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