INTERNATIONAL STANDARD

ISO 27789

First edition
2013-03-01

Health informatics — Audit trails for electronic health records

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

Reference number
ISO 27789:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 27789 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

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 if the privacy of subjects of care is to be maintained. In order to protect the consistency of health information, it is also important that its entire life cycle be fully auditable. Health records should be created, processed and managed in ways that guarantee the integrity and confidentiality of their contents and that support legitimate control by subjects of care in how the records are created, used and maintained.

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

Effective audit and logging can help to uncover misuse of EHR systems or EHR data and can help organizations 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 compliance with organizational access policy and can contribute to improving and refining the policy itself. But as such a policy has 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 International Standard 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 may reside in many different information systems within and across organizational 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 International Standard 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 International Standard

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, and

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

This International Standard 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 Comparision with related standards on electronic health record audit trails

This International Standard conforms to the requirements of ISO 27799:2008, insofar as they relate to auditing and audit trails.

Some readers may be familiar with Internet Engineering Task Force (IETF) Request for Comment (RFC) 3881.[13] (Readers not already familiar with IETF RFC 3881 need not refer to that document, as familiarity with it is not required to understand this International Standard.) Informational RFC 3881, dated 2004-09 and no longer listed as active in the IETF database, was an early and useful attempt at specifying the content of audit logs for healthcare. To the extent possible, this International Standard builds upon, and is consistent with, the work begun in RFC 3881 with respect to access to the EHR.

0.4 A note on terminology

Several closely related terms are defined in Clause 3. An *audit log* is a chronological sequence of *audit records*; each audit record contains evidence of directly pertaining to and resulting from the execution of a process or system function. As EHR systems can be complex aggregations of systems and databases, there may be more than one audit log containing information on system events that have altered a subject of care's EHR. Although the terms *audit trail* and *audit log* are often used interchangeably, in this International Standard the term *audit trail* refers to the collection of all audit records from one or more audit logs that refer to a specific subject of care or specific electronic health record or specific user. An *audit system* provides all the information processing functions necessary to maintain one or more audit logs.

Health informatics — Audit trails for electronic health records

1 Scope

This International Standard 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 which, complying with ISO 27799, create a secure audit record each time a user accesses, 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, access, update, etc.), and record the date and time at which the function was performed.

This International Standard 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 15408-2.[9]

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

2 Normative references

The following referenced documents are indispensable for the application 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 8601:2004, *Data elements and interchange formats — Information interchange — Representation of dates and times*

ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

[ISO/IEC 27000:2012, definition 2.1]

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

3.3
accountability
principle that individuals, organizations and the community are responsible for their actions and may be required to explain them to others

[ISO 15489-1:2001, definition 3.2]

3.4
audit
systematic and independent examination of accesses, additions or alterations to electronic health records to determine whether the activities were conducted, and the data were collected, used, retained or disclosed according to organizational standard operating procedures, policies, good clinical practice, and applicable regulatory requirement(s)

3.5
audit archive
archival collection of one or more audit logs

3.6
audit data
data obtained from one or more audit records

3.7
audit log
chronological sequence of audit records, each of which contains data about a specific event

3.8
audit record
record of a single specific event in the life cycle of an electronic health record

3.9
audit system
information processing system that maintains one or more audit logs

3.10
audit trail
collection of audit records from one or more audit logs relating to a specific subject of care or a specific electronic health record

3.11
authentication
provision of assurance that a claimed characteristic of an entity is correct

[ISO/IEC 27000:2012, definition 2.8]

3.12
authorization
granting of privileges, which includes the granting of privileges to access data and functions

Note 1 to entry: Derived from ISO 7498-2: the granting of rights, which includes the granting of access based on access rights.

3.13
authority
entity responsible for issuing certificates

3.14
availability
property of being accessible and useable upon demand by an authorized entity

[ISO/IEC 27000:2012, definition 2.10]

3.15
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO/IEC 27000:2012, definition 2.13]

3.16
Coordinated Universal Time
UTC
time scale which forms the basis of a coordinated radio dissemination of standard frequencies and time signals; it corresponds exactly in rate with international atomic time, but differs from it by an integral number of seconds

[IEC 60050-713:1998]

3.17
data integrity
property that data have not been altered or destroyed in an unauthorized manner

[ISO 7498-2:1989, definition 3.3.21]

3.18
electronic health record
EHR
comprehensive, structured set of clinical, demographic, environmental, social and financial data in electronic form, documenting the health care given to a single individual

