

Health informatics - Information security management  
in health using ISO/IEC 27002 (ISO 27799:2016)

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

See Eesti standard EVS-EN ISO 27799:2016 sisaldab Euroopa standardi EN ISO 27799:2016 ingliskeelset teksti.	This Estonian standard EVS-EN ISO 27799:2016 consists of the English text of the European standard EN ISO 27799:2016.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 10.08.2016.	Date of Availability of the European standard is 10.08.2016.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile [standardiosakond@evs.ee](mailto:standardiosakond@evs.ee).

ICS 35.240.80

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

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

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:

Aru 10, 10317 Tallinn, Eesti; koduleht [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto:info@evs.ee)

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Aru 10, 10317 Tallinn, Estonia; homepage [www.evs.ee](http://www.evs.ee); phone +372 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

English Version

Health informatics - Information security management in  
health using ISO/IEC 27002 (ISO 27799:2016)

Informatique de santé - Management de la sécurité de  
l'information relative à la santé en utilisant l'ISO/IEC  
27002 (ISO 27799:2016)

Medizinische Informatik - Informationsmanagement  
im Gesundheitswesen bei Verwendung der ISO/IEC  
27002 (ISO 27799:2016)

This European Standard was approved by CEN on 18 June 2016.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

## European foreword

This document (EN ISO 27799:2016) 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 February 2017, and conflicting national standards shall be withdrawn at the latest by February 2017.

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.

This document supersedes EN ISO 27799:2008.

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 27799:2016 has been approved by CEN as EN ISO 27799:2016 without any modification.

# Contents

	Page
<b>Foreword</b> .....	<b>vii</b>
<b>Introduction</b> .....	<b>viii</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>2</b>
<b>3 Terms and definitions</b> .....	<b>2</b>
<b>4 Structure of this International Standard</b> .....	<b>3</b>
<b>5 Information security policies</b> .....	<b>4</b>
5.1 Management direction for information security.....	4
5.1.1 Policies for information security.....	4
5.1.2 Review of the policies for information security.....	5
<b>6 Organization of information security</b> .....	<b>6</b>
6.1 Internal organization.....	6
6.1.1 Information security roles and responsibilities.....	6
6.1.2 Segregation of duties.....	7
6.1.3 Contact with authorities.....	7
6.1.4 Contact with special interest groups.....	7
6.1.5 Information security in project management.....	8
6.2 Mobile devices and teleworking.....	8
6.2.1 Mobile device policy.....	8
6.2.2 Teleworking.....	9
<b>7 Human resource security</b> .....	<b>9</b>
7.1 Prior to employment.....	9
7.1.1 Screening.....	9
7.1.2 Terms and conditions of employment.....	10
7.2 During employment.....	11
7.2.1 Management responsibilities.....	11
7.2.2 Information security awareness, education and training.....	11
7.2.3 Disciplinary process.....	11
7.3 Termination and change of employment.....	12
7.3.1 Termination or change of employment responsibilities.....	12
<b>8 Asset management</b> .....	<b>12</b>
8.1 Responsibility for assets.....	12
8.1.1 Inventory of assets.....	12
8.1.2 Ownership of assets.....	13
8.1.3 Acceptable use of assets.....	13
8.1.4 Return of assets.....	13
8.2 Information classification.....	14
8.2.1 Classification of information.....	14
8.2.2 Labelling of information.....	15
8.2.3 Handling of assets.....	15
8.3 Media handling.....	16
8.3.1 Management of removable media.....	16
8.3.2 Disposal of media.....	16
8.3.3 Physical media transfer.....	17
<b>9 Access control</b> .....	<b>17</b>
9.1 Business requirements of access control.....	17
9.1.1 Access control policy.....	17
9.1.2 Access to networks and network services.....	18
9.2 User access management.....	18
9.2.1 User registration and de-registration.....	18
9.2.2 User access provisioning.....	19

