This document is a preview generated by EVS

Health informatics - Security management in health using ISO/IEC 17799

Health informatics - Security management in health using ISO/IEC 17799

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN ISO 27799:2008 sisaldab Euroopa standardi EN ISO 27799:2008 ingliskeelset teksti.	This Estonian standard EVS-EN ISO 27799:2008 consists of the English text of the European standard EN ISO 27799:2008.
Standard on kinnitatud Eesti Standardikeskuse 18.08.2008 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.	This standard is ratified with the order of Estonian Centre for Standardisation dated 18.08.2008 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.
Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 01.07.2008.	Date of Availability of the European standard text 01.07.2008.
Standard on kättesaadav Eesti standardiorganisatsioonist.	The standard is available from Estonian standardisation organisation.

This document is a preview generated by EVS

ICS 35.240.80

Võtmesõnad:

Standardite reprodutseerimis- ja levitamisõigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel on keelatud ilma Eesti Standardikeskuse poolt antud kirjaliku loata.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:
Aru 10 Tallinn 10317 Eesti; www.evs.ee; Telefon: 605 5050; E-post: info@evs.ee

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 27799

July 2008

ICS 35.240.80

English Version

Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2008)

Informatique de santé - Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002 (ISO 27799:2008)

Medizinische Informatik - Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO 27799:2008)

This European Standard was approved by CEN on 15 June 2008.

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 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 Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, 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.

This document is a preview generated by EVS

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

Management Centre: rue de Stassart, 36 B-1050 Brussels

© 2008 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN ISO 27799:2008: E

This document is a preview generated by EVS

Foreword

This document (EN ISO 27799:2008) 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 January 2009, and conflicting national standards shall be withdrawn at the latest by January 2009.

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, 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 the United Kingdom.

Endorsement notice

The text of ISO 27799:2008 has been approved by CEN as a EN ISO 27799:2008 without any modification.

This document is a preview generated by EVS

Contents

Page

© ISO 2008 – All rights reserved

This document is preview generated by EVS

Introduction

This International Standard provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information by implementing ISO/IEC 27002[1)]. Specifically, this International Standard addresses the special information security management needs of the health sector and its unique operating environments. While the protection and security of personal information is important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, auditability and availability of personal health information. This type of information is regarded by many as being among the most confidential of all types of personal information. Protecting this confidentiality is essential if the privacy of subjects of care is to be maintained. The integrity of health information must be protected to ensure patient safety, and an important component of that protection is ensuring that the information's entire life cycle be fully auditable. The availability of health information is also critical to effective healthcare delivery. Health informatics systems must meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks. Protecting the confidentiality, integrity and availability of health information therefore requires health-sector-specific expertise.

The need for effective IT security management in healthcare is made all the more urgent by the increasing use of wireless and Internet technologies in healthcare delivery. If not implemented properly, these complex technologies will increase the risks to the confidentiality, integrity and availability of health information. Regardless of size, location and model of service delivery, all healthcare organizations need to have stringent controls in place to protect the health information entrusted to them. Yet many health professionals work as solo health providers or in small clinics that lack the dedicated IT resources to manage information security. Healthcare organizations must therefore have clear, concise and healthcare-specific guidance on the selection and implementation of such controls. This guidance must be adaptable to the wide range of sizes, locations, and models of service delivery found in healthcare. Finally, with increasing electronic exchange of personal health information between health professionals, there is a clear benefit in adopting a common reference for information security management in healthcare.

ISO/IEC 27002 is already being used extensively for health informatics IT security management through the agency of national or regional guidelines in Australia, Canada, France, the Netherlands, New Zealand, South Africa and the United Kingdom. Interest is growing in other countries as well. This International Standard (ISO 27799) draws upon the experience gained in these national endeavours in dealing with the security of personal health information and is intended as a companion document to ISO/IEC 27002. It is not intended to supplant ISO/IEC 27002 or ISO/IEC 27001. Rather, it is a complement to these more generic standards.

This International Standard applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information. These considerations have, in some cases, led the authors to conclude that application of certain ISO/IEC 27002 control objectives is essential if personal health information is to be adequately protected. This International Standard therefore places constraints upon the application of certain security controls specified in ISO/IEC 27002. This in turn has led to the inclusion in Clause 7 of several normative statements stating that the application of a given security control is mandatory. For example, 7.2.1 states that

> *Organizations processing health information, including personal health information,* ***shall*** *have a written information security policy that is approved by management, published, and then communicated to all employees and relevant external parties.*

1) This guideline is consistent with the revised version of ISO/IEC 27002:2005.

© ISO 2008 – All rights reserved

In the health domain, it is possible for an organization (a hospital, say) to be certified using ISO/IEC 27001 without requiring certification against, or even acknowledgement of, this International Standard. It is to be hoped, however, that as healthcare organizations strive to improve the security of personal health information, conformance with this International Standard, as a stricter standard for healthcare, will also become widespread.

All of the security control objectives described in ISO/IEC 27002 are relevant to health informatics but some controls require additional explanations with regard to how they can be used best to protect the confidentiality, integrity and availability of health information. There are also additional health-sector-specific requirements. This International Standard provides additional guidance in a format that persons responsible for health information security can readily understand and adopt.

This International Standard's authors do not intend to write a primer on computer security, nor to restate what has already been written in ISO/IEC 27002 or in ISO/IEC 27001. There are many security requirements that are common to all computer-related systems, whether used in financial services, manufacturing, industrial control, or indeed in any other organized endeavour. A concerted effort has been made to focus on security requirements necessitated by the unique challenges of delivering electronic health information that supports the provision of care.

Who should read this International Standard?

This International Standard is intended for those responsible for overseeing health information security and for healthcare organizations and other custodians of health information seeking guidance on this topic, together with their security advisors, consultants, auditors, vendors and third-party service providers.

