access" means the creation, reading, update, deletion of data. The contents of the audit log provide the information about the access "when", "who" and "access to whose" data to be protected. Table 1 describes the contents in access events.

Table 1 — Access events

Event	Contents
Access events to the personal health information	When, Who, Access to whose

6.2.2 Query events to the personal health information

Querying an EHR database in order to obtain personal health information is regarded as an auditable event. The query event is the query action itself, the reference to the personal health information resulting from the query is regarded as the access event. The contents of the audit record provide the information about the query "when", "who" and "what condition for querying". Table 2 describes the contents in query events.

Table 2 — Query events

Event	Contents
Query events to the personal health information	When, Who, What condition for querying

7 Audit record details

7.1 The general record format

Table 3 describes the general format of the audit records. Regarding to the record contents of each event, see Clause 8. The record format is defined after RFC 3881 [13] and ISO 12052(DICOM PS3.15) [1], with addition of the optional fields PurposeOfUse and ParticipantObjectPolicySet.

Table 3 — General format of the audit records

Type	Field name	Option	Description	Additional info.
Event related (1)	EventID	M	ID for the audited event	See 7.2
	EventActionCode	M	Type of action performed during the audited event	
	EventDateTime	M	Date/time of the audited event occurrence	
	EventOutcomeIndicator	U	Success or failure of the event	
	EventTypeCode	U	The category of the event	
User related (1..2)	UserID	M	ID for the person or process	See 7.3
	AlternateUserID	U	Alternative ID for user or process	
	UserName	U	Name of user or process	
	UserIsRequestor	U	Indicator that the user is or is not the requestor	
	RoleIDCode	U	Specification of the role the user plays when performing the event	
	PurposeOfUse	U	Code for the purpose of use of the data accessed	
	NetworkAccessPointTypeCode	U	Type of network access point	See 7.4
	NetworkAccessPointID	U	ID for network access point	
Audit system related (1)	AuditEnterpriseSiteID	U	Site ID of audit enterprise	See 7.5
	AuditSourceID	M	Unique ID of audit source	
	AuditSourceTypeCode	U	Type code of audit source	
Participant object related (0..N)	ParticipantObjectTypeCode	M	Code for the participant object type	

Multiplicity:

(1) :Only 1 exists,

(0..1) :0 or 1 exists,

(1..2) :1 or 2 exist(s)

(0..N) :0 to N exist(s)

Optionality:

M :Mandatory

MC :Conditional Mandatory

U :Optional

M/U :Mandatory or Optional related to events

Table 3 *(continued)*

Type	Field name	Option	Description	Additional info.
	ParticipantObjectTypeCodeRole	M	Object type code of role	
	ParticipantObjectDataLifeCycle	U	Identifier for the data life-cycle stage for the participant object	
	ParticipantObjectIDTypeCode	M	Type code of Participant Object ID	
	ParticipantObjectPolicySet	U	Permission PolicySet for ParticipantObjectID	
	ParticipantObjectSensitivity	U	Sensitivity defined by the policy for ParticipantObjectID	
	ParticipantObjectID	M	Identifies a specific instance of the participant object	See 7.6
	ParticipantObjectName	U	Object name of participant, such as a person's name	
	ParticipantObjectQuery	M/U	Contents of query for the participant object	
	ParticipantObjectDetail	U	Detail of participant object	
	ParticipantObjectDescription	U	Description of participant object	
Multiplicity: (1) :Only 1 exists, (0..1) :0 or 1 exists, (1..2) :1 or 2 exist(s) (0..N) :0 to N exist(s) **Optionality:** M :Mandatory MC :Conditional Mandatory U :Optional M/U :Mandatory or Optional related to events				

7.2 Trigger event identification

7.2.1 Event ID

Description: Unique identifier for a specific audited event, e.g. a menu item, program, rule, policy, function code, application name, or URL. It identifies the performed function.

Optionality*:* Mandatory

Format/Values: Coded value, either defined by the system implementers or as a reference to a standard vocabulary. The "code" attribute shall be unambiguous and unique, at least within Audit Source ID (see 7.5). Examples of Event IDs are program name, method name, or function name.

NOTE The coding is modelled after IHE ITI TF-1 and TF-2[12] and ISO 12052(DICOM PS3.15).

For implementation-defined coded values or references to standards, the XML schema in RFC 3881 defines the optional attributes as shown in Table 4.

Table 4 — Event ID reference attributes

Attribute	Value
CodeSystem	OID reference
CodeSystemName	Name of the coding system; strongly recommended to be valued for locally-defined code-sets.
CodeValue	The specific code within the coding system
DisplayName	The value to be used in displays and reports
OriginalText	Input value that was translated to the code

To support the requirement for unambiguous event identification, multiple values may not be specified.

Rationale: This identifies the audited function. For "Execute" Event Action Code audit records, this identifies the application function performed.

At least one of CodeSystem (OID) or CodeSystemName is mandatory.

7.2.2 Event action code

Description*:* Indicator for type of action performed in the audit event.

Optionality: Mandatory

Format/Values: Enumeration as shown in Table 5.

Table 5 — Event action codes

Value	Meaning	Examples
C	Create	Create a new database object, such as Placing an Order
R	Read /Query	Read or query data, such as a diagnosis
U	Update	Update data, such as Revise Personal Health Information
D	Delete	Make items inaccessible
E	Execute	Perform a system or application function such as search, extract, or use of an object's method

Rationale: This broadly indicates what kind of action was done on the Participant Object.

NOTE 1 Actions that are not enumerated above are considered an Execute of a specific function or object interface method or treated two or more distinct events. An application action, such as an authorization or digital signing, is a function Execute, and the Event ID would identify the function.

NOTE 2 For some applications, such as radiological imaging, a Query action can only determine the presence of data but not access the data itself. Auditing need not always make as fine a distinction.

NOTE 3 Compound actions, such as "Move", "Archive" or "Copy", would be logged by creating audit data for each operation - read, create, delete - or as an Execute of a function or method.

7.2.3 Event date and time

Description: A date/time specification that is unambiguous as to local time zones.

Optionality: Mandatory

Format/Values: A date/time representation that is unambiguous in conveying universal coordinated time (UTC). The time shall be in a UTC format as per ISO 8601-1 and shall be within a tolerance of no more than 250 ms of UTC.

Rationale: This ties an event to a specific date and time. Security audits typically require a consistent time base to eliminate time-zone issues arising from geographical distribution.

NOTE In a distributed system, some sort of common time base, e.g. an NTP [RFC 1305][22] server, is a good implementation tactic.

7.2.4 Event outcome indicator

Description: Indicates whether the event succeeded or failed

Optionality: Optional

Format/Values: Coded value. A code zero (0) indicates success. Values for failure of an event are not meaningful within the scope of this document.

Rationale: This field is specified to conserve compatibility with audit trails as defined in IETF RFC 3881[13].

7.2.5 Event type code

Description: Identifier for the category of event.

Optionality: Optional

Format/Values: Coded value enumeration, either defined by the system implementers or as a reference to a standard vocabulary. For implementation defined codes or references to standards, the XML schema in RFC 3881 defines the optional attributes as shown in Table 6.

Table 6 — Event type code reference attributes

Attribute	Value
CodeSystem	OID reference
CodeSystemName	Name of the coding system; strongly recommended to be valued for locally-defined code-sets
DisplayName	The value to be used in displays and reports
OriginalText	Input value that was translated to the code

Since events can be categorized in more than one way, there can be multiple values specified.

Rationale: This field enables queries of audit records by implementation-defined event categories.

7.3 User identification

7.3.1 User ID

Description: Unique identifier for the user actively participating in the event

Optionality: Mandatory

Format/Values: User identifier text string from the authentication system. It is a unique value within the Audit Source ID (see 7.4).

Rationale: This field ties an audit event to a specific user. In this context, a user can be a person, group, team, server, process, or task thread.

NOTE 1 For cross-system audits, especially with long retention, this user identifier is meant to permanently tie an audit event to a specific user via a unique key that retains its uniqueness over the entire lifetime of the archiving of the audit trail.

NOTE 2 For node-based authentication – where only the system hardware or process, but not a human user, is identified – User ID would be the node name.

NOTE 3 If the audit trail is used for clinical audit, or to provide evidence, where needed, of misuse, the audit trail can need to record sufficient information to unambiguously associate a unique identifier with an actual user.

7.3.2 Alternative user ID

Description: Alternative unique identifier for the user

Optionality: Optional

Format/Values: User identifier text string from authentication system. This identifier would be one known to a common authentication system, if available.

Rationale: In some situations, a user may authenticate with one identity but, to access a specific application system, may use a synonymous identify. The alternative identifier would then be the original identify used for authentication, and the User ID is the one known to and used by the application.