9.2.3	Management of privileged access rights	19
9.2.4	Management of secret authentication information of users	20
9.2.5	Review of user access rights	20
9.2.6	Removal or adjustment of access rights	21
9.3	User responsibilities	21
9.3.1	Use of secret authentication information	21
9.4	System and application access control	22
9.4.1	Information access restriction	22
9.4.2	Secure log-on procedures	22
9.4.3	Password management system	22
9.4.4	Use of privileged utility programs	23
9.4.5	Access control to program source code	23
<b>10</b>	<b>Cryptography</b>	<b>23</b>
10.1	Cryptographic controls	23
10.1.1	Policy on the use of cryptographic controls	23
10.1.2	Key management	24
<b>11</b>	<b>Physical and environmental security</b>	<b>24</b>
11.1	Secure areas	24
11.1.1	Physical security perimeter	24
11.1.2	Physical entry controls	25
11.1.3	Securing offices, rooms and facilities	25
11.1.4	Protecting against external and environmental threats	25
11.1.5	Working in secure areas	25
11.1.6	Delivery and loading areas	25
11.2	Equipment	26
11.2.1	Equipment siting and protection	26
11.2.2	Supporting utilities	26
11.2.3	Cabling security	27
11.2.4	Equipment maintenance	27
11.2.5	Removal of assets	27
11.2.6	Security of equipment and assets off-premises	27
11.2.7	Secure disposal or reuse of equipment	28
11.2.8	Unattended user equipment	28
11.2.9	Clear desk and clear screen policy	28
<b>12</b>	<b>Operations security</b>	<b>29</b>
12.1	Operational procedures and responsibilities	29
12.1.1	Documented operating procedures	29
12.1.2	Change management	29
12.1.3	Capacity management	30
12.1.4	Separation of development, testing and operational environments	30
12.2	Protection from malware	30
12.2.1	Controls against malware	30
12.3	Backup	31
12.3.1	Information backup	31
12.4	Logging and monitoring	31
12.4.1	Event logging	31
12.4.2	Protection of log information	32
12.4.3	Administrator and operator logs	33
12.4.4	Clock synchronisation	34
12.5	Control of operational software	34
12.5.1	Installation of software on operational systems	34
12.6	Technical vulnerability management	34
12.6.1	Management of technical vulnerabilities	34
12.6.2	Restrictions on software installation	35
12.7	Information systems audit considerations	35
12.7.1	Information systems audit controls	35

<b>13</b>	<b>Communications security</b>	<b>35</b>
13.1	Network security management	35
13.1.1	Network controls	35
13.1.2	Security of network services	36
13.1.3	Segregation in networks	36
13.2	Information transfer	36
13.2.1	Information transfer policies and procedures	36
13.2.2	Agreements on information transfer	37
13.2.3	Electronic messaging	37
13.2.4	Confidentiality or non-disclosure agreements	38
<b>14</b>	<b>System acquisition, development and maintenance</b>	<b>38</b>
14.1	Security requirements of information systems	38
14.1.1	Information security requirements analysis and specification	38
14.1.2	Securing application services on public networks	40
14.1.3	Protecting application services transactions	40
14.2	Security in development and support processes	40
14.2.1	Secure development policy	40
14.2.2	System change control procedures	41
14.2.3	Technical review of applications after operating platform changes	41
14.2.4	Restrictions on changes to software packages	41
14.2.5	Secure system engineering principles	42
14.2.6	Secure development environment	42
14.2.7	Outsourced development	42
14.2.8	System security testing	42
14.2.9	System acceptance testing	43
14.3	Test data	43
14.3.1	Protection of test data	43
<b>15</b>	<b>Supplier relationships</b>	<b>43</b>
15.1	Information security in supplier relationships	43
15.1.1	Information security policy for supplier relationships	43
15.1.2	Addressing security within supplier agreements	44
15.1.3	Information and communication technology supply chain	44
15.2	Supplier service delivery management	44
15.2.1	Monitoring and review of supplier services	45
15.2.2	Managing changes to supplier services	45
<b>16</b>	<b>Information security incident management</b>	<b>45</b>
16.1	Management of information security incidents and improvements	45
16.1.1	Responsibilities and procedures	45
16.1.2	Reporting information security events	45
16.1.3	Reporting information security weaknesses	46
16.1.4	Assessment of and decision on information security events	47
16.1.5	Response to information security incidents	47
16.1.6	Learning from information security incidents	47
16.1.7	Collection of evidence	47
<b>17</b>	<b>Information security aspects of business continuity management</b>	<b>48</b>
17.1	Information security continuity	48
17.1.1	Planning information security continuity	48
17.1.2	Implementing information security continuity	49
17.1.3	Verify, review and evaluate information security continuity	49
17.2	Redundancies	49
17.2.1	Availability of information processing facilities	49
<b>18</b>	<b>Compliance</b>	<b>50</b>
18.1	Compliance with legal and contractual requirements	50
18.1.1	Identification of applicable legislation and contractual requirements	50
18.1.2	Intellectual property rights	50
18.1.3	Protection of records	50