[ASTM E1769:1995]

3.19
EHR segment
part of an EHR that constitutes a distinct resource for the access policy

3.20
identification
performance of tests to enable a data processing system to recognize entities

[ISO/IEC 2382-8:1998, definition 08.04.12 (as identitiy authentication, identity validation)]

3.21
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

3.22
information security
preservation of confidentiality, integrity and availability of information

[ISO/IEC 27000:2012, definition 2.30]

3.23
integrity
property of protecting the accuracy and completeness of assets

[ISO/IEC 27000:2012, definition 2.36]

3.24
object identifier
OID
globally unique identifier for an information object

Note 1 to entry: The object identifiers used in this International Standard refer to code systems. These code systems may 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.

3.25
policy
set of legal, political, organizational, functional and technical obligations for communication and cooperation

[ISO/TS 22600]

3.26
privilege
capacity assigned to an entity by an authority

3.27
records management
field of management responsible for the efficient and systematic control of the 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

[ISO 15489-1, definition 3.16]

3.28
role
set of competences and/or performances associated with a task

3.29
sensitivity
measure of the potential or perceived potential to create harm to a data subject, or to be abused, or misused

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

[ISO/IEC 2382-8:1998, definition 08.01.06]

3.31
subject of care
person scheduled to receive, receiving or having received a health service

[ISO 18308:2011, definition 3.47]

3.32
user
person, device or program that uses an EHR system for data processing or health information exchange

4 Symbols and abbreviated terms

EHR	Electronic Health Record
HL7	Health Level Seven International
OID	Object Identifier
UTC	Coordinated Universal Time

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 health care and in many jurisdictions these requirements are set down in law.

Secure audit trails of access to electronic health records may support compliance 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

An organization responsible for maintaining an audit log shall identify the access policy governing all accesses logged.

The access policy shall be in accordance with ISO 27799:2008, 7.8.1.2, Access control policy.

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/TS 22600.[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 27799:2008, 7.8.2.2, Privilege management.

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

5.1.5 Secure audit records

Secure audit records shall be created each time personal health information is accessed, created, updated or archived, in accordance with ISO 27799:2008, 7.7.10.2, Audit logging. 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 compliance with the organization's policy and to evaluate its effectiveness.

This implies

— detecting unauthorized access to health records,

— evaluating emergency access,

— detecting abuse of privileges,

and support for:

— documenting access across domains, and

— evaluation of access policies.

NOTE Full assessment of compliance with the organization's policy can require additional data which are 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 subects 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 compliance 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 Healthcare provider's ethical or legal proof of action

The audit trails shall provide data to provide to care providers documented evidence of what information was viewed and which actions were taken (create, look-up, read, correct, update, extract, output, archive, etc.) in relation to the information when and by whom.

Retention of the audit records should be aligned with the legal terms of accountability within the jurisdiction.

Refer to HL7 EHR Records Management and Evidentiary Support (RM-ES).

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. The scope of this International Standard being limited to access to personal health information, only trigger events relating to accesss are specified here.

In order to generate the audit records which satisfy the requirement derived from Clause 5 (Requirements and uses of audit data), i.e. "when", "who", "whose", the following two events are mandatory:

a) Access events to personal health information,

b) Query events about personal health information.

Examples of out-of-scope events are:

— start-and-stop events of the application program;

— authentication events involving authentication of users;

— input and output events from/to the external environment;

— access events to information other than personal health information;

— security alert events related to the application programs;

— access events to the audit log preserved in the application programs;

— events generated by the operating system, middleware and so on;

— access events generated by using system utilities;

— physical connection/disconnection events of equipments to the network;

— start/stop events of the protection systems such as anti-virus protection systems;

— 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 International Standard, the access to the personal health information is regarded as the 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. See Table 1.

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”. See Table 2.

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 DICOM,[11] 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	Refer to 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	Refer to 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	Refer to 7.4
	NetworkAccessPointID	U	ID for network access point	
Audit system related (1)	AuditEnterpriseSiteID	U	Site ID of audit enterprise	Refer to 7.5
	AuditSourceID	M	Unique ID of audit source	
	AuditSourceTypeCode	U	Type code of audit source	

Table 3 *(continued)*

Type	Field name	Option	Description	Additional info.
Participant object related (0..N)	ParticipantObjectTypeCode	M	Code for the participant object type	Refer to 7.6
	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	
	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	
Multiplicity:		**Optionality:**		
(1)		M	Mandatory	
(0..1)	0 or 1 exists,	MC	Conditional Mandatory	
(1..2)	1 or 2 exist(s)	U	Optional	
(0..N)	0 to N exist(s)	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,[1] DICOM supplement 95[11].

