

Health informatics - Information security controls in
health based on ISO/IEC 27002 (ISO 27799:2025)

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO 27799:2026 sisaldab Euroopa standardi EN ISO 27799:2026 ingliskeelset teksti.	This Estonian standard EVS-EN ISO 27799:2026 consists of the English text of the European standard EN ISO 27799:2026.
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 and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 14.01.2026.	Date of Availability of the European standard is 14.01.2026.
Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

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

ICS 35.030, 35.240.80

Standardite ja standardilaadsete dokumentide reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele Eesti standardid ja standardilaadsed dokumendid on Eesti Standardimis- ja Akrediteerimiskeskuse intellektuaalomand ning neid kasutatakse litsentsi alusel dokumentide kasutuslepingu tingimuste kohaselt. Ilma Eesti Standardimis- ja Akrediteerimiskeskuse eelneva kirjaliku loata on keelatud standardite ja standardilaadsete dokumentide täielik või osaline reprodutseerimine, levitamine, muutmine või kasutamine mis tahes kujul ja viisil - sealhulgas kopeerimise, skaneerimise, salvestamise või jagamise teel digiplatvormidel (k.a masinõppe ja tehisintellekti rakendustes). Loata kasutamine väljaspool litsentsi tingimusi käsitletakse õigusrikkumisenä. Kui Teil on küsimusi standardite ja standardilaadsete dokumentide autoriõiguse kaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: Veebileht www.evs.ee; telefon +372 6055050; e-post info@evs.ee The right to reproduce and distribute standards and standard-like documents belongs to the Estonian Centre for Standardisation and Accreditation Estonian standards and standard-like documents are the intellectual property of the Estonian Centre for Standardisation and Accreditation and are made available under license in accordance with the terms and conditions of the document use agreement. Without the prior written permission of the Estonian Centre for Standardisation and Accreditation, the full or partial reproduction, distribution, modification, or use of standards and standard-like documents in any form or by any means - including photocopying, scanning, storing, or sharing via digital platforms (incl. in machine learning and artificial intelligence applications) - is strictly prohibited. Any unauthorized use beyond the scope of the granted license is prohibited and may result in legal action. If you have any questions about copyright, please contact Estonian Centre for Standardisation and Accreditation: Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee
--

English Version

Health informatics - Information security controls in health based on ISO/IEC 27002 (ISO 27799:2025)

Informatique de santé - Contrôles de sécurité de
l'information dans le domaine de la santé basés sur
l'ISO/IEC 27002 (ISO 27799:2025)

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

This European Standard was approved by CEN on 14 December 2025.

This European Standard was corrected and reissued by the CEN-CENELEC Management Centre on 11 March 2026.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

This document (EN ISO 27799:2026) 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 July 2026, and conflicting national standards shall be withdrawn at the latest by July 2026.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document supersedes CEN ISO/TS 14441:2013, EN ISO 27799:2016.

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN website.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO 27799:2025 has been approved by CEN as EN ISO 27799:2026 without any modification.



**International
Standard**

ISO 27799

**Health informatics — Information
security controls in health based on
ISO/IEC 27002**

*Informatique de santé — Contrôles de sécurité de l'information
dans le domaine de la santé basés sur l'ISO/IEC 27002*

**Third edition
2025-12**

This document is a preview generated by EVS



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
3.1 Terms and definitions	2
3.2 Abbreviated terms	3
4 General	3
4.1 Structure of this document	3
4.2 Safety	3
4.3 Selecting and applying controls	4
4.3.1 Determining controls	4
4.3.2 Application of guidance	4
4.3.3 Use with ISO/IEC 27001:2022	4
5 Organizational controls	4
5.1 Policies for information security	4
5.2 Information security roles and responsibilities	6
5.3 Segregation of duties	7
5.4 Management responsibilities	7
5.5 Contact with authorities	7
5.6 Contact with special interest groups	7
5.7 Threat intelligence	7
5.8 Information security in project management	8
5.9 Inventory of information and other associated assets	8
5.10 Acceptable use of information and other associated assets	9
5.11 Return of assets	9
5.12 Classification of information	9
5.13 Labelling of information	10
5.14 Information transfer	10
5.15 Access control	11
5.16 Identity management	11
5.17 Authentication information	12
5.18 Access rights	12
5.19 Information security in supplier relationships	13
5.20 Addressing information security within supplier agreements	13
5.21 Managing information security in the ICT supply chain	13
5.22 Monitoring, review and change management of supplier services	14
5.23 Information security for use of cloud services	14
5.24 Information security incident management planning and preparation	14
5.25 Assessment and decision on information security events	14
5.26 Response to information security incidents	14
5.27 Learning from information security incidents	14
5.28 Collection of evidence	15
5.29 Information security during disruption	15
5.30 ICT readiness for business continuity	15
5.31 Legal, statutory, regulatory and contractual requirements	16
5.32 Intellectual property rights	16
5.33 Protection of records	16
5.34 Privacy and protection of PII	16
5.35 Independent review of information security	17
5.36 Conformance with policies, rules and standards for information security	17
5.37 Documented operating procedures	18
5.38 HLT – Information security requirements analysis and specification	18

