SLOVENSKI STANDARD
oSIST prEN ISO 27799:2025

01-marec-2025

Nadomešča:
SIST EN ISO 27799:2017

Zdravstvena informatika - Vodenje informacijske varnosti v zdravstvu z uporabo standarda ISO/IEC 27002 (ISO/DIS 27799:2025)

Health informatics - Information security management in health using ISO/IEC 27002 (ISO/DIS 27799:2025)

Medizinische Informatik - Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO/DIS 27799:2025)

Informatique de santé - Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002 (ISO/DIS 27799:2025)

Ta slovenski standard je istoveten z: **prEN ISO 27799**

ICS:

35.030	Informacijska varnost	IT Security
35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

oSIST prEN ISO 27799:2025 **en,fr,de**

DRAFT International Standard

ISO/DIS 27799

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

Informatique de santé — Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002

ICS: 35.030; 35.240.80

ISO/TC **215**

Secretariat: **ANSI**

Voting begins on:
2025-01-20

Voting terminates on:
2025-04-14

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 27799:2025(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO *had not* received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC *215*, *Health informatics*.

This third edition cancels and replaces the second edition (ISO 27799:2016), which has been technically revised.

The main changes are as follows:

- alignment with the new structure of ISO/IEC 27002:2022 and other changes to that standard from the previous version
- revision and addition of controls specific to health
- removal of material that is in ISO/IEC 27002:2022 but was not in the previous version of that standard.
- addition of informative Annexes providing i) supplementary guidance on cybersecurity in health organizations and ii) example security and privacy requirements for health information systems.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 General

This document provides a set of information security controls including implementation guidance and other supporting information for health organizations. It is based on ISO/IEC 27002:2022 and has a similar structure.

0.2 Context and Background

When considering information security in the context of healthcare, a wide range of factors has to be taken into account including the following:

a) Equipment that relies on digital technologies for its operation and is deployed exclusively or predominantly in the healthcare domain. Medical devices incorporating health software are the prime example.

b) The need to balance clinical safety and effectiveness with information security.

c) Maintaining the privacy of subjects of care while ensuring access to relevant personal health information for diagnosis and treatment.

d) The distributed nature of personal health information both within and between organizations (possibly in different jurisdictions) resulting in the need for high levels of interoperability between diverse systems, applications and devices.

e) Users of many different kinds including doctors, nurses, other clinicians, trainees, students, healthcare assistants, technicians, administrative staff and volunteers as well as subjects of care and their proxies.

f) The multiple interdependencies and information flows between and within organizations responsible for one or more of: healthcare, clinical research, teaching, education and training.

g) The need for some healthcare services to be available on a continuous basis (24 hours a day every day) under normal circumstances. In addition, natural disasters and other unusual events that can lead to surges in demand for healthcare services.

h) Organizations providing health services as well as manufacturers or suppliers of systems, devices and equipment are all subject to a wide range of legal, statutory, regulatory and contractual requirements which can vary between jurisdictions.

i) Overlapping or incomplete requirements for accountability and professional responsibility between different professions (such as ICT and medical devices staff) for ensuring security and safety of systems, devices and equipment.

Given this overall context, healthcare has a number of sector-specific, if not unique, information security requirements. However, the controls in ISO/IEC 27002:2022 are intentionally generic, hence the need for this document.

0.3 Audience and Uses

This document is targeted at organizations that:

— provide healthcare services or are custodians of personal health information for other reasons;

— supply software, systems, devices, equipment or services that are used to process personal health information;

— are responsible for healthcare regulation, accreditation, inspection, assurance or similar.

Individuals for whom this document is particularly relevant include:

— ICT and medical devices or equipment professionals working in the types of organizations listed above;

— information security professionals (particularly those unfamiliar with the health domain): these professionals can include consultants, penetration testers, auditors and those working for bodies that provide certification to ISO/IEC 27001.

Appropriate implementation of the controls in this document can provide assurance to individuals, including subjects of care, their proxies and members of an organization's workforce. Appropriate implementation can also provide assurance to a wide range of stakeholder bodies including management and governance boards of healthcare organizations, other healthcare organizations with which information is exchanged or shared, public authorities, regulators, auditors, and organizations that finance, insure, accredit or inspect healthcare services.

This document can be used in healthcare settings when determining and implementing controls for an information security management system (ISMS) conformant to ISO/IEC 27001.

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

1 Scope

This document provides a set of information security controls, including implementation guidance, for health organizations. It is based on ISO/IEC 27002:2022.

In addition to generic ICT equipment and software used in many other environments, the scope of this document includes software and systems specifically for healthcare, such as electronic health record systems and medical devices incorporating health software. Such medical devices can be programmed or programmable and can contain software, firmware or both.

Also in scope is other digital equipment (such as that for environmental and infection control, building management, and physical security) that can be used in premises where healthcare is provided.

This document applies to health and other relevant information in all its aspects, whatever form the information takes (including text and numbers, sound recordings, drawings, images and video), by whatever means it has been acquired or captured, whatever means are used to store it (such as printing or writing on paper or storage electronically), and whatever means are used to transfer or exchange it (orally, by hand, by post, movement of storage media, direct links or networking).

This document is for organizations of all types and sizes that provide healthcare or are custodians of personal health information for other reasons. The information that they are responsible for can be stored and processed in many possible ways and locations, including on premises or in the cloud, but remains in scope.

This document applies to all physical settings where healthcare is intended to be delivered, such as hospitals, clinics and other locations or facilities designated for healthcare purposes such as ambulances and mobile imaging or diagnostic units. It also applies to care provided elsewhere, such as in residential premises. In addition to the range of settings, this document applies to all methods of service provision including remote or virtual healthcare.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27002:2022, ISO 81001-1:2021 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1 Terms and definitions

3.1.1
health
complete physical, mental and social well-being

Note 1 to entry: Health is not merely the absence of disease or infirmity.