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/View/Print/Query	Display or print data, such as a diagnosis
U	Update	Update data, such as Revise Personal Health Information
D	Delete	Make items unaccessible
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 themselves. Auditing need not always make as fine a distinction.

NOTE 3 Compound actions, such as "Move," "Archive" or "Copy", would be audited 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 in ISO 8601:2004 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 [RFC1305] 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 International Standard.

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 RFC3881 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 may be categorized in more than one way, there may 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 may 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 to be used for clinical audit, or to provide evidence, where needed, of misuse, the audit trail might 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-output 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 27799:2008, 7.8.2.2 (Privilege management), and ISO/TS 22600[6] specify that the 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/TS 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/TS 22600[6] and ISO/TS 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 (Informative)
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 compliance 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 personal accountability. Internet IP addresses, in particular, are highly volatile and can be assigned to 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

— 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: Conditional mandatory

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
7	ISO level 1-3 network component
8	ISO level 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 may 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 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 common data architecture documents), a set of related participant objects identified by accession number or study number, may be identified. Note, though, that 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.

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

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
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

Description: Identifier for the data life-cycle stage for the participant object. This can be used to provide an audit trail for data, over time, as it passes through the system.

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

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
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 [RFC2396] 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 version 2.4 Table 207 or ISO 12052[1] (DICOM)[1] defined media types.

For implementation-defined codes or references to standards, the XML schema in RFC3881 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 may 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 Consider this to 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*:* Optional

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

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.

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.
	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 is 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.
Occurrence source system related (1)	AuditEnterpriseSiteID	U	The logical location of the occurrence source system. Used to modify AuditSourceID.
	AuditSourceID	M	The unique ID of the occurrence source system.
	AuditSourceTypeCode	U	The type code of the occurrence source system.

Table 18 *(continued)*

Category	Field Name	Option	Restriction of values
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 value is set. EV 1 (patient)
	ParticipantObjectDataLifeCycle	U	The lifecycle stage ID of the participant object.
	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.
	ParticipantObjectDetail	U	The detail of the participant object instance.
Participant object related (information of accessed EHR segment) (1..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 value 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.

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.
	EventActionCode	M	The action executed in the event which 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 is 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 which responds to the query. This is a unique value at the audit source (AuditSourceID).
	AlternateUserID	U	The alternative ID of the process which responds to the query.
	UserName	U	The name of the process which 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
Occurrence source system related (1)	AuditEnterpriseSiteID	U	The logical location of the occurrence source system. Used to modify AuditSourceID.
	AuditSourceID	M	The unique ID of the occurrence source system.
	AuditSourceTypeCode	U	The type code of the occurrence 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 value is set. EV 3 (report)
	ParticipantObjectDataLifeCycle	U	The life cycle 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 which is coded by base 64. These contents shall be analysed by the developer vendor.
	ParticipantObjectDetail	U	The detail of the participant object instance.

9 Secure management of audit data

9.1 Security considerations

In relation to the maintenance of confidentiality and integrity of health records and the integrity and availability of health information systems, the following criteria are stated in IETF RFC 3881:

> *Audit data shall be secured at least to the same extent as the underlying data and activities being audited. This includes access controls as well as data integrity and recovery functions. This document acknowledges the need for, but does not specify, the policies and technical methods to accomplish this.*
>
> *It is conceivable that audit data might have unintended uses, e.g. tracking the frequency and nature of system use for productivity measures. ASTM standard E2147-01[10] states, in paragraph 5.3.10, "Prohibit use for other reasons than to enforce security and to detect security breaches in record health information systems, for example, the audits are not to be used to explore activity profiles or movement profiles of employees."*

Management of audit records should follow the International Standard on records management ISO 15489-1.[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 the documents IETF RFC 4810 and IETF RFC 4998.

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 should be maintained over the logical 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 document all instances when the audit trail has been out of service, turned off or not functional by a system failure.

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

9.3 Retention requirements

An organization responsible for maintaining an audit log shall define the retention policy governing the audit records.

Retention of the audit records should follow legal requirements and relevant 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) document all occasions when the audit trail has been out of service, turned off or by a system failure, and

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

9.5 Access to audit data

Access to audit data needs to 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 may 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 the use of audit logs.