7.3.3 User name

Description: The human-meaningful name for the user

Optionality: Optional

Format/Values: Text string

Rationale: The User ID and Alternative User ID may be internal or otherwise obscure values. This field assists the auditor in identifying the actual user.

7.3.4 User is requestor

Description: Indicator that the user is or is not the requestor, or initiator, for the event being audited.

Optionality: Optional

Format/Values: Boolean, default/assumed value is “true”

Rationale: This value is used to distinguish between requestor-users and recipient-users. For example, a report can be retrieved by a user (the requestor). Or a user (the requestor) may initiate a report to be sent to another user (who is the recipient of the report but not the requestor).

7.3.5 Role ID code

Description: Specification of the role(s) the user exercises when performing the event, as assigned in role-based access control security. Such role-based access control systems map each user to one or more roles, and each role to one or more system functions.

Optionality: Optional; multi-valued

Format/Values: Coded value, with attribute “code” valued with the role code or text from authorization system. More than one value may be specified, because more than one role-based access control system and/or taxonomy may be in use. Note that both ISO 27799:2016, 9.2.3 and ISO 22600 (all parts)[6] specify that user of a health information system containing personal health information accesses its services in a single role (i.e. users who have been registered with more than one role then designates a single role during each health information system access session).

It is recommended to use a coding system compatible with the functional roles defined in ISO 21298[4] and listed in Table 7.

The vocabulary identification for this list of coded values can be referenced by the following OID, specified using the Abstract Syntax Notation One (ASN.1) defined in ISO/IEC 8824-1[7] and ISO/IEC 8824-2[8]:

Vocabulary Identification: iso (1) standard (0) functional and structural roles (21298) functional role vocabulary (4)

Table 7 — Functional role ID codes

role_identifier	role_name	description
01	Subject of care	principal data subject of the electronic health record
02	Subject of care agent	e.g. parent, guardian, carer, or other legal representative
03	Personal healthcare professional	healthcare professional or professionals with the closest relationship to the patient, often the patient's family doctor
04	Privileged healthcare professional	nominated by the subject of care OR nominated by the healthcare facility of care (if there is a nomination by regulation, practice, etc. such as an emergency over-ride)
05	Healthcare professional	party involved in providing direct healthcare to the patient
06	Health-related professional	party indirectly involved in patient care, teaching, research, etc.
07	Administrator	any other parties supporting service provision to the patient

This identifies a high-level list of functional roles to enable interoperable exchanges across jurisdictional or domain boundaries. This can be applied to manage the creation, access, processing, and communication of health information. More granular functional roles may be asserted within a domain or jurisdiction or may be agreed upon for communications between such domains or jurisdictions.

The codes may be implementation-defined or reference a standard vocabulary enumeration. For implementation defined codes or references to standards, the XML schema in RFC 3881 defines the optional attributes as shown in Table 8.

Table 8 — Role ID code reference attributes

Attribute	Value description
CodeSystem	OID reference
CodeSystemName	Name of the coding system; strongly recommended to be valued for locally-defined code-sets
Display Name	The value to be used in displays and reports
OriginalText	Input value that was translated to the code

Rationale: This value ties an audited event to a user's role. This role is a key element in policies for control of access to personal health information

Additional guidance can be found in ISO 22600 (all parts)[6] and ISO 21298[4].

7.3.6 Purpose of use

Description: Indicates the purpose for which the accessed personal health information will be used

Optionality: Optional

Format/Values: Coded value enumeration, either defined by the system implementers or as a reference to a standard vocabulary.

It is recommended to use a coding system compatible with the scheme for classification of purposes for processing of personal health information defined in ISO/TS 14265[2] and listed in Table 9.

The vocabulary identification for this list of coded values can be referenced by the following OID, specified using the Abstract Syntax Notation One (ASN.1) defined in ISO/IEC 8824-1[7] and ISO/IEC 8824-2[8]:

Vocabulary Identification: iso (1) standard (0) Classification of Purposes for processing personal health information (14265) Terminology for classifying purposes for processing personal health information (1)

Table 9 — Purpose classification

Code	Classification Term	Description
1	Clinical care provision to an individual subject of care	To inform persons or processes responsible for providing healthcare services to the subject of care
2	Emergency care provision to an individual subject of care	To inform persons needing to provide healthcare services to the subject of care urgently, possibly requiring consent and over-ride policies distinct from those pertaining to Purpose 1 above
3	Support of care activities within the provider organization for an individual subject of care	To inform persons or processes enabling others to provide healthcare services to the subject of care, by coordinating activities and/or facilities
4	Enabling the payment of care provision to an individual subject of care	To inform persons or processes responsible for enabling the availability of funds and/or permissions from a paying party for providing healthcare services to the subject of care
5	Health service management and quality assurance	To inform persons or processes responsible for determining the availability, quality, safety, equity and cost-effectiveness of healthcare services
6	Education	To support the learning and professional development of healthcare professionals
7	Public Health Surveillance, Disease Control	To inform persons or processes with responsibility to monitor populations or sub-populations for significant health events and then intervene to provide healthcare or preventive care services to relevant individuals
8	Public safety emergency	To inform persons with responsibility for the protection of the public in a situation in which there is considered to be a significant risk to members of the public, possibly requiring consent and over-ride policies distinct from those pertaining to Purpose 7 above.
9	Population health management	To inform persons or processes with responsibility to monitor populations or sub-populations for health events, trends or outcomes in order to inform relevant strategy and policy
10	Research	To support the discovery of generalizable knowledge
11	Market Studies	To support the discovery of product or organization specific knowledge
12	Legal Procedure	To inform persons or processes responsible for enforcing legislation, or undertaking legally authorized criminal, civil or regulatory investigation
13	Subject of Care Uses	To inform the subject of care or his or her legally authorized agent in support of the subject of care's own interests or in the case of the deceased to support the care of a family member.
14	Unspecified	Disclosure on the basis of authorizations not requiring a purpose to be declared or purposes for which the other categories in this clause do not apply

Rationale: This field enables assessing conformity of the audited event with the organization's access policy.

7.4 Access point identification

7.4.1 Network access point type code

Description: An identifier for the type of network access point that originated the audit event.

Optionality: Optional

Format/Values: Enumeration as shown in Table 10.

Table 10 — Access point type codes

Value	Meaning
1	Machine Name, including DNS name
2	IP Address
3	Telephone Number

Rationale: This datum identifies the type of network access point identifier of the user device for the audit event. It is an optional value that may be used to group events recorded on separate servers for analysis of access according to a network access point's type.

7.4.2 Network access point ID

Description: An identifier for the network access point of the user device for the audit event. This could be a device id, IP address, or some other identifier associated with a device.

Optionality: Optional

Format/Values: Text may be constrained to only valid values for the given Network Access Point Type, if specified. Recommendation is to be as specific as possible where multiple options are available.

Rationale: This datum identifies the user's network access point, which may be distinct from the server that performed the action. It is an optional value that may be used to group events recorded on separate servers for analysis of a specific network access point's data access across all servers.

NOTE Network Access Point ID is not a substitute for identifying the user. Internet IP addresses, in particular, can be highly volatile and the same one can be associated with more than one person in a short time period.

EXAMPLE 1

Network Access Point ID: 192.0.2.2

Network Access Point Type Code: 2 = IP address

EXAMPLE 2

Network Access Point ID: 610-555-1212

Network Access Point Type Code: 3 = Phone Number

7.5 Audit source identification

7.5.1 Overview

Audit trail data can be collected from various sources, such as the following:

— Information systems security data;

— Directory services;

— Access policy definition services;

— Application-level access data.

Secure services are required to obtain these data.

The following data are required primarily for application systems and processes. Since multi-tier, distributed, or composite applications make source identification ambiguous, this collection of fields may repeat for each application or process actively involved in the event. For example, multiple value-

sets can identify participating web servers, application processes, and database server threads in an n-tier distributed application. Passive event participants, e.g. low-level network transports, need not be identified.

Depending on implementation strategies, it is possible that the components in a multi-tier, distributed, or composite applications may generate more than one audit record for a single application event. Various data in the audit record may be used to identify such cases, supporting subsequent data reduction. This document anticipates that the repository and reporting mechanisms perform data reduction when required, but does not specify those mechanisms.

7.5.2 Audit enterprise site ID

Description: Logical source location within the healthcare enterprise network; e.g. a hospital or other provider location within a multi-entity provider group.

Optionality: Optional

Format/Values: Unique identifier text string within the healthcare enterprise. Optional when the audit system is uniquely identified by Audit Source ID.

Rationale: This value differentiates among the sites in a multi-site enterprise health information system.