[SOURCE: World Health Organization constitution, https://www.who.int/about/governance/constitution , modified changed second part of definition into a note.]

3.1.2
health software
software intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a medical device

Note 1 to entry: Health software fully includes what is considered software as a medical device.

[SOURCE: ISO 81001-1:2021, 3.3.9]

3.1.3
healthcare
care activities, services, management or supplies related to the health of an individual

3.1.4
personal health information
information about an identifiable person that relates to the physical or mental health of the individual

Note 1 to entry: Personal health information may include:

a) information about the registration of the individual for the provision of health services;

b) information about payments or eligibility for healthcare in respect to the individual;

c) a number, symbol, or particular assigned to an individual to uniquely identify the individual for health purposes;

d) any information about the individual that is collected in the course of the provision of health services to the individual;

e) information derived from the testing or examination of a body part or bodily substance;

f) identification of a person (for instance a health professional) as a provider of healthcare to the individual.

Note 2 to entry: Personal health information does not include information that, either by itself or when combined with other information available to the holder, is anonymized and, therefore, the identity of the individual who is the subject of the information cannot be ascertained from the information.

3.1.5
subject of care
person who seeks to receive, is receiving, or has received healthcare

[SOURCE: ISO 13940:2015, 5.2.1, modified - the words "healthcare actor with a person role" replaced with "person"]

3.1.6
subject of care proxy
person with the right to take decisions on behalf of the subject of care

EXAMPLE 1 Parents of children who are not yet adults.

EXAMPLE 2 Guardians of adults with learning disabilities or lacking mental capacity.

[SOURCE: ISO 13940:2015, 5.2.3.3.1 modified and examples added]

3.2 Abbreviated terms

HLT health

ICT information and communication technology

ISMS information security management system

PII personally identifiable information

4 General

4.1 Structure of this Document

This document lists all the controls in ISO/IEC 27002:2022, using the same control titles and structure as Clauses 5-8 in that standard, and:

a) indicates which controls (including their purposes, guidance and any other information) in ISO/IEC 27002:2022 apply unchanged in health;

b) for certain controls in ISO/IEC 27002:2022: provides guidance, other information, or both on how to apply the controls in health;

c) for the remaining controls in ISO/IEC 27002:2022: supplements what each control is, its purpose and guidance. Other information for health is also provided in some of these instances;

d) specifies controls that are specific to health and that are not based on any existing controls in ISO/IEC 27002:2022. These additional controls have the same layout as the controls in ISO/IEC 27002 and the control titles are prefixed with "HLT" (for HeaLTh).

In relation to ISO/IEC 27002:2022, controls in c) and d) are supplementary and additional respectively.

This document contains 4 Annexes:

— Annex A is a reference list of the controls specific to health, namely those under c) and d). The Annex also complements ISO/IEC 27001:2022, Annex A.

— Annex B provides a mapping table showing the correspondence of the HLT controls in this document with controls in ISO 27799:2016. It provides support for the transition between the two editions and complements ISO/IEC 27002:2022, Annex B.

— Annex C provides information on aspects of healthcare that are of particular importance in the context of information security.

— Annex D provides requirements for the development and acquisition of health IT systems and a mapping to MDS2 (manufacturer disclosure statement for medical device security).

4.2 Safety

Security, safety and health information system effectiveness are interdependent. It is essential to take this into account when assessing and managing risks and their risk control measures. For example, a risk that systems or data will not be available at the point-of-care is not just a security risk; it can have significant impact on safety if decision-making about care is compromised. In turn, this can impact the effectiveness of the health system.

A consequence of the interdependence of security, safety and effectiveness is that well-intended risk control measures can, in some instances, adversely impact one or both of the other properties. For instance, adding controls to reduce the risk resulting from unauthorized access can impact system usability and availability and hence compromise system effectiveness. It can also result in system workarounds that adversely impact safety.

Safety should be taken into account in all aspects of information security management in health, including the selection and application of controls. Accordingly, any impacts on safety should be considered when implementing controls in this document.

4.3 Selecting and applying controls

4.3.1 Determining controls

Determining controls is dependent on the organization's decisions following a risk assessment with a clearly defined scope. Decisions related to identified risks should be based on the criteria for risk acceptance, risk treatment options and the risk management approach applied by the organization. The determination of controls should also take into consideration all relevant national and international legislation and regulations. Control determination also depends on the manner in which controls interact with one another to provide defence in depth.

Health organizations should select information security controls from this document and ISO/IEC 27002 as appropriate. In addition, new information security controls can be designed to meet specific needs as necessary.

4.3.2 Application of Guidance

Where healthcare-specific guidance for a control is provided in this document and the control is being implemented, that guidance should either be followed or the reason for not following it should be documented along with an explanation of how the control's purpose will be met ('comply or explain').

Within the guidance for some controls, there are cross references to other controls in this document and/or to other standards. Such cross-references are for information.

4.3.3 Use with ISO/IEC 27001:2022

The supplementary and additional controls, as listed in Annex A, can be used when determining and implementing controls in health settings for an information security management system (ISMS) that is conformant to ISO/IEC 27001.

It is a requirement of ISO/IEC 27001:2022, 6.1.3 that organizations produce a Statement of Applicability. The controls in Annex A can also be used in this connection.

5 Organizational controls

5.1 Policies for information security

Control 5.1, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

The information security policy should set out the approach to managing information security and be approved by the highest management level, then reviewed at least annually and after the occurrence of any serious security incident.

Purpose for health (supplementary)

To ensure top-management commitment to information security, that is kept up to date.

Guidance for health

The information security policy should contain statements on:

a) the need for health information security;