
Zdravstvena informatika - Revizijske sledi za elektronske zdravstvene zapise (ISO 27789:2013)

Health informatics - Audit trails for electronic health records (ISO 27789:2013)

Medizinische Informatik - Audit Trails für elektronische Gesundheitsakten (ISO 27789:2013)

iTeh STANDARD PREVIEW

Informatique de santé - Historique d'expertise des dossiers de santé informatisés (ISO 27789:2013)

(standards.itteh.ai)

SIST EN ISO 27789:2013

Ta slovenski standard je istoveten z: EN ISO 27789:2013<http://standards.itteh.ai/catalog/standards/sist/en-iso-27789-2013/495-9b54-f8db12cfb78d/sist-en-iso-27789-2013>**ICS:**

35.240.80

Uporabniške rešitve IT v
zdravstveni tehnikiIT applications in health care
technology**SIST EN ISO 27789:2013****en**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 27789:2013

<https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013>

EUROPEAN STANDARD

EN ISO 27789

NORME EUROPÉENNE

EUROPÄISCHE NORM

March 2013

ICS 35.240.80

English Version

Health informatics - Audit trails for electronic health records (ISO 27789:2013)

Informatique de santé - Historique d'expertise des dossiers de santé informatisés (ISO 27789:2013)

Medizinische Informatik - Audit-Trails für elektronische Gesundheitsakten (ISO 27789:2013)

This European Standard was approved by CEN on 16 February 2013.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

[SIST EN ISO 27789:2013](https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013)

<https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013>



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents	Page
Foreword.....	3

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO 27789:2013](https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013)
<https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013>

Foreword

This document (EN ISO 27789:2013) has been prepared by Technical Committee ISO/TC 215 "Health informatics" in collaboration with Technical Committee CEN/TC 251 "Health informatics" the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2013, and conflicting national standards shall be withdrawn at the latest by September 2013.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

iTeh STANDARD PREVIEW
Endorsement notice
(standards.iteh.ai)

The text of ISO 27789:2013 has been approved by CEN as EN ISO 27789:2013 without any modification.

SIST EN ISO 27789:2013
<https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 27789:2013

<https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013>

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*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO 27789:2013](https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013)

[https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-
f8db12cfb78d/sist-en-iso-27789-2013](https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013)



Reference number
ISO 27789:2013(E)

© ISO 2013

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 27789:2013

<https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	4
5 Requirements and uses of audit data	5
5.1 Ethical and formal requirements.....	5
5.2 Uses of audit data.....	6
6 Trigger events	7
6.1 General.....	7
6.2 Details of the event types and their contents.....	7
7 Audit record details	8
7.1 The general record format.....	8
7.2 Trigger event identification.....	9
7.3 User identification.....	11
7.4 Access point identification.....	14
7.5 Audit source identification.....	15
7.6 Participant object identification.....	17
8 Audit records for individual events	23
8.1 Access events.....	23
8.2 Query events.....	24
9 Secure management of audit data	26
9.1 Security considerations.....	26
9.2 Securing the availability of the audit system.....	27
9.3 Retention requirements.....	27
9.4 Securing the confidentiality and integrity of audit trails.....	27
9.5 Access to audit data.....	27
Annex A (informative) Audit scenarios	28
Annex B (informative) Audit log services	35
Bibliography	44

ISO 27789:2013(E)**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*.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO 27789:2013](https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013)

<https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013>

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 Comparison with related standards on electronic health record audit trails

ISO 27789:2013(E)

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.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST EN ISO 27789:2013](#)

<https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-f8db12cfb78d/sist-en-iso-27789-2013>

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

ISO 27789:2013(E)**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]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 27789:2013

[https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-](https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-8e5d2efb78d/sist-en-iso-27789-2013)

[8e5d2efb78d/sist-en-iso-27789-2013](https://standards.iteh.ai/catalog/standards/sist/d30fa8c2-bf39-4c05-9b54-8e5d2efb78d/sist-en-iso-27789-2013)

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 identity 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]