NOTE This is defined by the application that generates the audit record. It contains a unique code that identifies a business organization (owner of data) that is known to the enterprise. The value further qualifies and disambiguates the Audit Source ID. Values can vary depending on type of business. There can be levels of differentiation within the organization.

7.5.3 Audit source ID

Description: Identifier of the source where the event originated.

Optionality: Mandatory

Format/Values: Unique identifier text string, at least within the Audit Enterprise Site ID

Rationale: This field ties the event to a specific source system. It may be used to group events for analysis according to where the event occurred.

7.5.4 Audit source type code

Description: Code specifying the type of source where event originated.

Optionality: Optional

Format/Values: Coded-value enumeration, optionally defined by system implementers or as a reference to a standard vocabulary. Unless defined or referenced, the default values for the “code” attribute are as shown in Table 11.

Table 11 — Audit source type codes

Value	Meaning
1	End-user interface
2	Data acquisition device or instrument
3	Web server process tier in a multi-tier system
4	Application server process tier in a multi-tier system
5	Database server process tier in a multi-tier system
6	Security server, e.g. a domain controller

Table 11 *(continued)*

Value	Meaning
7	OSI layer 1–3 network component
8	OSI layer 4–6 operating software
9	External source, other or unknown type

For implementation defined codes or references to standards, the XML schema in RFC 3881 defines the optional attributes as shown in Table 12.

Table 12 — Audit source type reference attributes

Attribute	Value
CodeSystem	OID reference
CodeSystemName	Name of the coding system; strongly recommended to be valued for locally-defined code-sets
DisplayName	The value to be used in displays and reports
OriginalText	Input value that was translated to the code

Since audit sources may be categorized in more than one way, there may be multiple values specified.

Rationale: This field indicates which type of source is identified by the Audit Source ID. It is an optional value that may be used to group events for analysis according to the type of source where the event occurred.

7.6 Participant object identification

7.6.1 Overview

The objects of an auditable event are referred to as participant objects. The following data assist the auditing process by indicating specific instances of data or objects that have been accessed.

These data are required unless the values for Event Identification, Active Participant Identification, and Audit Source Identification are sufficient to document the entire auditable event. Production audit records containing these data might be enabled or suppressed, as determined by healthcare organization policy and regulatory requirements.

Because events may have more than one participant object, this group can be a repeating set of values. For example, depending on institutional policies and implementation choices:

— Two participant object value-sets can be used to identify access to personal health information by medical record number plus the specific healthcare encounter or episode for the subject of care.

— A subject of care and his/her authorized representative may be identified concurrently.

— An attending physician and consulting referrals may be identified concurrently.

— All subjects of care identified on a work list may be identified.

In some cases (e.g. radiological studies or transfers of large numbers of HL7®[1)] common data architecture documents), a set of related participant objects identified by accession number or study number, may be identified. Each audit record documents only a single usage instance of such participant object relationships and does not serve to document all relationships that can be present or possible.

1) HL7® is the trademarks of the Healthcare Information Management Systems Society in the United States and trademarks of IHE Europe in the European Community. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named.

7.6.2 Participant object type code

Description: Code for the participant object type being audited. This value is distinct from the user's role or any user relationship to the participant object.

Optionality: Mandatory

Format / Values: Enumeration as shown in Table 13.

Table 13 — Participant object type codes

Value	Meaning
1	Person
2	System Object
3	Organization
4	Other

Rationale: To describe the object being acted upon. In addition to queries on the subject of the action in an auditable event, it is also important to be able to query on the object type for the action.

7.6.3 Participant object type code role

Description: Code representing the functional application role of Participant Object being audited. These codes are specific to ISO 12052 (DICOM PS3.15).

Optionality: Mandatory

Format/Values: Enumeration, specific to Participant Object Type Code, as shown in Table 14.

Table 14 — Participant object role codes

Value	Meaning	Participant Object Type Codes
1	Subject of care	1 - Person
2	Location	3 - Organization
3	EHR segment	2 - System Object
4	Resource	1 – Person 3 - Organization
5	Master file	2 - System Object
6	User	1 - Person 2 - System Object (non-human user)
7	List	2 - System Object
8	Health professional	1 - Person
9	Subscriber	3 - Organization
10	Guarantor	1 - Person 3 - Organization
11	Security User Entity	1 - Person 2 - System Object
12	Security User Group	2 - System Object
13	Security Resource	2 - System Object
14	Security Granularity Definition	2 - System Object
15	Provider	1 – Person 3 - Organization

Table 14 *(continued)*

Value	Meaning	Participant Object Type Codes
16	Data Destination	2 - System Object
17	Data Repository	2 - System Object
18	Schedule	2 - System Object
19	Customer	3 - Organization
20	Job	2 - System Object
21	Job Stream	2 - System Object
22	Table	2 - System Object
23	Routing Criteria	2 - System Object
24	Query	2 - System Object

A "Security Resource" is an abstract securable object, e.g. a screen, interface, document, program, etc. – or even an audit log or repository.

Rationale: For some detailed audit analysis, it may be necessary to indicate a more granular type of participant, based on the application role it serves.

7.6.4 Participant object data life cycle and record entry lifecycle events

Description: This can be used to provide an audit trail for data, over time, as it passes through the system. Codes 1-16 originate from ISO 12052 (DICOM PS3.15). "Record entry lifecycle" events have evolved over time within the ISO/HL7 standards and now consist of 27 discrete events (which can occur during the lifespan of an EHR "record entry").

Optionality: Optional

Format/Values: Enumeration as shown in Table 15.

Table 15 — Participant object stage codes

Value	Meaning
1	Origination/Creation
2	Import/Copy from original
3	Amendment
4	Verification
5	Translation
6	Access/Use
7	De-identification
8	Aggregation, summarization, derivation
9	Report
10	Export/Copy
11	Disclosure
12	Receipt of disclosure
13	Archiving
14	Logical deletion
15	Permanent erasure/Physical destruction
16	Reclassification
Value	**Meaning**
access	Access/View Record Lifecycle Event: Occurs when an agent causes the system to obtain and open a record entry for inspection or review
hold	Add Legal Hold Record Lifecycle Event: Occurs when an agent causes the system to tag or otherwise indicate special access management and suspension of record entry deletion/destruction, if deemed relevant to a lawsuit or which are reasonably anticipated to be relevant or to fulfill organizational policy under the legal doctrine of "duty to preserve"
amend	Amend (Update) Record Lifecycle Event: Occurs when an agent makes any change to record entry content currently residing in storage considered permanent (persistent)
archive	Archive Record Lifecycle Event: Occurs when an agent causes the system to create and move archive artefacts containing record entry content, typically to long-term offline storage
attest	Attest Record Lifecycle Event: Occurs when an agent causes the system to capture the agent's digital signature (or equivalent indication) during formal validation of record entry content
decrypt	Decrypt Record Lifecycle Event: Occurs when an agent causes the system to decode record entry content from a cipher
deidentify	De-Identify (Anonymize) Record Lifecycle Event: Occurs when an agent causes the system to scrub record entry content to reduce the association between a set of identifying data and the data subject in a way that might or might not be reversible
deprecate	Deprecate Record Lifecycle Event: Occurs when an agent causes the system to tag record entry(ies) as obsolete, erroneous or untrustworthy, to warn against its future use
destroy	Destroy/Delete Record Lifecycle Event: Occurs when an agent causes the system to permanently erase record entry content from the system
disclose	Disclose Record Lifecycle Event: Occurs when an agent causes the system to release, transfer, provision access to, or otherwise divulge record entry content
encrypt	Encrypt Record Lifecycle Event: Occurs when an agent causes the system to encode record entry content in a cipher
extract	Extract Record Lifecycle Event: Occurs when an agent causes the system to selectively pull out a subset of record entry content, based on explicit criteria
link	Link Record Lifecycle Event: Occurs when an agent causes the system to connect related record entries
merge	Merge Record Lifecycle Event: Occurs when an agent causes the system to combine or join content from two or more record entries, resulting in a single logical record entry

