

SVENSK STANDARD

SS-EN ISO 27789:2013



Fastställt/Approved: 2013-03-14
Publicerad/Published: 2013-03-15
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 35.240.80

Hälsoinformatik – Spårbarhet vid revision av elektronisk patientjournal (ISO 27789:2013)

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

This preview is downloaded from www.sis.se. Buy the entire standard via <https://www.sis.se/std-89442>

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka

Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet

Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standardpaket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete

Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.



Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence

As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work

We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception

With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00



Europastandarden EN ISO 27789:2013 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av EN ISO 27789:2013.

The European Standard EN ISO 27789:2013 has the status of a Swedish Standard. This document contains the official version of EN ISO 27789:2013.

© Copyright/Upphovsrätten till denna produkt tillhör SIS, Swedish Standards Institute, Stockholm, Sverige. Användningen av denna produkt regleras av slutanvändarlicensen som återfinns i denna produkt, se standardens sista sidor.

© Copyright SIS, Swedish Standards Institute, Stockholm, Sweden. All rights reserved. The use of this product is governed by the end-user licence for this product. You will find the licence in the end of this document.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

Denna standard är framtagen av kommittén för Hälso- och sjukvårdsinformatik, SIS/TK 334.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

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.



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

Management Centre: Avenue Marnix 17, B-1000 Brussels

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

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.

Endorsement notice

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

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

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