A.2 Case of the disgruntled celebrity

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 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 discovered 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 (including queuing and local storage?) 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.

  — compliance with RFC 3881, to make searching possible

  — where radiology workflow is being audited, compliance with ISO 12052[1] (DICOM).

The above-mentioned scenario brings up 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 may 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. We want to record a "code" for this violation, but not clearly identify in plain text in the audit record.

On the audit side, we could standardize:

— Categories of security alert – need a mechanism to send a security alert. We would have 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

— We can have a 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 a minimum provide the ability to dump all data from the audit database so you can do 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, as follows:

High-profile subjects of care where the attacker is *not* highly motivated

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

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 (to a reporting service?) 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 has to 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: do not 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[1] (DICOM) queries, laboratory 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 – are there any unusual queries?

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

In this scenario, a subject of care does not want her next door neighbour, a healthcare provider, to be aware of her health status, the data subject may issue a consent directive to her primary care physician to block all access from the healthcare provider neighbour to her healthcare record. If 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 the fact 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 analyse 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 as above by healthcare provider neighbour, either should be caught by application or show up as queries 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

A new public health registry just went live and whoever built the server neglected to change the administrator password. A random hacker finds the server and starts using it to bombard other systems with spam from the public health registry. An unusually high volume of audit events as well as administrator accesses from an unknown IP address causes a trigger to be sent to the security officer who quickly checks the audit logs and realizes what is going on and is able to put a stop to it. Further analysis of the audit logs shows some additional vulnerabilities that were not apparent when the system was installed, and additional hardening is done to improve the security of the system.

This is a different type of application service and also a different type of audit.

Firewalls would be generating these audit records. Router logs are not healthcare specific.

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

The fact that an alert was sent is audited as well.

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.

How can we respond to this in a timely way? Can Audit and monitoring help detect unusual prescribing of controlled pharmaceuticals? (sudden jump in morphine prescriptions?) The least the system can help with is that once the privilege-abusing user is discovered, providing evidence of unauthorized registrations as well as a list of all "physicians" registered by the privilege-abusing user's account.

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 her laboratory results for two weeks now, when the physician told her that by using the new Lab Information System the results should be accessible in less than 48 h. When she calls her physician's office, the office has a record of the lab. order, but not the results. The nurse calls the laboratory 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 laboratory technician checks where the results were sent and realizes that the results were sent to the wrong physician's office. The laboratory technician resends the results to the correct recipient and just to be sure, 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 got them. The nurse calls the data subject to let her know that the results are in.

Some additional details would need to be added to audit logs in order to support this scenario such as: tracking order numbers, report numbers, etc. A balance would need to be set between adding too much detail to logs and an analysis that can correlate orders with queries in the audit log. The question to answer is: should this be done in workflow management or with the audit log? The radiology world does this with workflow management, bi-directionally. (Confirmation of reports being sent, received AND read, as well as container numbers, etc.) . Reporting workflows could be handled by a separate audit – lab. reporting and confirmation DB. An interface could allow for the capability of matching laboratory reporting logs with other audit logs during investigations. For example: a log correlation service.

There could be a workflow reporting and audit service as part of the information system be it laboratories or prescribing or radiology. Integration with logistics should also be taken into consideration. (shipping, etc.)

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 – how can this need for remedial action be automatically triggered and resolved?

This scenario differs in that it is neither a real-time monitoring nor administration, but a use of the audit system to verify workflow.

There is a non-administrative user in this scenario who may be using an interface to the audit repository that needs to be user-friendly and different from the usual interface.

Questions to answer in this scenario:

— Can the system detect if a message gets lost?

— Can the system detect if a transaction occurred? Since transactions are auditable events, this information should be captured.

— Is there a way to analyse the existence or absence of success or failure messages?

— When an error message happens (response failed), this can tie in to the monitoring service; i.e.: if the system can detect it, report the loss

— Picking up a mismatch between a notification sent and a notification delivered is a matching/analysis function that is out of scope of an audit standard.

A security person would also want to see: if the corrcct person did not get the laboratory message at the right time, did anyone else get messages at this time?

This is partly a workflow/reporting/performance scenario. The audit service may want to expose a capability to the workflow service.

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 laboratory order and, as a result, overloading systems.

This is a system administration and performance measurement use case, like 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 may 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 (was it reset more than usual?) 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 we be monitoring for and are these in or out of scope of the audit services(s).