Table 15 *(continued)*

Value	Meaning
originate	Originate/Retain Record Lifecycle Event: Occurs when an agent causes the system to: a) initiate capture of potential record content, and b) incorporate that content into the storage considered a permanent part of the health record
pseudonymize	Pseudonymize Record Lifecycle Event: Occurs when an agent causes the system to remove record entry content to reduce the association between a set of identifying data and the data subject in a way that may be reversible
reactivate	Re-activate Record Lifecycle Event: Occurs when an agent causes the system to recreate or restore full status to record entries previously deleted or deprecated
receive	Receive/Retain Record Lifecycle Event: Occurs when an agent causes the system to a) initiate capture of data content from elsewhere, and b) incorporate that content into the storage considered a permanent part of the health record
reidentify	Re-identify Record Lifecycle Event: Occurs when an agent causes the system to restore information to data that allows identification of information source and/or information subject
unhold	Remove Legal Hold Record Lifecycle Event: Occurs when an agent causes the system to remove a tag or other cues for special access management had required to fulfil organizational policy under the legal doctrine of "duty to preserve"
report	Report (Output) Record Lifecycle Event: Occurs when an agent causes the system to produce and deliver record entry content in a particular form and manner
restore	Restore Record Lifecycle Event: Occurs when an agent causes the system to recreate record entries and their content from a previous created archive artefact
transform	Transform/Translate Record Lifecycle Event: Occurs when an agent causes the system to change the form, language or code system used to represent record entry content
transmit	Transmit Record Lifecycle Event: Occurs when an agent causes the system to send record entry content from one (EHR/PHR/other) system to another
unlink	Unlink Record Lifecycle Event: Occurs when an agent causes the system to disconnect two or more record entries previously connected, rendering them separate (disconnected) again
unmerge	Unmerge Record Lifecycle Event: Occurs when an agent causes the system to reverse a previous record entry merge operation, rendering them separate again
verify	Verify Record Lifecycle Event: Occurs when an agent causes the system to confirm compliance of data or data objects with regulations, requirements, specifications, or other imposed conditions based on organizational policy

Rationale: Institutional policies for privacy and security may optionally fall under different accountability rules based on data life cycle. This provides a differentiating value for those cases.

7.6.5 Participant object ID type code

Description: Describes the identifier that is contained in Participant Object ID.

Optionality: Mandatory

Format Values: Coded-value enumeration, specific to Participant Object Type Code, using attribute-name "code". The codes in Table 16 are the default set.

Table 16 — Participant object ID type codes

Value	Meaning	Participant Object Type Codes
1	Medical Record Identifier	1 - Person
2	Subject of Care Identifier	1 - Person
3	Encounter Identifier	1 - Person
4	Insurance Enrolee Identifier	1 - Person

Table 16 *(continued)*

Value	Meaning	Participant Object Type Codes
5	National personal identifier for healthcare services (e.g. Social Security Number)	1 - Person
6	Account Identifier	1 – Person 3 - Organization
7	Guarantor Identifier	1 – Person 3 - Organization
8	Report Name	2 - System Object
9	Report Identifier	2 - System Object
10	Search Criteria	2 - System Object
11	System User Identifier	1 – Person 2 - System Object
12	Uniform Resource Identifier (URI)I	2 - System Object
13	Object Identifier (e.g. record identifier, lab test Identifier, etc.)	2 – System Object

User Identifier and URI [RFC 2396][23] text strings are intended to be used for security administration trigger events to identify the objects being acted-upon.

The codes may be the default set stated above, implementation-defined, or reference a standard vocabulary enumeration, such as HL7® V2 Table 0207 Processing Mode[21] or ISO 12052 (DICOM PS3.15) defined media types.

For implementation defined codes or references to standards, the XML schema in RFC 3881 defines the optional attributes as shown in Table 17.

Table 17 — Participant object ID code reference attributes

Attribute	Value
CodeSystem	OID reference
CodeSystemName	Name of the coding system; strongly recommended to be valued for locally-defined code-sets
DisplayName	The value to be used in displays and reports
OriginalText	Input value that was translated to the code

Rationale: Required to distinguish among various identifiers that can synonymously identify a participant object.

7.6.6 Participant object Permission PolicySet

Description: Pointer to the policies that govern access to the Participant Object ID

Optionality: Optional

Format /Values: Values are institution- and implementation-defined text strings.

7.6.7 Participant object sensitivity

Description: Denotes policy-defined sensitivity for the Participant Object ID such as VIP, HIV status, mental health status, or similar topics.

Optionality: Optional

Format/Values: Values are institution- and implementation-defined text strings.

7.6.8 Participant object ID

Description: Identifies a specific instance of the participant object.

Optionality: Mandatory

Format/Values: Text string. Value format depends on Participant Object Type Code and the Participant Object ID Type Code.

Rationale: This field identifies a specific instance of an object, such as a subject of care, to detect/track privacy and security issues.

NOTE This field might be the primary unique identifier key for the object, so it can be a composite data field as implemented.

7.6.9 Participant object name

Description: An instance-specific descriptor of the Participant Object ID audited, such as a person's name.

Optionality: Optional

Format/Values: Text string

Rationale: This field may be used in a query/report to identify audit events for a specific person, e.g. where multiple synonymous Participant Object IDs (subject of care identifier, medical record identifier, encounter identifier, etc.) have been used.

7.6.10 Participant object query

Description: The actual query for a query-type participant object.

Optionality: Conditional mandatory

Format/Values: Base 64 encoded data

Rationale: For query events, it may be necessary to capture the actual query input to the query process in order to identify the specific event. Because of differences among query implementations and data encoding for them, this is a base 64 encoded data blob. It may be subsequently decoded or interpreted by downstream audit analysis processing.

7.6.11 Participant object detail, Participant object description

Description: Implementation-defined data about specific details of the object accessed or used.

Optionality: Optional

Format: Type-value pair. The “type” attribute is an implementation-defined text string. The “value” attribute is a base 64 encoded data blob.

Rationale:

Specific details or values from the object accessed may be desired in specific auditing implementations. The type-value pair enables the use of implementation-defined and locally-extensible object type identifiers and values. For example, a clinical diagnostic object may contain multiple test results, and this element could document the type and number and type of results.

Many possible data encodings are possible for these elements, so the value is a base 64 encoded data blob. It may be subsequently decoded or interpreted by downstream audit analysis processing.

8 Audit records for individual events

8.1 Access events

This audit record, as shown in Table 18, describes creation, reading, modification and deletion of the personal health information.

Table 18 — Audit record format for access events

Category	Field Name	Option	Restriction of values
Event related	EventID	M	ID of audit event. Following value is set: EV (110110, DCM, "Patient Record")
	EventActionCode	M	The action executed in the event which generated the audit log. Following value is set: EV: "C" (Create) "R" (Read) "U" (Update) "D" (Delete)
	EventDateTime	M	The data/time of the event's occurrence:
	EventOutcomeIndicator	U	Code for success (or failure) of the event
	EventTypeCode	U	The type of event:
User related (1..2)	UserID	M	The ID of the person or process operating the data. In case that both the person and the process are known, both are to be included. This is a unique value at the audit source (AuditSourceID).
	AlternateUserID	U	The alternative ID of the person or the process operating the data.
	UserName	U	The name of the person or process operating the data.
	UserIsRequestor	U	This value shows if the person or the process operating the data are the requester of this event or not. Following value is set: EV TRUE
	RoleIDCode	U	The role of the person or the process operating the data when performing the event.
	PurposeOfUse	U	Code indicating the purpose of use of the data accessed
	NetworkAccessPointTypeCode	U	Type code of the network access point.
	NetworkAccessPointID	U	ID for the network access point.
Source system related (1)	AuditEnterpriseSiteID	U	The logical location of the source system. Used to modify AuditSourceID.
	AuditSourceID	M	The unique ID of the source system.
	AuditSourceTypeCode	U	The type code of the source system.
Participant object related (information of accessed patient) (1)	ParticipantObjectTypeCode	M	The type code of the participant object. Following value is set: EV 1 (person)
	ParticipantObjectTypeCodeRole	M	The role code of the participant object. Following values is set. EV 1 (patient)
	ParticipantObjectDataLifeCycle	U	The lifecycle stage ID of the participant object.

Table 18 *(continued)*

Category	Field Name	Option	Restriction of values
	ParticipantObjectIDTypeCode	M	The type code that contained in ParticipantObjectID. Following value is set: EV 2 (patient ID).
	ParticipantObjectPolicySet	U	The active Permission PolicySet for ParticipantObjectID e.g. patient consent information
	ParticipantObjectSensitivity	U	The policy-defined sensitivity for ParticipantObjectID.
	ParticipantObjectID	M	The instance ID of the participant object. Patient ID is set.
	ParticipantObjectName	U	The name of the participant object. Subject of care's name is set.
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	The detail of the participant object instance.
	ParticipantObjectDescriptiom	U	The description of the participant object instance.
Participant object related (information of accessed EHR segment) (0..N))	ParticipantObjectTypeCode	M	The type code of the participant object. Following value is set: EV 2 (system object)
	ParticipantObjectTypeCodeRole	M	The role code of the participant object. Following values is set. EV 3 (EHR segment)
	ParticipantObjectDataLifeCycle	U	The lifecycle stage ID of the participant object.
	ParticipantObjectIDTypeCode	M	The type code that contained in ParticipantObjectID. Following value is set: EV 13 (Object ID).
	ParticipantObjectPolicySet	U	The active Permission PolicySet for ParticipantObjectID
	ParticipantObjectSensitivity	U	The policy-defined sensitivity for ParticipantObjectID.
	ParticipantObjectID	M	The instance ID of the participant object. EHR segment ID is set.
	ParticipantObjectName	U	The name of the participant object. EHR segment name is set.
	ParticipantObjectDetail	U	The detail of the participant object instance.
	ParticipantObjectDescriptiom	U	The description of the participant object instance.