18.1.4	Privacy and protection of personally identifiable information .....	51
18.1.5	Regulation of cryptographic controls .....	52
18.2	Information security reviews.....	52
18.2.1	Independent review of information security.....	52
18.2.2	Compliance with security policies and standards.....	52
18.2.3	Technical compliance review .....	53
<b>Annex A (informative)</b>	<b>Threats to health information security.....</b>	<b>54</b>
<b>Annex B (informative)</b>	<b>Practical action plan for implementing ISO/IEC 27002 in healthcare .....</b>	<b>59</b>
<b>Annex C (informative)</b>	<b>Checklist for conformance to ISO 27799.....</b>	<b>72</b>
<b>Bibliography</b>	.....	<b>98</b>



## 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](http://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](http://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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/TC 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO 27799:2008), which has been technically revised.

## 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. It is based upon and extends the general guidance provided by ISO/IEC 27002:2013 and 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 is to 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 is to 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.

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 therefore need clear, concise, and health-care-specific guidance on the selection and implementation of such controls. This International Standard is to 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 (including use of wireless and Internet services), 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, the United Kingdom and elsewhere. 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 the ISO/IEC 27000-series of standards. Rather, it is a complement to these more generic standards.

ISO 27799 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. ISO 27799 therefore places constraints upon the application of certain security controls specified in ISO/IEC 27002.

All of the security control objectives described in ISO/IEC 27002 are relevant to health informatics, but some controls require additional explanation in regard to how they can best be used 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.

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 ISO 27799. It is to be hoped, however, that as healthcare organizations strive to improve the security of personal health information, conformance with ISO 27799 as a stricter standard for healthcare will also become widespread.

### Objectives

Maintaining information confidentiality, availability, and integrity (including authenticity, accountability and auditability) are the overarching goals of information security. In healthcare, privacy of subjects of care depends upon maintaining the confidentiality of personal health information. To maintain

confidentiality, measures is also be taken to maintain the integrity of data, if for no other reason than that it is possible to corrupt the integrity of access control data, audit trails, and other system data in ways that allow breaches in confidentiality to take place or to go unnoticed. In addition, patient safety depends upon maintaining the integrity of personal health information, failure to do this can also result in illness, injury or even death. Likewise, a high level of availability is an especially important attribute of health systems, where treatment is often time-critical. Indeed, disasters that could lead to outages in other, non-health related, IT systems may be the very times when the information contained in health systems is most critically needed. Moreover, denial of service attacks against networked systems are increasingly common.

The controls discussed in this International Standard are those identified as appropriate in healthcare to protect confidentiality, integrity and availability of personal health information and to ensure that access to such information can be audited and accounted for. These controls help to prevent errors in medical practice that might ensue from failure to maintain the integrity of health information. In addition, they help to ensure that the continuity of medical services is maintained.

