FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/FDIS
27789**

ISO/TC **215**

Secretariat: ANSI

Voting begins on:
2021-05-19

Voting terminates on:
2021-07-14

Health informatics — Audit trails for electronic health records

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

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/FDIS 27789:2021(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

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

The main changes compared to the previous edition are as follows:

— harmonization between audit record format and DICOM format;

— review of the content in Annex A;

— review of the chart in Annex B;

— bibliography update.

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

Introduction

0.1 General

Personal health information is regarded by many as among the most confidential of all types of personal information and protecting its confidentiality is essential to maintain the privacy of subjects of care. In order to protect the consistency of health information, it is also important that its entire life cycle be fully auditable. Health records should be created, processed and managed in ways that guarantee the integrity and confidentiality of their contents and that support legitimate control by subjects of care in how the records are created, used and maintained.

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

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

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

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

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

0.2 Benefits of using this document

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

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

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

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

0.3 Related standards on electronic health record audit trails

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

Health informatics — Audit trails for electronic health records

1 Scope

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

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

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

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

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

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

2 Normative references

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

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

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

ISO/TS 21089:2018, *Health informatics - Trusted End-to-End Information Flows*

3 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.7
audit archive
archival collection of one or more audit logs

3.8
audit data
data obtained from one or more audit records

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

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

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

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

[SOURCE: GCST]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.21
identification
process of recognizing the attributes that identify the object

[SOURCE: ISO 16678:2014, 2.1.7]

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

[SOURCE: ISO 2382:2015, 2121623]

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

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

3.24
integrity
property of accuracy and completeness

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

3.25
object identifier
OID
globally unique identifier for an information object

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

3.26
policy
set of rules related to a particular purpose

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

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

3.27
privilege
capacity assigned to an entity by an authority

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

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

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

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

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

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

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

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

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

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

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

[SOURCE: COACH; OMG]

4 Abbreviated terms

HL7 ® Health Level Seven

5 Requirements and uses of audit data

5.1 Ethical and formal requirements

5.1.1 General

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

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

5.1.2 Access policy

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

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

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

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

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

5.1.3 Unambiguous identification of information system users

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

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

5.1.4 User roles

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

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

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

5.1.5 Secure audit records

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

5.2 Uses of audit data

5.2.1 Governance and supervision

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

This implies

— detecting unauthorized access to health records,

— evaluating emergency access, and

— detecting abuse of privileges.

and support for:

— documenting access across domains, and

— evaluation of access policies.

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

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

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

5.2.2 Subjects of care exercising their rights

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

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

— assessing accountability for the content of the record,

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

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

5.2.3 Evidence and retention requirements

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

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

The following documents provides guidance and further information:

— ISO/TS 21089;

— ISO/HL7 10781. [20]

6 Trigger events

6.1 General

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

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

— Access events to personal health information;

— Query events about personal health information.

Examples of out-of-scope events are:

a) Start and stop events of the application program;

b) Authentication events involving authentication of users;

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

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

e) Security alert events related to the application programs;

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

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

h) Access events generated by using system utilities;