8.2 Query events

In this audit record, shown in Table 19, the event of a Query being issued or received is described. It does not record the response to the query, but merely the fact that a query was issued.

Table 19 — Audit record format of query events

Category	Field Name	Option	Restriction of values
Event related.	EventID	M	ID of audit event. Following value is set: EV (110112, DCM, "Query")
	EventActionCode	M	The action executed in the event that generated the audit log. Following value is set: EV "E" (Execute)
	EventDateTime	M	The data/time of the event's occurrence:
	EventOutcomeIndicator	U	Code for success (or failure) of the event
	EventTypeCode	U	The type of event:
Questioner related(1)	UserID	M	The process operating the data. This is a unique value at the audit source AuditSourceID).
	AlternateUserID	U	The alternative ID of the person or the process operating the data.
	UserName	U	The name of the process operating the data.
	UserIsRequestor	U	This value shows if the person or the process operating the data are the requester of this event or not.
	RoleIDCode	U	The role of the person or the process operating the data when performing the event.
	PurposeOfUse	U	Code indicating the purpose of use of the data accessed
	NetworkAccessPointTypeCode	U	Type code of the network access point.
	NetworkAccessPointID	U	ID for the network access point.
Question ahead related(1)	UserID	M	The ID of the process that responds to the query. This is a unique value at the audit source (AuditSourceID).
	AlternateUserID	U	The alternative ID of the process that responds to the query.
	UserName	U	The name of the process that responds to the query.
	UserIsRequestor	U	This value shows if the process that responds to the query is the requester of this event or not.
	RoleIDCode	U	The role code of the process that operated the data at the execution time.
	NetworkAccessPointTypeCode	U	Type code of the network access point.
	NetworkAccessPointID	U	ID for the network access point.
Alternative participant related(0..N)	UserID	M	The ID of the participant that is related and known. Especially the person or process is the requestor. This is a unique value at the audit source (AuditSourceID).
	AlternateUserID	U	The alternative ID of the alternative participant.
	UserName	U	The alternative name of the alternative participant.
	UserIsRequestor	U	This value shows if the alternative participant is the requester of this event or not.
	RoleIDCode	U	The role of the alternative participant.
	NetworkAccessPointTypeCode	U	Type of the network access point.
	NetworkAccessPointID	U	ID for the network access point.

Table 19 *(continued)*

Category	Field Name	Option	Restriction of values
Source system related (1)	AuditEnterpriseSiteID	U	The logical location of the source system. Used to modify AuditSourceID.
	AuditSourceID	M	The unique ID of the source system.
	AuditSourceTypeCode	U	The type code of the source system.
Participant object related (query contents) (1)	ParticipantObjectTypeCode	M	The type code of the participant object. Following value is set: EV 2 (system)
	ParticipantObjectTypeCodeRole	M	The role code of the participant object. Following values is set. EV 3 (report)
	ParticipantObjectDataLifeCycle	U	The lifecycle stage ID of the participant object.
	ParticipantObjectIDTypeCode	M	The type included in ParticipantObjectID. Following value is set: EV 10 (query formula)
	ParticipantObjectPolicySet	U	The active Permission PolicySet for ParticipantObjectID
	ParticipantObjectSensitivity	U	The policy-defined sensitivity for ParticipantObjectID.
	ParticipantObjectID	M	The instance ID of the participant object.
	ParticipantObjectName	U	The name of the participant object.
	ParticipantObjectQuery	M	The query contents that is coded by base 64. When there is a requirement to analyse the contents, this shall be performed by the developer vendor.
	ParticipantObjectDetail	U	The detail of the participant object instance.
	ParticipantObjectDescription	U	The description of the participant object instance.

9 Secure management of audit data

9.1 Security considerations

IETF RFC 3881, 7 states the criteria in relation to the maintenance of confidentiality and integrity of health records and the integrity and availability of health information systems.

Management of audit records should follow ISO 15489.[3] Security requirements for archiving of audit records are similar to those for archiving of electronic health records specified in ISO/TS 21547[5].

Guidance on long-term archiving while assuring data integrity guidance is also given in IETF RFC 4810[24] and IETF RFC 4998[25].

Special attention should be given to the security of distributed audit trails. Whereas electronic health records may be distributed over multiple information systems and spanning distinct security policy domains, this also pertains to audit trails. Security shall be maintained over the distributed audit trails.

9.2 Securing the availability of the audit system

The audit system shall provide sufficient measures to ensure that entries are made in the audit trail whenever the health information system is operational.

The audit system shall log all instances when the audit trail has been out of service, turned off or not functional because of a system failure.

The audit system shall show or report which audits are on/off at any given time.

9.3 Retention requirements

Audit records shall be subject to a retention policy, determined by the organization responsible for the audit log.

Retention of the audit records should follow relevant requirements and policies.

Retention of the audit records should support the life of the health records, data and documents.

9.4 Securing the confidentiality and integrity of audit trails

The audit system shall provide sufficient security measures to protect audit logs from tampering. In particular, it shall

a) secure access to audit records,

b) safeguard access to system audit tools to prevent misuse or compromise,

c) keep track of all actions to the audit trail by a secure log specifying time, action and actor,

d) log all occasions when the audit trail has been out of service, turned off or not functional because of a system failure, and

e) report of which audits are on/off at any given time.

9.5 Access to audit data

Access to audit data shall be strictly controlled and itself subject to audit. Access should be by an appropriate information system that can enforce these controls, rather than directly to the audit trail itself.

Auditing facilities should provide analysis of the audit trail by any of the coded or named fields defined in Clause 7, with date/time periods where appropriate individually or in combination (e.g. all access by user X, all "delete" events by users of role "Y", all events involving subject of care "Z" in the past month, etc.).

In some cases, it can be necessary for an audit user to access information sources in addition to the audit trail, for example to spot patterns (e.g. all searches on children carried out by a user who is not a paediatrician or affiliated with paediatrics).

Annex A
(informative)

Audit scenarios

A.1 Overview

There are many types of audit: security, privacy, forensic, provisioning, system performance, network performance, configuration management, intrusion detection, etc. This annex describes various scenarios for use of audit logs.

A.2 Case of the data subject sensitivity

A.2.1 General

The scenario in each case is described below.

A.2.2 Disgruntled celebrity or VIP

While a celebrity is in hospital, someone on staff, aware of the subject of care's celebrity status uses the nursing information system to look up the subject of care's room number and health record information, and sells it to a newspaper for cash.

The subject of care, upon finding his/her picture on the cover of a prominent newspaper, complains to the hospital's privacy officer. The privacy officer uses the audit repository to scan through all the accesses to the subject's health record and discovers one that occurred outside of the scheduled check-up times. Two nurses were on staff at that time and after some investigation, one of them confesses and is reprimanded.

This scenario depends on both audit recording as well as a process for auditing the activity that was recorded. It should include

- creation of audit record /log,
- transmission of audit record /log to repository,
- reception of audit record /log,
- storing of audit record/log,
- querying/searching audit log to determine what happened. This in turn requires
  - search by date capability, and
  - audit systems that, at a minimum
    - identify every user that was reported to have looked at a given subject of care's records,
    - identify every instance of a given user accessing any subject of care's record, and
    - identify every instance of a node accessing a subject of care's record.
  - conformity with RFC 3881, to make searching possible
  - where radiology workflow is being audited, conformity with ISO 12052 (DICOM PS3.15).

A.2.3 Additional subject sensitivity

In addition to the scenario above, there is a number of potential subjects of care with specific audit needs:

— Subjects where the attacker is highly motivated, e.g. a subject who is unknowingly being stalked.

— A victim of violence:

The subject of care notifies the privacy officer to disable access to personal health information by tagging it differently from labels used to identify a VIP (Administration can have a standard set of tags to identify this kind of data subject). For audit, this case should not record that the subject of care is a "victim of violence" but rather should record that a security violation alert was sent to the privacy officer or security officer. It would be useful to record a "code" for this violation but not clearly identify it in plain text in the audit record.

On the audit side, the following could be standardized:

— Categories of security alert – need a mechanism to send a security alert. There would be a security alert for a potential stalking/illicit activity scenario as well as stronger alerts for the scenarios outlined below.