NOTE 1 Most systems use NTP which generates audit records; those should be saved in the audit repository and monitored.

NOTE 2 Audit servers by nature need to be hardened and protected

NOTE 3 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 has disabled the audit system of the machine that is under attack.

(Some local policies may 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 may 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 may 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. (Alternate: 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.

A.12 Case of a user trying to brute-force a password

The audit server receives reports of a number of login failures and should raise/trigger an alarm quickly.

Annex B
(informative)

Audit log services

B.1 Services in diagram

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

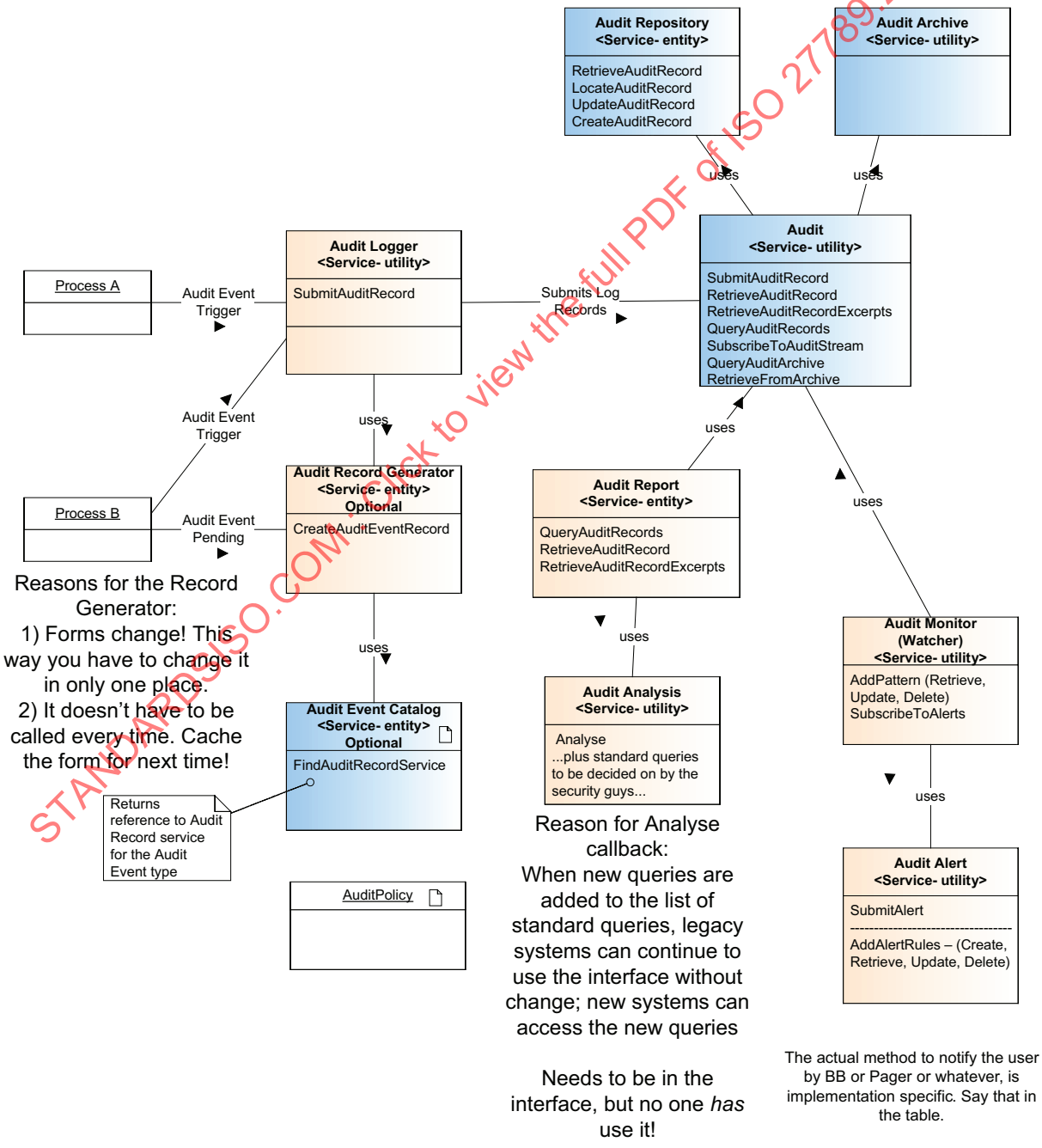

Figure B.1 — Audit class diagram