5.39	HLT – Uniquely identifying subjects of care	19
5.40	HLT – Validation of displayed/printed data	20
5.41	HLT – Publicly available health information	20
5.42	HLT – Emergency communication	21
5.43	HLT – External incident reporting	21
6	People controls	22
6.1	Screening	22
6.2	Terms and conditions of employment	22
6.3	Information security awareness, education and training	23
6.4	Disciplinary process	23
6.5	Responsibilities after termination or change of employment	23
6.6	Confidentiality or non-disclosure agreements	24
6.7	Remote working	24
6.8	Information security event reporting	24
6.9	HLT – Management training	25
7	Physical controls	25
7.1	Physical security perimeters	25
7.2	Physical entry	26
7.3	Securing offices, rooms and facilities	26
7.4	Physical security monitoring	26
7.5	Protecting against physical and environmental threats	26
7.6	Working in secure areas	26
7.7	Clear desk and clear screen	26
7.8	Equipment siting and protection	27
7.9	Security of assets off-premises	27
7.10	Storage media	27
7.11	Supporting utilities	28
7.12	Cabling security	28
7.13	Equipment maintenance	28
7.14	Secure disposal or re-use of equipment	29
8	Technological controls	29
8.1	User endpoint devices	29
8.2	Privileged access rights	29
8.3	Information access restriction	29
8.4	Access to source code	29
8.5	Secure authentication	30
8.6	Capacity management	30
8.7	Protection against malware	30
8.8	Management of technical vulnerabilities	30
8.9	Configuration management	31
8.10	Information deletion	31
8.11	Data masking	32
8.12	Data leakage prevention	32
8.13	Information backup	32
8.14	Redundancy of information processing facilities	32
8.15	Logging	32
8.16	Monitoring activities	32
8.17	Clock synchronization	33
8.18	Use of privileged utility programs	33
8.19	Installation of software on operational systems	33
8.20	Networks security	33
8.21	Security of network services	33
8.22	Segregation of networks	33
8.23	Web filtering	34
8.24	Use of cryptography	34
8.25	Secure development life cycle	34
8.26	Application security requirements	34

8.27	Secure system architecture and engineering principles	34
8.28	Secure coding	34
8.29	Security testing in development and acceptance	35
8.30	Outsourced development	35
8.31	Separation of development, test and production environments	35
8.32	Change management	35
8.33	Test information	35
8.34	Protection of information systems during audit testing	35
8.35	HLT – Zero trust principles	36
Annex A (informative) Information security controls for health reference		37
Annex B (informative) Correspondence of this document with ISO 27799:2016		39
Annex C (informative) Information security in health organizations		40
Annex D (informative) Example security and privacy requirements for health information systems and their mapping to the ISO 27799 controls and IEC/TS 81001-2-2 security capabilities		51
Bibliography		71

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).

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*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 251, *Health informatics*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This third edition cancels and replaces ISO 27799:2016 and ISO/TS 14441:2013, which have 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 was originally only in the second edition of this document but was subsequently included in ISO/IEC 27002:2022;
- addition of informative Annexes providing supplementary guidance on cybersecurity in health organizations and, based on ISO/TS 14441:2013, 5.3, updated 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 contains a set of information security controls for health organizations. It considers all the controls in ISO/IEC 27002:2022 and, in some cases, supplements the controls or provides guidance on their application in health. There are also some additional controls specific to health which are not derived from any in ISO/IEC 27002:2022.

0.2 Context and background

Factors that affect information security in healthcare include the following:

- a) Use of 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 accreditation, inspection, assurance or certification services for information security.

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 controls in health based on ISO/IEC 27002

1 Scope

This document provides 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.

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

This document applies to 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*

ISO 81001-1, *Health software and health IT systems safety, effectiveness and security — Part 1: Principles and concepts*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 27002:2022, ISO 81001-1 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>