— Will have codes and trust the application to detect a pattern

— Capability to apply policy to audit processing, where the policy defines when and what to alert

— Need to use this functionality from syslog: selective forwarding of logs that match specific (simple) patterns to a separate application that is not part of the basic audit service. This other "watcher" application will "look" for bad behaviour and send alerts (this kind of application could also work for hardware problems).

— Basic data extract capability from the audit archive

— Option: add a plug-in for specific searches of audit repository, but at minimum provide the ability to dump all data from the audit database in order to do the manual analysis in phase 1

Notification service can be simple or sophisticated but needs to know what to send where. The notification service can be an optional dependent service. There are two variations on this case to be considered:

a) High-profile subjects of care where the attacker is not highly motivated:

   Initial threat environment: Subjects where the attacker is not highly funded or motivated; i.e.: the attacker will not spend a lot of time bribing an insider or won't spent time as an insider directly querying a database. These are only examples of inappropriate "normal" transactions. Audit repository should be query-able for accesses by IP, PID, user, interval of time, etc.

b) High-profile subjects of care where the attacker is highly motivated:

   Attackers who have used the query capabilities of underlying databases and not just the exposed search functions of the repository interface to obtain information (e.g.: database administrators).

Required functionality: Query audit logs according to subject of care ID, access time and user ID, generic analysis of repository

Audit repository will need to be able to dump audit records based on PID, system ID, time window, etc.

Reporting service will receive coded info from repository and display report in whatever way they choose (preferably a usable one)

Required interface: (where audit repository shall send a message that report service and analysis service can understand) (provided interface is the other half)

Four levels:

a) Events related to a specific subject of care: don't bother looking at any queries, just tell me if there are audit events associated with this data subject.

b) Tell me queries that you know would have returned results about a data subject even if the data subject's ID is not listed: deterministic/not time sensitive queries (like XDS stored queries).

c) Give me all events subject to a few windows of criterion: user, time window, event type and set of systems of interest. (e.g.: all logins and logouts).

d) Complex: custom queries, ISO 12052 (DICOM) queries, lab workflow queries that are workflow dependent and require you to know state of database at the time the query was done.

Levels a, b and c may be via direct interface to repository.

An analysis service may be used for item d and layered on top.

Potential functionality: Query audit logs manually or using analysis service

Potential new scope for audit: Perform analysis/comparison/correlation between scheduling logs and audit logs to show unscheduled/unusual accesses.

Optional services: Query repository/analysis service

A.3 Case of the enforced legislative right to privacy (retrospective, not active)

In this scenario, a subject of care does not want his/her next door neighbour, a healthcare provider, to be aware of his/her health status. The data subject can issue a consent directive to his/her primary care physician to block all access from the healthcare provider neighbour to his/her healthcare records. A few weeks later, the privacy officer in the primary care physician's clinic receives an alert that the neighbour tried to access the records in violation of institutional policy and that the access was refused. The privacy officer notifies the data subject of the attempted access and that it was unsuccessful.

Required functionality: List accesses to health records by physician/user login; list/show failed accesses; and provide alerts when an event that is unauthorized by consent directive is captured.

— Low/high profile use case also needs the retrospective audit analysis capability. "give me the data and I'll analyze it".

— This scenario exists only to determine that audit needs to be able to be "queried" by PID, as well as success/fail event outcomes.

Issues:

— In the real world, there is a lot of automated pre-staging and caching of data. For most transactions, the provider or name of the subject of care is often not included in the data, but in related application information. Case in point: When an individual is scheduled for an appointment, their data are pre-fetched to the examination room screen. The audit service would need to be able to collate who was logged in to the examination room at the time that the examination was scheduled.

— For an unauthorized attempt to access healthcare records by a healthcare provider neighbour as above, the query should either be caught by the application or show up as a query from an unexpected source.

— The "watcher service" could have a whitelist of examination rooms that can pre-fetch data and send a notification if the query comes from an unexpected source and/or against a consent or access directive. The definition of when and what the watcher service notifies is a local policy issue.

A.4 Case of a compromised server

If the environment of the EHR registry server is compromised, the registry server can adversely affect the information assets of other organizations (springboard attack). Security measures in the server environment can be handled by using standard IT industry measures, for examples, audit logs such as firewall and router. These very measures are excluded from the audit log defined in this document but it is an important matter in server operation so it is necessary to obtain an appropriate audit log.

Required functionality: need to fit "architecturally" with what the regular IT industry does to handle this.

A.5 Case of a privileged user who abuses those privileges

An individual asks his/her partner to get a job as a registration agent for a new Drug Information System/Provider Registry and then register the individual and others as physicians with e-prescribing rights so that they can illegally prescribe pharmaceuticals.

Often, real-life suspicion or random analysis of audit logs are the only way to uncover this kind of event.

Required Functionality: List successful registration events by user

Optional functionality: Cross-reference between Audit service and other services to determine scope of breach

Potential functionality for ID Mgmt service: Verify Identities in provider registry against credential providers

A.6 Case of misdirected test results

A subject of care has been waiting for his/her lab results for two weeks now, when the physician told him/her that by using the new Lab Information System the results should be accessible in less than 48 h. When he/she calls his/her physician's office, the office has a record of the lab order but not the results. The nurse calls the lab and asks what happened to the test. The lab checks their audit logs and finds the received lab order number as well as the lab results that were sent in response. The lab tech checks where the results were sent and realizes that the results were sent to the wrong physician's office. The lab tech resends the results to the correct recipient and checks the ARR to make sure the results were properly re-sent (successful event outcome and correct recipient) and calls the nurse to ask if she/she received them. The nurse calls the data subject to let him/her know that the results have been received.

Required functionality: Show events and sender and recipient

Potential functionality: Results were sent to the wrong place because there was an error in provider registry and the incident uncovered a need to correct/update the provider registry.

A.7 Case of the wayward transactions

A hospital system administrator notices an unusual number of failed transactions. After checking many system diagnostics, the system administrator can determine that every few hours there is a huge slowdown in bandwidth but not why. The administrator checks the logs and realizes that Application B is sending two of every single lab order and, as a result, is overloading systems.

This is a system administration and performance measurement use case as is the compromised server scenario. The information that needs to be audited is very different from the privacy and security use cases.

General audit system can stay consistent across the board and use the same capabilities to send and store the logs. The information that will be logged and where they get logged will be determined by local configuration policy.

At first, this is a web service to ARR interface that says “return to me anything unusual”, for values of unusual such as “more than five consecutive failed logins or failed transaction outcomes”.

In the current world, this kind of audit is handled by making the raw data stream available to the administrator to analyse with the most basic of tools.

The system might not want to offer analytic details to the incoming audit stream but could make the raw audit stream available through an interface in case anyone else wanted to write an analysis for it.

This case could be expanded to include variables such as wireless monitoring using medical devices and remote monitoring by subjects of care.

A.8 Case of the disappearing audit records — Audit repository as target

Someone tries to cover their tracks. Consistent time is necessary in all services/systems in order to be able to notice data gaps because the easiest thing for an attacker to do is shut down a portion of auditing during an attack or illicit transaction. Selective audit shutdown is challenging, so there is usually a noticeable gap. A second feature of an audit-related attack is to attack the time server itself, so there is a need to audit the accuracy of the time server and client in order to uncover potential incidents.

Implementation note: Routers are a good point (close and connected) to serve as time servers in order to ensure that systems are all synchronized. An application could/should be on the lookout for “abnormal” gaps in audit traffic. “Normal” audit traffic should be defined locally.

As audit servers are a prime target, how do we audit whether an audit server is being attacked, and what, if any unusual behaviours should be monitored for and are these in or out of scope of the audit services(s).

Most systems use NTP, which generates audit records. Those can be saved in the audit repository and monitored.

NOTE 1 Audit servers by nature need to be hardened and protected

NOTE 2 Consider maintaining local copies of audit records.

Consistent time is a capability that is required and a dependency of the audit service. (It needs to be used and working, not just available.)

Requirement: The audit repository and associated services shall be secured, including access controls and audit controls.

A.9 Case of a hacker creating fake audit records

A sophisticated attacker plugs in a laptop that generates falsified audit records to conceal the fact that he/she has disabled the audit system of the machine that is under attack.

(Some local policies might choose to use digital signatures in order to detect masquerading of audit records.)

A.10 Case of a hacker sniffing audit records and uses them in a nefarious way

Audit records can also be vulnerable to traffic analysis or changes to remove critical info mid-stream.

Mitigation: Keep personal health information out of audit records. If that is impossible, audit records can be encrypted either by record or session/stream.

A.11 Case of a strange (authorized/unauthorized) configuration change

Someone acting as a system administrator installs an update to local system software. (Alternative: Malware attack/random attacker installs an http logger and captures all http traffic to detect system vulnerabilities.)

