SLOVENSKI STANDARD
oSIST prEN ISO 27789:2011

01-marec-2011

Zdravstvena informatika - Revizijske sledi za elektronske zapise v zdravstvenem varstvu (ISO/DIS 27789:2010)

Health informatics - Audit trails for electronic health records (ISO/DIS 27789:2010)

Medizinische Informatik - Audit Trails für elektronische Gesundheitsakten (ISO/DIS 27789:2010)

Informatique de santé - Historique d'expertise des dossiers de santé informatisés (ISO/DIS 27789:2010)

Ta slovenski standard je istoveten z: **prEN ISO 27789**

ICS:

35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

oSIST prEN ISO 27789:2011 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN ISO 27789

December 2010

ICS 35.240.80

English Version

Health informatics - Audit trails for electronic health records (ISO/DIS 27789:2010)

Informatique de santé - Historique d'expertise des dossiers de santé informatisés (ISO/DIS 27789:2010)

Medizinische Informatik - Audit Trails für elektronische Gesundheitsakten (ISO/DIS 27789:2010)

This draft European Standard is submitted to CEN members for parallel enquiry. It has been drawn up by the Technical Committee CEN/TC 251.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (prEN ISO 27789:2010) 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 document is currently submitted to the parallel Enquiry.

Endorsement notice

The text of ISO/DIS 27789:2010 has been approved by CEN as a prEN ISO 27789:2010 without any modification.

DRAFT INTERNATIONAL STANDARD ISO/DIS 27789

ISO/TC **215**

Secretariat: **ANSI**

Voting begins on:
2010-12-09

Voting terminates on:
2011-05-09

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Health informatics — Audit trails for electronic health records

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

ICS 35.240.80

ISO/CEN PARALLEL PROCESSING

This draft has been developed within the International Organization for Standardization (ISO), and processed under the **ISO-lead** mode of collaboration as defined in the Vienna Agreement.

This draft is hereby submitted to the ISO member bodies and to the CEN member bodies for a parallel five-month enquiry.

Should this draft be accepted, a final draft, established on the basis of comments received, will be submitted to a parallel two-month approval vote in ISO and formal vote in CEN.

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

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*, Subcommittee SC , .

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

Introduction

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 organisations and subjects of care obtain redress against users abusing their access privileges. For auditing to be effective, audit trails must 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 must anticipate the occurrence of unforeseen or emergency cases, analysis of the audit logs will for those cases become the primary means of ensuring access control.

This 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 will contain 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 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 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.

Benefits of using this standard

Standardisation of audit trails on access to electronic health records will achieve 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.

Who should read this standard?

This 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.

Comparision with related standards on electronic health record audit trails

This standard conforms to the requirements of ISO 27799:2008, *Health informatics — Security management in health using ISO/IEC 27002,* 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 *Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications* [1]. (Readers not already familiar with IETF RFC 3881 need not refer to that document, as familiarity with it is not required to understand this ISO 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 ISO standard builds upon, and is consistent with, the work begun in RFC 3881 with respect to access to the EHR.

A Note on Terminology

Several closely related terms are defined in section 3 (Terms and definitions). 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 standard the term *audit trail* will refer 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

Electronic health records for subjects of care may reside in many different information systems within and across organisational or jurisdictional boundaries. To keep track of all actions that involve records on a particular subject of care, a common framework is a prerequisite.

Audit trails for electronic health records that are distributed across different systems need a common framework to keep the complete set of personal health information auditable. This document specifies this common framework in terms of audit trigger events and audit data.

ISO 27799 requires information systems containing personal health information to create a secure audit record each time a user accesses, creates, updates, or archives personal health information via the system. This audit record will at 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.

The scope of this standard is restricted to actions performed on electronic health records. These actions are governed by the access policy for the domain where the electronic health record resides. Audit trails for electronic health records can help ascertain compliance with the access policy.

The audit trails specified by this standard will not contain any personal health information from the electronic health record, other than identifiers. The audit record will only contain links to EHR segments as defined by the governing access policy.

Specification and use of audit logs for system management and system security purposes, such as the detection of performance problems, application flaws, or support for a reconstruction of data, are outside the scope of this document.These are already covered by general computer security standards such as ISO/IEC 15408 [6] .

Examples will be given of services for secure audit log management.

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 27799:2008, *Health informatics — 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
ensuring that the resources of a data processing system can only be accessed through authorized channels by authorized entities