There are additional considerations that shape the goals of health information security. These includes the following:

- a) honouring legislative obligations as expressed in applicable data protection laws and regulations protecting a subject of care is right to privacy;<sup>1)</sup>
- b) maintaining established privacy and security best practices in health informatics;
- c) maintaining individual and organizational accountability among health organizations and health professionals;
- d) supporting the implementation of systematic risk management within health organizations;
- e) meeting the security needs identified in common healthcare situations;
- f) reducing operating costs by facilitating the increased use of technology in a safe, secure, and well managed manner that supports, but does not constrain current health activities;
- g) maintaining public trust in health organizations and the information systems these organizations rely upon;
- h) maintaining professional standards and ethics as established by health-related professional organizations (insofar as information security maintains the confidentiality and integrity of health information);
- i) operating electronic health information systems in an environment appropriately secured against threats;
- j) facilitating interoperability among health systems, since health information increasingly flows among organizations and across jurisdictional boundaries (especially as such interoperability enhances the proper handling of health information to ensure its continued confidentiality, integrity and availability).

#### Relation to information governance,<sup>2)</sup> corporate governance and clinical governance

While health organizations may differ in their positions on clinical governance and corporate governance, the importance of integrating and attending to information governance ought to be beyond debate as a vital support to both. As health organizations have become ever more critically dependent on information systems to support care delivery (e.g. by exploiting decision support technologies and trends towards “evidence based” rather than “experience based” healthcare), it has become evident that

1) In addition to legal obligations, a wealth of information is available on ethical obligations relating to health information, the code of ethics of the World Health Organization. These ethical obligations may also, in certain circumstances, impact health information security policy.

2) Note that in some countries, information governance is referred to as information assurance.

events in which losses of integrity, availability and confidentiality occur may have a significant clinical impact and that problems arising from such impacts will be seen to represent failures in the ethical and legal obligations inherent in a “duty of care”.

All countries and jurisdictions will undoubtedly have case studies where such breaches have led to misdiagnoses, deaths, or protracted recoveries. Clinical governance frameworks need therefore to treat effective information security risk management as equal in importance to care treatment plans, infection management strategies and other “core” clinical management matters. This International Standard will assist those responsible for clinical governance in understanding the contribution made by effective information security strategies.

#### Health information to be protected

There are several types of information whose confidentiality, integrity and availability<sup>3)</sup> needs to be protected by

- a) personal health information,
- b) pseudonymized data derived from personal health information through some methodology for pseudonymous identification,
- c) statistical and research data, including anonymized data derived from personal health information by removal of personally identifying data,
- d) clinical/medical knowledge not related to any specific subjects of care, including clinical decision support data (e.g. data on adverse drug reactions),
- e) data on health professionals, staff and volunteers,
- f) information related to public health surveillance,
- g) audit trail data, produced by health information systems, that contain personal health information or pseudonymous data derived from personal health information, or that contain data about the actions of users in regard to personal health information, and
- h) system security data for health information systems, including access control data and other security related system configuration data, for health information systems.

The extent to which confidentiality, integrity and availability need to be protected depends upon the nature of the information, the uses to which it is put, and the risks to which it is exposed. For example, statistical data [item c) above] may not be confidential, but protecting its integrity may be very important. Likewise, audit trail data [item g) above] might not require high availability (frequent archiving with a retrieval time measured in hours rather than seconds might suffice in a given application) but its content might be highly confidential. Risk assessment can properly determine the level of effort needed to protect confidentiality, integrity and availability (see [B.4.4](#)). The results of regular risk assessment need to be fitted to the priorities and resources of the implementing organization.

#### Threats and vulnerabilities in health information security

Types of information security threats and vulnerabilities vary widely, as do their descriptions. While none are truly unique to healthcare, what is unique in healthcare is the array of factors to be considered when assessing threats and vulnerabilities.

By their nature, health organizations operate in an environment where visitors and the public at large can never be totally excluded. In large health organizations, the sheer volume of people moving through operational areas is significant. These factors increase the vulnerability of systems to physical threats. The likelihood that such threats will occur may increase when emotional or mentally ill subjects of care or relatives are present.

---

3) Level of availability depends upon the uses to which the data will be put.

The critical importance of correctly identifying subjects of care and correctly matching them to their health records leads health organizations to collect detailed identifying information. Regional or jurisdictional patient registries (i.e. registries of subjects of care) are sometimes the most comprehensive and up-to-date repositories of identifying information available in a jurisdiction. This identifying information is of great potential value to those who would use it to commit identity theft and so should be rigorously protected.