The audit process should capture: date, time, and location of update as well as a "description of the change", which includes software version numbers, file checksums, etc.

The audit repository (or configuration audit repository) should be occasionally examined to: confirm that authorized configuration updates took place when they were supposed to, and to detect unauthorized or unexpected configuration changes.

Another aspect of the audit log/service should record all configuration changes, updates, etc., including software installs, hardware installs, and configuration changes.

The audit system shall support remedial action as well as real-time analysis to detect an adverse event in progress.

It is desirable but more difficult to generalize this to hardware.

Annex B
(informative)

Audit log services

B.1 Services in diagram

The Service Oriented Architecture (SOA) audit class diagram (see Figure B.1) serves to illustrate the audit log services that are described in this annex.

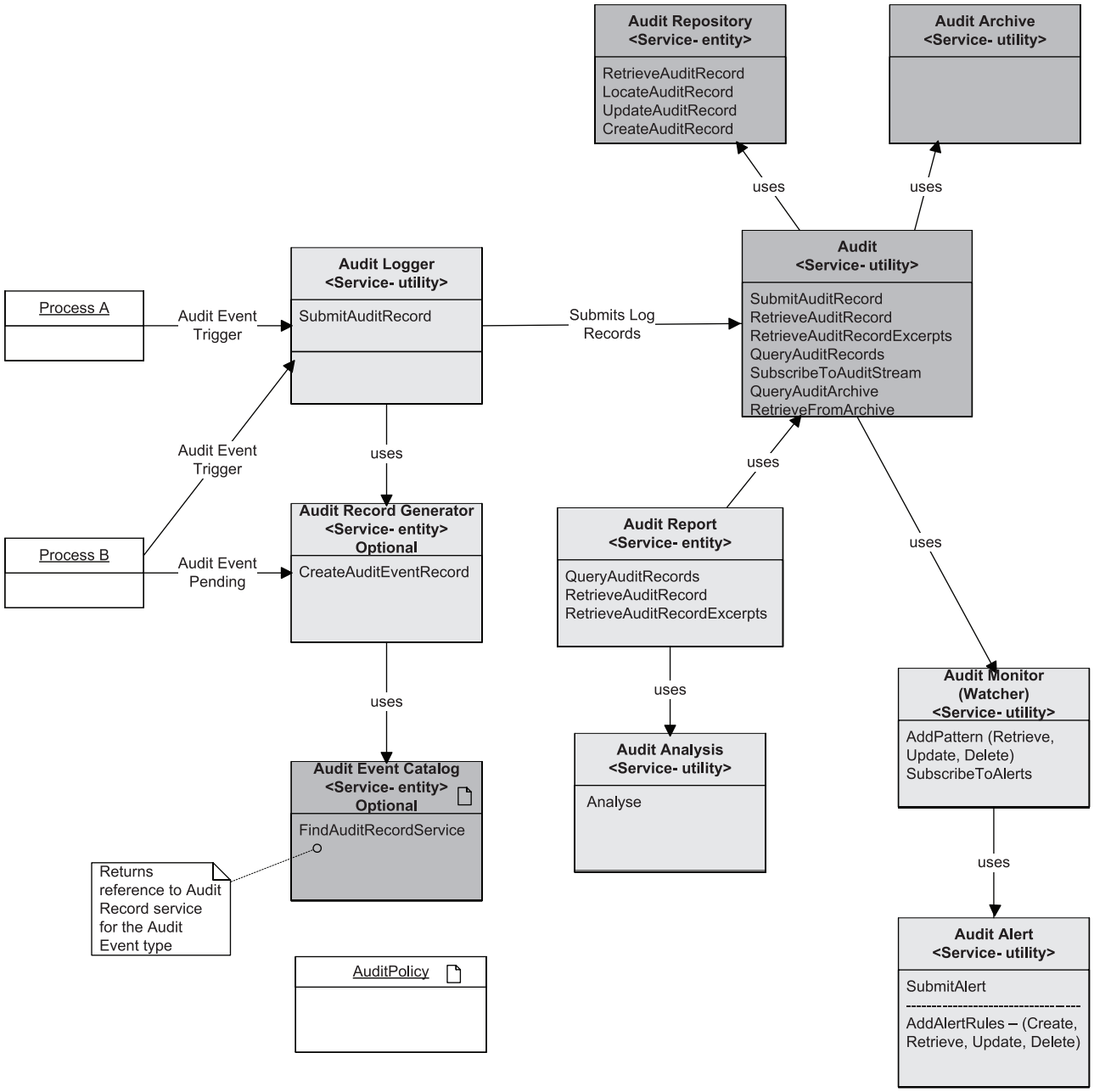

Figure B.1 — Audit class diagram

B.2 Audit Logger Service

Capability name: SubmitAuditEvent

Description: Submits an audit event to be handled.

Precondition

— Audit Event Record not null

— Audit Event Record complies with schema (record will not be rejected if it does not conform).

Inputs: **Audit Event Record (details to be determined)**

Outputs: **null**

Postconditions: Record is accepted

Exception Conditions

Error report if audit event cannot be recorded because:

— AuditEventRecord is null

— AuditEventRecord doesn't follow the agreed upon schema

— Service temporarily unavailable

— Service is unavailable (basic telecom provisioning problem)

Exceptions can be ignored by application but shall be implemented by audit service.

Relationship to levels of conformance

Miscellaneous notes: Assumptions:

System shall have consistent time

Repository will have a "fan-out" capability to send it to monitoring services, pagers, wherever the record should be sent depending on what the event is

Need ability to communicate expected Audit Event Record Schema

Both client and service systems shall have consistent time for reliable results

Other relevant content: At the detailed description, we will want to talk about reliable delivery, caching, monitoring, etc.

B.3 Audit Record Generator Service

Capability name: CreateAuditEventRecord (OPTIONAL)

Description: Creates a blank audit event record

Precondition: null

Inputs: **AuditEventType**

Outputs: **AuditEventRecord**

Postconditions: A blank audit event record template of the appropriate type has been created. If AuditEventType is null, a blank audit event that contains all the fields of every event type is returned. (e.g.: all of RFC 3881 , ISO 12052 (DICOM PS3.15) standards, plus whatever is defined in local policy as required auditable fields)

Exception Conditions: AuditEventType not recognized. If event type is not recognized, then capability will return warning, list of all recognized event types, plus full schema of all possible fields.

Relationship to levels of conformance: to be determined

Miscellaneous notes

The purpose of this capability is to add the capability to change the schema in one place and allow all applications to notice that the schema has changed and update the schema that they are using without having to change any code.

It also can communicate to the application what information is required to submit the audit event. This capability also gives you the flexibility to have more than one repository or to store both locally and remotely without the client needing to know anything.

AuditRecordGenerator can use the AuditEventCatalogue determine the proper schema for the event type being requested. This, along with the exception for inaccurate schema in the AuditLogger, will allow clients to detect when the local copy of the schema they have cached is out of date and permit schema revisions to be distributed to the clients without code changes.

Other relevant content

This is an optional service. Experienced implementers would cache the response on the client side to save time for schemas that have not changed.

B.4 Audit Event Catalogue Service

Capability Name: FindAuditEventService

Description: Returns the Audit Event Schema for the requested type. This service is not directly visible to the client, but is exposed for the use of the Audit Logger and AuditEventRecordGenerator services.

Precondition: null

Inputs: **AuditEventType**

Outputs: **AuditEventSchema**

Invariants

Postconditions

Exception Conditions: **AuditEventType is not a recognized type.**

Relationship to levels of conformance

Miscellaneous notes

This class provides the central location for AuditEvent Schema definition and should be used as the source of local copies of the schema for the client systems. Through the AuditRecordGenerator, the schemas can be propagated to the clients automatically.

Other relevant content

This is merely a background service. Indirectly accessible to the client through the previous service.

B.5 Audit Monitor Service

An alertName is defined as a pattern of events with a unique name; e.g.: “look for this data subject’s ID. “In real life, if there are worries about someone spying on a data subject, any accesses to that data subject’s info should generate an alert.

Capability Name: SubscribeToAlert

Description: Called by AuditAlert services to let the monitor service know that the AuditAlert service would like to be informed when there is a security alert.

Precondition: alertName is valid, i.e.: has an associated pattern that has been added.

Inputs

— alertName (note: Some alertNames may be predefined, but otherwise only add patterns)

— subscriberReference (format note: in SOAP it would be the end point address of the web service, in Java it is the address of the interface. The reference would need to be unique to avoid collisions.)

Outputs: **Null**

Invariants

Postconditions

— AuditAlert service that made the call is now known to the AuditMonitor

— Exception Conditions Invalid alertName

Miscellaneous notes

Assumption: Everyone has agreed on a pattern language.