Benefits of using this International Standard

ISO/IEC 27002 is a broad and complex standard and its advice is not tailored specifically to healthcare. This International Standard allows for the implementation of ISO/IEC 27002, within health environments, in a consistent fashion and with particular attention to the unique challenges that the health sector poses. By following it, healthcare organizations help to ensure that the confidentiality and integrity of data in their care are maintained, that critical health information systems remain available, and that accountability for health information is upheld.

The adoption of this guidance by healthcare organizations both within and among jurisdictions will assist interoperation and enable the safe adoption of new collaborative technologies in the delivery of healthcare. Secure and privacy-protective information sharing can significantly improve healthcare outcomes.

As a result of implementing this guidance, healthcare organizations can expect to see the number and severity of their security incidents reduced, allowing resources to be redeployed to productive activities. IT security will thereby allow health resources to be deployed in a cost-effective and productive manner. Indeed, research by the respected Information Security Forum and by market analysts has shown that good all-round security can have as much as a 2 % positive effect upon organizations' results.

Finally, a consistent approach to IT security, understandable by all involved in healthcare, will improve staff morale and increase the trust of the public in the systems that maintain personal health information.

How to use this International Standard

Readers not already familiar with ISO/IEC 27002 are urged to read the introductory sections of that International Standard before continuing. Implementers of this Intenational Standard (ISO/IEC 27799) must first thoroughly read ISO/IEC 27002, as the text below will frequently refer the reader to the relevant sections of that International Standard. The present document cannot be fully understood without access to the full text of ISO/IEC 27002.

General readers not already familiar with health information security and its goals, challenges, and broader context, will benefit from reading a brief introduction, to be found in Clause 5.

This document is a preview generated by EVS

 © ISO 2008 – All rights reserved

Readers seeking guidance on how to implement ISO/IEC 27002 in a health environment will find a practical action plan described in Clause 6. No mandatory requirements are contained in this clause. Instead, general advice and guidance are given on how best to proceed with the implementation of 27002 in healthcare. The clause is organized around a cycle of activities (plan/do/check/act) that are described in ISO/IEC 27001 and that, when followed, will lead to a robust implementation of an information security management system.

Readers seeking specific advice on the eleven security control clauses and 39 main security control categories described in ISO/IEC 27002 will find it in Clause 7. This clause leads the reader through each of the eleven security control clauses of ISO/IEC 27002. Minimum requirements are stated where appropriate and, in some cases, normative guidelines are set out on the proper application of certain ISO/IEC 27002 security controls to the protection of health information.

This International Standard concludes with three informative annexes. Annex A describes the general threats to health information. Annex B briefly describes tasks and related documents of the information security management system. Annex C discusses the advantages of support tools as an aid to implementation. The Bibliography lists related standards in health information security.

This document is a preview generated by EVS

© ISO 2008 – All rights reserved

Health informatics — Information security management in health using ISO/IEC 27002

This document is a preview generated by EVS

1 Scope

1.1 General

This International Standard defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that standard[2)].

This International Standard specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information.

This International Standard applies to health information in all its aspects, whatever form the information takes (words and numbers, sound recordings, drawings, video and medical images), whatever means are used to store it (printing or writing on paper or electronic storage) and whatever means are used to transmit it (by hand, via fax, over computer networks or by post), as the information must always be appropriately protected.

This International Standard and ISO/IEC 27002 taken together define *what* is required in terms of information security in healthcare; they do not define *how* these requirements are to be met. That is to say, to the fullest extent possible, this International Standard is technology-neutral. Neutrality with respect to implementing technologies is an important feature. Security technology is still undergoing rapid development and the pace of that change is now measured in months rather than years. By contrast, while subject to periodic review, standards are expected on the whole to remain valid for years. Just as importantly, technological neutrality leaves vendors and service providers free to suggest new or developing technologies that meet the necessary requirements that this International Standard describes.

As noted in the introduction, familiarity with ISO/IEC 27002 is indispensable for an understanding of this International Standard.

1.2 Scope exclusions

The following areas of information security are outside the scope of this International Standard:

a) methodologies and statistical tests for effective anonymization of personal health information;

b) methodologies for pseudonymization of personal health information (see bibliographic Reference [10] for an example of an ISO Technical Specification that deals specifically with this subject);

c) network quality of service and methods for measuring availability of networks used for health informatics;

d) data quality (as distinct from data integrity).

2) This guideline is consistent with the revised version of ISO/IEC 27002:2005.

© ISO 2008 – All rights reserved

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/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 Health terms

3.1.1
health informatics
scientific discipline that is concerned with the cognitive, information-processing and communication tasks of healthcare practice, education and research, including the information science and technology to support these tasks

[ISO/TR 18307:2001, definition 3.73]

3.1.2
health information system
repository of information regarding the health of a subject of care in computer-processable form, stored and transmitted securely, and accessible by multiple authorized users

NOTE Adapted from ISO/TR 20514:2005, definition 2.25.

3.1.3
healthcare
any type of service provided by professionals or paraprofessionals with an impact on health status

[European Parliament, 1998, as cited by WHO]

3.1.4
healthcare organization
generic term used to describe many types of organizations that provide healthcare services

[ISO/TR 18307:2001, definition 3.74]

3.1.5
health professional
person who is authorized by a recognised body to be qualified to perform certain health duties

NOTE Adapted from ISO/TS 17090-1:2002, definition 3.18.

3.1.6
healthcare provider
any person or organization who is involved in, or associated with, the delivery of healthcare to a client, or caring for client wellbeing

3.1.7
identifiable person
one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

[ISO 22857:2004, definition 3.7]

This document is a preview generated by EVS

 © ISO 2008 – All rights reserved