Many health organizations are chronically under-funded and their staff members are sometimes obliged to work under significant stress and with systems kept in service long after they ought to have been retired. These factors can increase the potential for certain types of threat and can exacerbate vulnerabilities. On the other hand, clinical care involves a range of professional, technical, administrative, ancillary and voluntary staff, many of whom see their work as a vocation. Their dedication and diversity of experience can often usefully reduce exposure to vulnerabilities. The high level of professional training received by many health professionals also sets healthcare apart from many other industrial sectors in reducing the incidence of insider threats.

The health environment, with its unique threats and vulnerabilities should therefore be considered with special care. [Annex A](#) contains an informative list of the types of threat that need to be considered by health organizations when they assess risks to the confidentiality, integrity and availability of health information and to the integrity and availability of related information systems.

#### 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.

This International Standards 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.

#### Benefits of using this International Standard

ISO/IEC 27002 is a broad and complex International Standard and its advice is not tailored specifically to healthcare. ISO 27799 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 is maintained, that critical health information systems remain available and that accountability for health information is upheld.

The adoption of this International Standard by healthcare organizations both within and among jurisdictions will assist interoperability 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 International Standard, 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 clauses of that standard before continuing. The implementers of ISO 27799 is to read first thoroughly ISO/IEC 27002, as the text below will frequently refer the reader to the relevant clauses of that standard. The present International Standard cannot be fully understood without access to the full text of ISO/IEC 27002.

Readers seeking guidance on how to implement ISO/IEC 27002 in a health environment will find a practical action plan described in [Annex B](#). No mandatory requirements are contained in this clause. Instead, general advice and guidance are given on how best to proceed with implementation of ISO/IEC 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 security control security control categories and clauses described in ISO/IEC 27002 will find it in the clauses of this International Standard with the same clause number and title as is found in ISO/IEC 27002. This clause leads the reader through each of the eleven security control clauses of the 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.

Once ISO/IEC 27002 has been put into place, the ongoing management is considered essential if the benefits of the International Standard are to be maintained. Clause 18 discusses compliance assessment and the requirements for ongoing information security management. [Annex C](#) contains a self-assessment matrix with regard to compliance.

This International Standard concludes with four informative appendices.

[Annex A](#) describes the general threats to health information. [Annex B](#) briefly describes a practical action plan for implementing complementary information security related International Standards. [Annex C](#) provides a checklist for compliance to ISO 27799. [Clause 2](#) lists the standards that are cited in a normative way; the Bibliography lists other related standards in health information security.

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

## 1 Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard.<sup>4)</sup>

This International Standard provides implementation guidance for the controls described in ISO/IEC 27002 and supplements them where necessary, so that they can be effectively used for managing health information security. 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 in their care.

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 storage electronically), and whatever means are used to transmit it (by hand, through fax, over computer networks, or by post), as the information is 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, International 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 to an understanding of this International Standard.

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 Bibliography for a brief description of a Technical Specification that deals specifically with this topic);
- c) network quality of service and methods for measuring availability of networks used for health informatics;
- d) data quality (as distinct from data integrity).

---

4) This International Standard is consistent with the revised version of ISO/IEC 27002.

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

### 3.1 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

[SOURCE: ISO/TR 18307:2001, 3.73]

### 3.2 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 authorised users

[SOURCE: ISO/TR 20514:2005]

### 3.3 healthcare

type of services provided by professionals or paraprofessionals with an impact on health status

[SOURCE: European Parliament, 1998, as cited by WHO]

### 3.4 healthcare organization

organization that provides healthcare services

[SOURCE: ISO/TR 18307:2001, 3.74]

### 3.5 health professional

person who is authorised by a recognised body to be qualified to perform certain health duties

[SOURCE: ISO 17090-1:2013]

### 3.6 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

[SOURCE: ISO 22857:2013, 3.7]

### 3.7 patient

subject of care (3.9) consisting of one person