In order to be able to "subscribe AND get the history of the last hour's events", the interface can call both this capability PLUS the queryauditrecords capability from the Audit Report Service.

Need to specify how to capture and use a parameter that allows the subscriber to specify an expiry date for the subscription.

Expiry of subscriptions: There is no date specified to the monitor service. If the client wants the subscription to expire, the alert/notification service implementation can handle scheduling of subscriptions. The monitor service should be light.

Capability Name: UnsubscribeFromAlerts

Description: Called by AuditAlert service to let the monitor service know that the AuditAlert service would no longer like to be informed of audit events.

Note that subscribing to the monitor service is not the same as subscribing to a notification service. A notification service is subscribed to by individuals at different times. A monitor service is subscribed to by a service like a notification service. It is a simpler service designed to do pattern-matching, not sophisticated alerting and notifying.

Precondition

Inputs

— alertName

— subscriberReference

Outputs: **Null**

Postconditions: Subscription is no longer registered.

Exception Conditions

Relationship to levels of conformance

Miscellaneous notes

Other relevant content: Send an audit event

Capability Name: AddPattern

Description: Allows the AuditAlert service to specify a new type of event pattern to look for, with specification of how to determine that alertable condition has occurred.

Precondition

— alertName is not null, and is unique

— eventPattern is not null and properly specified

Inputs: **alertName, eventPattern**

Outputs: **Null**

Postconditions: New Pattern is added to those the AlertMonitor knows about, associated with the name alertName

Exception Conditions

— alertName already exists

— alertName is null

— eventPattern not valid

Relationship to levels of conformance

Miscellaneous notes

Assumption: Everyone has agreed on a pattern language.

Assumption: Patterns are associated with creator somehow…

Policy for access to a particular instance could be: “this user/URL/etc can modify…”

Other relevant content: Send Audit event

Capability Name: RetrievePattern

Description: Allows the AuditAlert service to retrieve a pattern. If the alertName is not valid or NULL, it returns a list of all patterns.

Precondition

Inputs: **alertName**

Outputs: **Details of pattern, or list of all registered or available patterns.**

Postconditions: Pattern or list of patterns.

Exception Conditions: **None**

Miscellaneous notes

This in itself is an auditable event. It is up to local policies to determine if it is the service that sends the audit event, or the application that uses it. I.e.: This should be decided by the implementers.

Other relevant content: Optional: Send audit event

Capability Name: DeletePattern

Description: Deletes a pattern that is no longer applicable. If there are still listeners subscribed to the pattern and the forcedDelete parameter is present and true, then the Delete is a forced Delete. If the parameter is not present and true, and there are still listeners subscribed, then DeletePattern should fail and send an exception to the requestor..

Precondition: alertName is not null

Inputs

— alertName

— forcedDelete parameter

Outputs: **Null**

Postconditions

— Pattern and all subscribers to that pattern are deleted.

— I.e.: NULL output

Exception Conditions: **If there are subscribers to the alert and forcedDelete is not present and true, then send an exception to the delete requestor.**

Relationship to levels of conformance

Miscellaneous notes: Deletion of listeners should notify the originator and /or listeners.

Don't forget to "raise an event" that there are still subscribers. Other handling or listing of subscribers can be left up to implementation.

If available, DeletePattern should send a list of the remaining subscribers when the delete fails.

Other relevant content: Send audit event

B.6 Alert or Notification Service

Capability Name: SubmitNotification

Description: Submits an alert message to be handled.

Precondition

Inputs: **NotificationMessage**

Outputs: **Null**

Postconditions: AlertMessage delivered per applicable rules

Exception Conditions

— AlertMessage is null.

— AlertMessage processing error.

Relationship to levels of conformance

Miscellaneous notes

The actual method to notify the user (e.g. Pager or other medium) is implementation specific.

Other relevant content Send an audit event after submitting an alert

Name: SetNotificationRuleSet

Description: Create and maintain the rules used to determine how an AlertMessage is to be handled, i.e.: where it is to be sent.

Precondition: AlertRuleSet is not null.

AlertRuleSet format shall be recognized and processable by Service.

Inputs: **NotificationRuleSet**

Outputs: **Null**

Postconditions: New NotificationRuleSet has been set

Exception Conditions

— AlertRule null

— Unknown rule

Relationship to levels of conformance

Capability Name: RetrieveAlertRules

Description: Retrieves a copy of the alert rules currently in effect in this service.

Precondition: none

Inputs: **none**

Outputs: **AlertRules**

Invariants: AlertRules are not changed

Postconditions: AlertRules output contains the complete set of AlertRules in effect.

Exception Conditions: **none**

Relationship to levels of conformance

Miscellaneous notes

Other relevant content

B.7 Audit Report Service

Name: QueryAuditService

Description: Queries the Audit Service for records matching the pattern or query parameters requested in the query filter

Precondition: QueryFilter is not null. If all records are being requested, a * pattern (or equivalent in agreed upon query language) should be used.

Query Filter language should be agreed upon

Inputs: **QueryFilter**

Outputs: **List of unique id's for the requested records**

Postconditions: The record ids matching the query filter have been returned.

Exception Conditions

— QueryFilter is null

— QueryFilter can't be parsed

Relationship to levels of conformance

Miscellaneous notes

Other relevant content

Name: RetrieveAuditRecord

Description: Retrieves a specific audit record.

Precondition: RecordId is not null

Inputs: **RecordId**

Outputs: **The requested record, if it exists. Null otherwise.**

Postconditions: The record corresponding to the RecordId is returned

Exception Conditions: **RecordId is null**

Name: RetrieveAuditRecordExcerpt

Description: Retrieves the excerpt specified by the field descriptions from the record matching the record id

Precondition: record id is not null

field descriptions valid

Inputs

— RecordId

— FieldDescriptions

Outputs: **An Audit Record Excerpt matching the requested fields from the record that matches the id, if the id exists. Null otherwise**

Postconditions: The requested excerpt is returned

Exception Conditions

— RecordId is null

— Field descriptions not valid

Relationship to levels of conformance

B.8 Audit Analysis Service

Capability name: Analyse

Description: Performs a requested analysis

Precondition: Analysis request is a valid algorithm

Inputs: **AnalysisAlgorithm**

Outputs: **AnalysisReport**

Postconditions: AnalysisAlgorithm has been performed and the results returned.

Exception Conditions: **AnalysisAlgorithm is invalid**

Relationship to levels of conformance

Bibliography

[1] ISO 12052, *Health informatics — Digital imaging and communication in medicine (DICOM) including workflow and data management*

[2] ISO/TS 14265, *Health Informatics - Classification of purposes for processing personal health information*

[3] ISO 15489-1:2016, *Information and documentation — Records management — Part 1: Concepts and principles*

[4] ISO 21298, *Health informatics — Functional and structural roles*

[5] ISO/TS 21547, *Health informatics — Security requirements for archiving of electronic health records — Principles*

[6] ISO 22600 (all parts), *Health informatics — Privilege management and access control*

[7] ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1) — Part 1: Specification of basic notation*

[8] ISO/IEC 8824-2, *Information technology — Abstract Syntax Notation One (ASN.1) — Part 2: Information object specification*

[9] ISO/IEC 15408 (all parts), *Information technology — Security techniques - Evaluation criteria for IT security*

[10] ISO/TR 20514:2005, *Health informatics — Electronic health record — Definition, scope and context*

[11] ISO 16678:2014, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*

[12] IHE IT Infrastructure Technical Framework, Volume 1: Integration Profiles and Volume 2: Transactions

[13] IETF RFC 3881, *Security Audit & Access Accountability Message – XML Data Definitions for Healthcare Applications*

[14] ISO 19101-2:2018, *Geographic information — Reference model — Part 2: Imagery*

[15] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[16] ISO/IEC 2382:2015, *Information technology — Vocabulary*

[17] IEC 60050-713:1998, *International Electrotechnical Vocabulary (IEV) - Part 713: Radiocommunications: transmitters, receivers, networks and operation*

[18] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

[19] ISO 13940, *Health informatics — System of concepts to support continuity of care*

[20] ISO/HL7 10781, Health Informatics — HL7 Electronic Health Records-System Functional Model, Release 2 (EHR FM)

[21] HL7®international, HL7 Version 2 Product Suite

[22] IETF RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*

[23] IETF RFC 2396, *Uniform Resource Identifiers (URI): Generic Syntax*

[24] IETF RFC 4810, *Long-Term Archive Service Requirements*

[25] IETF RFC 4998, *Evidence Record Syntax (ERS)*

[26] ISO/TS 17975:2015, *Health informatics — Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information*

ICS 35.240.80

Price based on 46 pages