

DIN EN ISO 27799:2026-03 (E)

Health informatics - Information security controls in health based on ISO/IEC 27002 (ISO 27799:2025); English version EN ISO 27799:2026

Contents

Page

- Foreword..... vi
- Introduction vii
- 1 Scope..... 1**
- 2 Normative references 1**
- 3 Terms, definitions and abbreviated terms 1**
 - 3.1 Terms and definitions2
 - 3.2 Abbreviated terms3
- 4 General 3**
 - 4.1 Structure of this document3
 - 4.2 Safety.....3
 - 4.3 Selecting and applying controls4
 - 4.3.1 Determining controls4
 - 4.3.2 Application of guidance.....4
 - 4.3.3 Use with ISO/IEC 27001:20224
- 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 responsibilities7
 - 5.5 Contact with authorities7
 - 5.6 Contact with special interest groups.....7
 - 5.7 Threat intelligence7
 - 5.8 Information security in project management8
 - 5.9 Inventory of information and other associated assets8
 - 5.10 Acceptable use of information and other associated assets9
 - 5.11 Return of assets9
 - 5.12 Classification of information.....9
 - 5.13 Labelling of information10
 - 5.14 Information transfer10
 - 5.15 Access control.....11
 - 5.16 Identity management.....11
 - 5.17 Authentication information12
 - 5.18 Access rights.....12
 - 5.19 Information security in supplier relationships13
 - 5.20 Addressing information security within supplier agreements13
 - 5.21 Managing information security in the ICT supply chain.....13
 - 5.22 Monitoring, review and change management of supplier services14
 - 5.23 Information security for use of cloud services14
 - 5.24 Information security incident management planning and preparation14
 - 5.25 Assessment and decision on information security events14
 - 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 continuity15
 - 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